National Motor Freight Traffic Association

A Survey of Heavy Vehicle Cyber Security

September 21, 2015

(Updated January 4, 2016)

NMFTA • 1001 North Fairfax • Suite 600 • Alexandria, Virginia 22314 • TEL: 703-838-1810

[PAGE INTENTIONALLY LEFT BLANK]

Disclaimers

The information contained in this document is subject to change without notice. The information contained in this document is presented in good faith, and is believed to be correct, but correctness and completeness is subject to the limitations of an expedited research and writing cycle.

Certain statements contained herein may be statements of future expectations and other forward-looking statements that are based on management's current views and assumptions and involve known and unknown risks and uncertainties that could cause actual results, performance or events to differ materially from those expressed or implied in such statements. In addition to statements which are forward-looking by reason of context, the words ‘may, will, should, expects, plans, intends, anticipates, believes, estimates, predicts, potential, or continue’ and similar expressions identify forward-looking statements.

Actual results, performance or events may differ materially from those in such statements due to, without limitation, (i) general economic conditions, including in particular economic conditions in NMFTA’s core business and core markets, (ii) performance of financial markets, including emerging markets, (iii) changes in regulatory environment in which the NMFTA operates.

The matters discussed herein may also involve risks and uncertainties described from time to time in NMFTA’s filings. The company assumes no obligation to update any forward-looking information contained herein.

Trademarks

[PAGE INTENTIONALLY LEFT BLANK]

TABLE OF CONTENTS

1 Introduction

Of the 270 million registered vehicles in the United States in 2013,[1] approximately 249 million of them were cars and light trucks. And, each year, at least 10 million new vehicles are registered (as much of the older inventory is retired). The modern automobile is heavily computerized and includes millions of lines of software code that controls a significant portion of the vehicles functionality. Automobiles are also more frequently being "connected" via such services as GM OnStar®, BMW Assist®, Ford SYNC®, Fiat-Chrysler-Jeep Uconnect®, etc. which allow remote diagnostics and assistance. Any time there are computer systems and connectivity there is always the chance for mischief by malicious users looking to "hack" the system. As has been seen in many prominent stories in the media recently, hackers have been able to take control of these computer systems and make them act contrary to the benefit of the occupant(s) of the vehicle.

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 trucks on the road each year.

Modern heavy vehicles are typically as computerized as passenger vehicles, but they are harder for security researchers to get their hands on. And, as a consequence, there is a lack of studies by security researchers into their specific vulnerabilities.

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"; heavy duty vehicles have been more pervasively "connected" for telematics, fleet management, and engine management using both satellite and cellular communication technologies for quite some time. The hardest part of hacking vehicles is really gaining access, ideally remote access. Yet, it seems that not only do heavy vehicles have many more avenues for remote access, but they also have a broader attack surface in general due to a larger number of advanced computerized features and fleet homogeneity.

In this paper we have tried to survey the available literature and knowledge on heavy vehicle system design, security vulnerabilities, potential consequences of a breach, current ongoing hacking activity, as well as the current state of affairs on who is doing what, if anything, to secure heavy vehicles. Due to the near absence of experimental data on heavy vehicles we have had to research passenger vehicle security and extrapolate how that information applies to heavy vehicles. This seems mostly 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. As a large amount of the research in this area is being conducted and funded by government agencies, we cannot exclude the possibility that more data and information exists specifically for heavy vehicles but that it has not been published or we have not been able to locate it within the limited timeframe that we have had to prepare this paper.

[1] 2013 is the latest year for which figures are available (NHTSA 2015 Publication).

2 Background

The muscle cars of the 1960s are iconic. During this "golden age" of automobiles, engines -- in even the most basic models -- were largely carbureted *mechanical* big block, large-displacement models which were optimized for horse power. Emissions (pollution) and fuel efficiency were not prime concerns.

Since those days, engine, exhaust systems and the powertrain technology changed to meet increasing constraints in terms of fuel efficiency, emissions, and safety. The revolution in microprocessors (embedded computers) has become an ever increasing and important part of the response. Driven by automotive manufacturers themselves -- who invested heavily in (new) electronics divisions -- a 'virtuous' cycle ensued and carbureted engines with their crude electro mechanical and pneumatic/vacuum-pressure feedback and controls were largely replaced by interconnected (often reprogrammable) computers, sensors and actuators. Performance now meant computer control in order to maintain acceptable output (power or torque), satisfy emissions requirements (reduce pollution) and meet or exceed fuel efficiency (CAFE MPG) requirements.[2]

2.1 Vehicle Computer Systems Overview

Today's vehicle is composed of a number of interconnected sensors, actuators and microprocessors called Electronic Control Units (ECUs) tied together by a local network throughout the vehicle 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 was 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 data from the many sensors in the vehicle as well as analyze the results with respect to expected (and legislatively mandated) performance criteria.

A frustrated vehicle owner might find the Malfunction Indicator Light (MIL) -- or Check Engine Light (CEL) --- begging for their attention; however, meaningful information would only be available to their mechanic when accessing an Onboard Diagnostic (OBD) port, which might be located anywhere in the car, to read the manufacturers proprietary Diagnostic Trouble Codes (DTC).

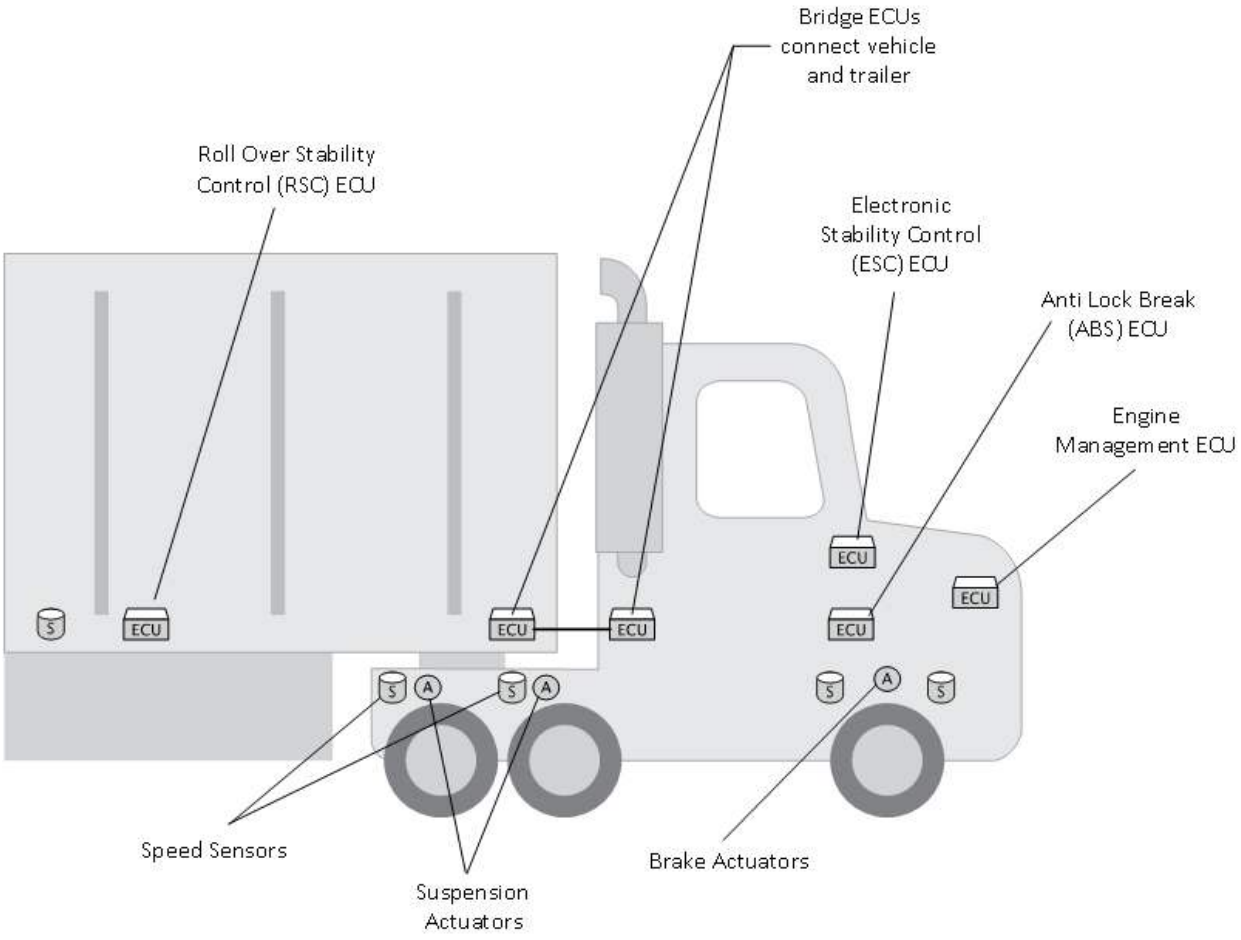
OBD standards progressed slowly until the OBD-II California Air Resources Board (CARB) standard was mandated in 1994 for all model year (MY) 1996 vehicles to be sold in California. The EPA extended the OBD-II requirement to *all* MY 1996 cars sold in the United States. European regulators would adopt highly congruent OBD standards. The European On Board Diagnostics (EOBD) standard was phased in from 2001 through 2007 for cars and light trucks with gasoline and diesel engines.

ODB-II standardizes diagnostic routines, messages and specifies both the design and placement of the diagnostic connector. 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

[2] Indeed, today's reader is likely to only encounter engines without microcontroller ECUs in their lawnmower and other such power tools. However, even these are increasingly subject to tightened EPA emission controls.

required MY 2008 cars to all use a well-defined 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.



There are interesting differences between SAE J1939 and OBD-II. However, in summary analysis, both standards have a common weakness, the CAN bus. The SAE J1939 avails itself of an enhanced messaging protocol running on the CAN bus, manages many communications with some basic security and is generally less 'chatty'. However, our analysis is that heavy vehicles using SAE J1939 will be susceptible to the same attack vectors which exploit the CAN bus to compromise vehicle ECUs.

In the next three sections, we will examine why vehicles have evolved to have such extensive computerization on the CAN network *(the good)*, the vulnerabilities that are inherent in this architecture *(the bad)*, and how those vulnerabilities are exploited *(and the ugly)*.

[PAGE INTENTIONALLY LEFT BLANK]

3 The Good: Computers Drive Vehicle Feature Evolution

The computerization of vehicles has progressed well beyond direct engine management. The Engine Management Unit (EMU) is but one of many Electronic Control Units (ECUs) active in core vehicle architecture.

At its *core*, a vehicle consists of an *engine* and *drivetrain* (transmission, differential and axles to transfer power to the wheels), *brakes* and *wheels* (steering and drive). Each of these core systems is, today, under significant control by ECUs. Additionally, there are groups of sensors, actuators, and intelligent ECUs grouped together for purposes such as managing the fuel system, engine cooling and lubrication, throttle control and exhaust. It can be useful to think of these component groups as systems in and of themselves. And, it is important to appreciate that they may be (physically or logically) component (i.e. sub-systems) of other systems that implement mechanisms for monitoring (sensors), adjustment (actuators) and intelligent controller (ECU) of key functionality.

Similarly, the functions for commanding control of a vehicle are, at their *core*, the means *steering*, *braking*, and *control* of the *drivetrain* (gear selection and throttle control). Again, each of these systems is, today, under significant control by ECUs.

But a vehicle is more than just these core systems. Every day travel with a car, getting from A to B:

- needs to be done in safety. Minimum vehicle equipment regulations mandate features such as windshield wipers, driver and passenger front air bags, tensioned seat belts, door locks, anti-theft controls, and headlights and signals. And, sophisticated driver assistance in the form of Electronic Stability Control. And,

- is preferably done in comfort. We should also acknowledge that few drivers would welcome a vehicle without some form of entertainment system (radio, CD player, etc) and climate control (heater and yes, please, air conditioning). Why not have power seats and remote locking too. The list continues; and, yes, each feature involves microprocessor ECU control.

No one spends more time in their vehicle than commercial drivers; and, commercial drivers expect safety and comfort in the truck too.

3.1 Driver Assistance: Computer Actuated Braking: ABS > TCS > RSC > ESC

Computer assisted braking systems have been available since the 1970's, yet then -- and for decades to follow -- most drivers still learned about pumping their brakes as they entered a skid. Today, Anti-Lock Braking (ABS) systems are a nearly ubiquitous safety feature and, as a consequence, drivers today learn to trust the computer to automatically modulate the brakes for them.

In an ABS system, sensors report the rotational speed of each wheel to a microcontroller which is able to actuate, i.e. physically control, braking pressure. If a wheel is detected as rotating significantly slower than the others, then braking force is reduced (or modulated). As ABS systems have evolved, the braking force applied to each *individual* wheel is now often under computer control.

With wheel speed known and braking under computer control, it is possible to implement additional control logic. If sensors show one wheel, or even both wheels on the same axle, is (are) moving

significantly faster than other wheels, then application of braking force to those wheels can help restore traction. And, indeed, therein is the foundation of a basic Traction Control System (TCS).

With some additional logic, but still the same configuration of sensors and actuators, we can teach (upgrade the programming of) an ABS controller to include TCS; yet, it is still a single discrete system with wires directly linking the sensors and actuators with a singular (ABS or combined ABS/TCS) controller.

As discrete control wiring gives way to networked devices, the same functionality may be implemented, but in a very different way. Sensors can now share information with, and actuators can take their instruction from, any device on the network. In such an environment, logic implemented on two different controllers -- one for ABS and one for TCS -- could be used, each relying upon the same networked wheel sensors to make decisions and then calling for action, when required, by the networked brake actuators.[3]

More advanced functionality is enabled by expanding the available (network of) sensors:

- A multi-axis inertial sensor (gyroscopic) sensor (there is probably one in your mobile phone these days) can report pitch, roll and yaw accelerations and angles. Although not typically a problem for Class 1 and 2 passenger vehicles and light trucks -- which have lower centers of gravity and less dynamic loadings than heavy freight vehicles -- this collection of sensors and brake actuators is enough to introduce an electronics control unit to implement roll over stability control (RSC) in any size of vehicle (or even a semi-trailer independent of, or in cooperation with, the tractor pulling it).

- With the addition of a sensor reporting steering angle, there is sufficient sensor data available to *determine and compare* both the *intended* and the *actual* directions of travel. A divergence typically occurs as a skid (understeer or oversteer) when a driver attempts a maneuver (perhaps due to accident avoidance or failure to judge the road trajectory) which exceeds the available traction (perhaps due to adverse road conditions such as rain, ice, snow, hydroplaning).

  In vehicle dynamics, when a vehicle is making a turn (or attempting to holding a lane on a curving road), it is said to understeer when the front (steering) wheels have insufficient traction to hold the *intended* (or commanded) direction of travel.

  In the case of oversteer, the rear wheels break traction and begin to slide and again the vehicle cannot hold its intended direction. Enter a corner driving a car, understeer and you run wide (but yaw stable, or "plowing out"); oversteer and you take the corner too sharply (yaw unstable, even "spinning out" or "jackknifing" if towing a trailer).

With a basic Electronic Stability Control (ESC) system, the ESC ECU can detect these events and actuate brakes to attempt to restore traction and directional control to the driver.

[3] Some technical data sheets suggest that many ECUs may have a more direct relationship with their most important sensor data.

The networked ECUs collaborate in a virtuous cycle. As we increase the number of sensors (providing operational and environmental data) and actuators (interacting with the physical systems of the vehicle) on the vehicle, additional under the hood safety systems become technically easier to implement and more economic (less expensive) to deploy. As a consequence, (safety) functionalities become even more sophisticated. We see how this works in more advanced ESC systems where additional actuators under independent ECU control are able to: dynamically adjust suspension variables (e.g. stiffness and rebound); control the differential distribution of drive power to the wheels (All Wheel Drive); and/ or reduce acceleration through throttle management (as necessary for cruise control).

3.2 Integration of ECUs Enhances Comfort and Safety

ECUs are so pervasive that it may not be obvious how they relate to basic automotive features. Inexpensive microcontrollers can (and do) automate simple controls, replacing elements of a driver routine. For example, when it starts to rain, the wipers are engaged. Employ a more sophisticated rain sensor and control program and the wiper speed will adjust to the intensity of the downpour. When night falls, or when you enter a tunnel, vehicle lights can be turned on. Again, a more sophisticated implementation would automatically dim high beams when faced with oncoming traffic.

As one evaluates their experience of a vehicle, it becomes clear that the more interconnected and computerized these systems, the greater the benefits in comfort and safety. Indeed, safety critical systems interact in subtle, and often non obvious ways, with the everyday comfort systems. Your radio knows how fast you are going. Your key fob, telematics system and even your phone can control your door locks, but the locking system also talks to the collision safety computers. And, with vehicle telematics, there is more communication happening than you can directly observe.

Networked Convenience; ECUs working together for your comfort

As you enter your vehicle, which you have remotely unlocked (Remote Keyless Entry), the cabin lights illuminate for an interval allowing you to prepare for your journey. The car will recognize your unique key, disable the immobilizer and automatically adjust the power seat to your preferred position. Press the 'start' button, and computers will quickly run diagnostics. "Prognostics" will communicate via the inbuilt telematics to the manufacturer that when the vehicle is next in for service, an engine sensor might need to be replaced. But you won't be bothered with such detail. You hear the engine start, and doors automatically lock (Central Locking System). You will be notified, often through a configurable display -- which is, of course, really a computer screen -- if any door is still ajar, and if there are any conditions of which you should be aware (the left rear tire pressure is low and you should top up on windshield fluid). And, if you haven't done so already, you will be increasingly encouraged (nagged) to fasten your seat belt.

The in-vehicle entertainment system (it is far from just a radio these days) may mute itself for a period as a reminder to heed these safety warnings, but it soon lets you know it has linked (via Bluetooth) to your phone. The destination you looked up earlier is transferred to your navigation system, and as the initial directions appear on the screen, the iTunes® tracks you downloaded the night before to your home computer, having synched with your phone, now begin to play over the stereo. And, once you are moving, and road noise becomes more intrusive, the volume will be subtly increased for your comfort and convenience so that you can focus on the road ahead ... until, again, being muted as you take an

incoming call -- hands free, of course -- answered from a button on your steering wheel or by tapping the touch screen on your center console. Your journey is over. At the office you realize that you may have forgotten to lock your car. No worries; a few taps on your phone and the doors are secured.

Networked Safety; ECUs working together for your safety

As the journey is about to begin, sensors detect occupants and encourage them to engage their seat belts; if the occupant is above a certain weight, supplementary restraints (air bag) systems are enabled and the doors automatically locked. Sensor data on acceleration/deceleration is continuously monitored to determine if an impact event (accident) has occurred. Should the worst occur, the pre-collision system ECUs will also analyze the force, location and direction of the impact. Seat belts are automatically tensioned, bringing occupants tighter into their seats. If the event is deemed to have a high probability of injury to the occupants, the air bags are deployed. Newer air bag systems may deploy the air bags in stages in response to the specifics of the impact. The engine is stopped, fuel cut and doors automatically unlocked as your car notifies a control center via the integrated telematics system that there has been an impact (accident) at your (GPS determined) location and the operator attempts to contact you and determine if further assistance (accident recovery or emergency services) is required.

3.3 Automated Driver Assistance Systems (ADAS)

Just as actuator control of *braking* lead to ABS, TCS, RSC and ESC systems, implementation of actuator control of the *drivetrain* and, as is increasingly common, even *steering* is enabling the development of additional Advanced Driver Assistance Systems (ADAS). It is useful to consider some examples:

ADAS made possible by adding actuated drivetrains:

- Highway speed management via conventional cruise control (CCC) only requires knowledge of vehicle speed and actuator control over the accelerator component of the drivetrain. In Adaptive Cruise Control (ACC) systems, the addition of (radar or lidar) sensor data about the distance to objects ahead allows the ACC computer to 'see ahead' and adjust speed to maintain following distance.

- This ability to see ahead also allow computers to scan for possible collisions (e.g. rear ending another car or an imminent head on impact) and implement Automatic (or Autonomous) Emergency Braking (AEB) systems which can engage the vehicle brakes gradually or suddenly brake according to the calculated scenario. AEB systems have also evolved to include optimizing for lower speeds in urban environments to help avoid (or mitigate the impact of) collisions with pedestrians.

ADAS made possible by addition of actuated steering:

- Sensors mounted on a vehicle can provide the data necessary for a vehicle's computer to determine if a car *could* be parked in a given space; however, this does not mean that every

driver is *capable* of parking -- or desires the additional stress of trying to park -- in tight places.[4] Early systems helped guide a driver into a space. However, once a vehicle has actuator control of braking, drivetrain[5] and steering, the computer can park the car itself; this feature is known by many branded names, but we will generically refer to it as Automated Parking Assistance (APA).

- A Lane Departure Warning (LDW) system that monitors lane markings to alert a driver when they appear to unintentionally drift out of their lane (as opposed to commanding a lane change). When actuated steering is available, the computer can gently adjust steering angles to hold the vehicle position, even as the road curves ahead, a feature known as Lane Keeping Assist (LKA).

Vehicle Automation | Automated Driving

Once actuators have the ability to physically operate all of a vehicle's core control systems -- steering, braking and the drivetrain -- that vehicle begins to transcend in functionality from a collection of systems *assisting the driver* to a level of automation where a vehicle can actually drive itself in a number of conditions; the driver's role becomes monitoring the car as it drives itself.

For example, several manufacturers have refined and expanded the expertise gained in implementing ADAS vehicle control technologies (Adaptive Cruise Control, Lane Keep Assist, Autonomous Emergency Braking and Automated Parking Assist) and an ever increasing array of ultrasonic, radar and camera systems to automate driving in traffic. For example, these systems -- which (Daimler) Mercedes brands as "Stop & Go Pilot" and BMW brands as "Traffic Jam Assist" -- can match vehicle speeds, slow in traffic, even to a stop and resume moving, all the time steering as necessary to follow the road.

When Heavy Commercial Vehicles Aren't Leading the Way, They Are Rarely Far Behind

It would be a mistake to assume that these ADAS technologies are just in luxury consumer vehicles. Indeed, the adoption of safety technologies in heavy commercial vehicles has often been ahead of that in light vehicles.

- Daimler now offers a version of their "Stop & Go" technology in trucks, even using common branding of the feature in trucks as in their luxury sedans. Again, this advanced ADAS technology evolves from offerings such as LDW, which Daimler has offered in Freightliner trucks since 2002.

- The requirement for ABS in new class 3 and above trucks (and trailers) was phased in by the NHTSA between 1997 and 2001 (FMVSS 105). Europe preceded the US in requiring ABS for heavy trucks [6] and has required ABS for new passenger cars since 2007. Although ABS was

[4] Many states do not assess parallel parking skills as part of driver licensing. Hence, new drivers might not have been taught the skill. Regardless, in an urban environment, parallel parking is a necessary (and not just desirable) skill. A skill that ADAS technologies may eventually make redundant.

[5] In this case including not just throttle, but also gear selection for forward and reverse.

[6] At least for Class 8; information on lighter classes has not been researched.

already a rather common safety feature in US passenger vehicles, NHTSA did not require ABS for new cars until MY 2012.[7]

- The *NTSB* has *recommended* ESC on heavy trucks since 2011; And, the *NHTSA* recently announced that ESC will be required on Class 7 & 8 trucks manufactured after August 1, 2017 (FMVSS 136). The requirement for ESC in light vehicles did not take effect until MY 2012 (FMVSS 135).

- From November, 2015, LDW and AEB will be required in new trucks sold in the European Union.

No driver spends more time inside their vehicles than commercial drivers; and, the impact and cost of accidents is significantly greater, per incident, with heavy commercial vehicles. Hence, comfort, performance, safety and convenience in trucking has developed in parallel with light vehicles.

3.4 Intelligent Transportation Systems (ITS), V2V and V2I Networking

Looking beyond the current advanced computer controlled safety and convenience features for heavy vehicles we find an area of research and development called Intelligent Transportation Systems. Imagining Intelligent Transportation Systems (ITS) have been the work of futurists, think tanks and visionaries for decades. This area of study includes things such as Connected Vehicles, Intelligent Highways, and Intelligent Transportation Systems with Technology Transforming Transportation which aim to achieve zero fatalities and zero delays. This is the stuff of science fiction movies like "I, Robot" in which computers control and move cars in an efficient and safe manner. This level of technology requires vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) communication.

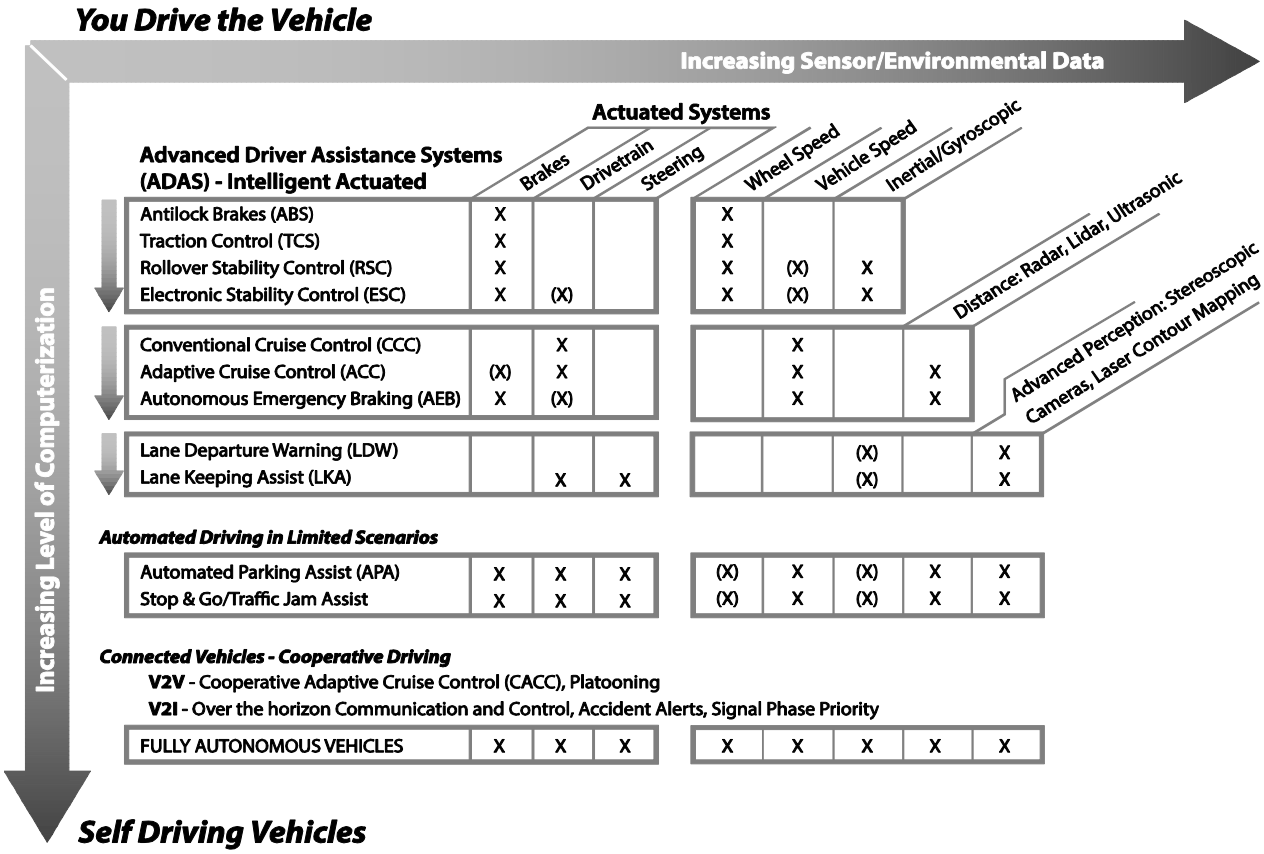
Examples of Vehicle to Vehicle (V2V) communication systems include Forward Collision Warning (FCW), Lane Change Warning (LCW), and Curve Speed Warning (CSW). These are extensions of existing features already in the automobile market such as automatic emergency braking and adaptive cruise control. In this instance, two or more vehicles “communicate”, i.e. send messages to each other to warn of sudden braking, lane changes, and excessive speeds going into curves. The vehicles receiving these messages could take corrective action by alerting the driver, engaging brakes, making steering corrections, and other actions to avoid an accident. This type of technology is required for heavy vehicle platooning in which a lead vehicle could control one more additional vehicles in a caravan type formation.

Vehicle to Infrastructure (V2I) communication systems include concepts such as red light warning (ELR) curve speed warnings (CSW), and Stop Sign Gap Assist (SSGA), Railroad Crossing Violation Warning (RCVW), Spot Weather Impact Warning, Oversize Vehicle Warning, Reduce Speed/Work Zone Warning, Signal Phase and Timing (SPaT) priority movement for emergency vehicles. In these scenarios the vehicles interact with their environment such as bridges, tunnels, stop lights, construction zones, etc. using short range communication messages. In some instances the exchange would be limited to information messages for drivers but in others advanced computer controlled proactive actions are contemplated to adjust speed, direction of travel, etc.

[7] Since ABS is necessary in an ESC system, ABS became a mandatory safety system for light vehicles when ESC was mandated. ABS was never required in previous standards.

While some of the interaction can be done in passive fashion using inductive loops, video algorithms, and license plate readers, much of this type of interconnectivity would necessitate a wireless connection between the vehicle and other vehicles and infrastructure around it. The SAE J2735 standard for messages over IEEE 1609/ IEEE 802.11p Wireless Access in Vehicular Environments (WAVE) has been developed to enable Dedicated Short Range Communication (DSRC) in the ITS program. DSRC is designed for high speed communications between with vehicles for V2V or V2I; this "short" range technology has an effective range up to 1,000 meters. The U.S. Department of Transportation is actively researching and developing DSRC for “active safety” initiatives which involve V2V and V2I.

3.5 Summary



Computer and communication advancements continue to fuel the feature evolution within both passenger vehicles and heavy vehicles. Small ECUs can now have inexpensive, independent processing capabilities rivaling that of many standalone PCs of only a few years ago complete, with full operating systems. The continued innovation and development of inexpensive communication technologies such as cellular, RFID, Bluetooth, and others continue to push the boundaries of what and how even the smallest components can be connected. This is resulting in more and more safety-critical actions being put under computer control in the quest for efficiency and highway safety. The most disconcerting part of our feature survey was the almost total lack of discussion regarding cyber security for these advanced systems.

[PAGE INTENTIONALLY LEFT BLANK]

4 The Bad: Engine Computer and Network Vulnerability Overview

4.1 Local Networks for Controllers and the ISO CAN Bus

Automotive ECU networks are much like any Industrial Distributed Control Systems (DCS). Historically, Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems have assumed that they operate in a non-hostile environment and security concerns have been secondary to functionality during development and implementation. With knowledge of the Programmable Logic Controllers (PLC), sensors and actuators on the controller area network, an engineer is able to achieve logical control of physical processes as expansive as a refinery, pipeline, power grid or nuclear plant -- or, the functionality of an automobile or truck.

The "controller area network" can be thought of as a *generic* term for a simple network architecture which enables sensors, actuators, microcontrollers, ECUs and PLCs to communicate in harsh environments without an intermediating host computer. However, Controller Area Network (CAN) is also a collection of formally defined standards and the most commonly used standard for vehicle, ICS and SCADA networks.

CAN [8] was originally developed by Bosch in the early 1980s and was gradually adopted by many automobile manufacturers as a low cost, robust solution for interconnecting the components of their increasingly computerized vehicles. The second major revision of CAN was released in 1991, specifying in version 2.0A 11-bit device identifiers and CAN2.0B 29-bit identifiers. Light vehicle manufacturers generally used the 11-bit CAN 2.0A . Heavier vehicles would layer specify enhanced functionality layered on top of 29-bit CAN2.0B in SAE J1939 networks.

CAN was further codified in 1992 as ISO 11898 "Road Vehicles -- Controller Area Network". Although other low level network designs remained in use , the CARB and EPA mandate for OBD-II was refined in 2005 to specify that MY 2008 cars must use the CAN (ISO 11898) Bus standard. In addition, light vehicle manufacturers have to enable a pass-thru protocol (SAE J2534 to allow each ECU in the vehicle to be interrogated through the OBD-II (SAE J1962) diagnostic port. The equivalent standard in heavy vehicles used to interrogate ECUs over the J1939 CAN network is RP1210.

Although the listing of standards may be arduous to review, the comparatively simple reality is that both car (OBD-II/SAE J1962) and heavy vehicle (SAE J1939) networks (1) move the control messages between ECUs on a CAN network, and (2) the ECUs can be accessed and reprogrammed over that CAN network.

4.2 The ISO CAN Bus is logically similar to Ethernet

In the context of personal computing in the internet age, most people appreciate that using the Internet begins with connecting to a network, usually an Ethernet (or a WiFi bridge to an Ethernet). Plug in and you get a physical (MAC) address. At this point, you are attached "on" the network and it is possible to have very low level device to device network adapter communications. An Internet Protocol (IP) address will be necessary to logically communicate with other devices. Once your computer has its IP address, the Transmission Control Protocol (TCP) will manage communications between devices as you

[8] Note: For the purposes of this paper from here onward, unless otherwise indicated, **CAN** only refers to the defined vehicle standards and not controller area networks in the generic sense.

seek to engage services through network ports and higher level protocols such as HTTP, communicating through port 80, for presentation to your browser application.

Any networked exchange of information between devices, such as that sketched above, may be described using the ISO Open Systems Interconnection (OSI) model. The OSI is a conceptual framework that describes seven layers for interconnecting systems in which data can be imagined as moving between layers. These layers are the (7) Application, (6) Presentation, (5) Session, (4) Transport, (3) Network, (2) Data link and (1) Physical layers.[9] Each layer is responsible for communication with the layer above and below it (if any) and has no knowledge of the specifics of these other layers.

Ethernet is defined at *physical* and *data link* layers of the OSI model. Bosch originally designed CAN as a *data link* layer specification, independent of physical media. However, as standardized for the use in automotive electronics in ISO 11898, the CAN bus is -- like Ethernet -- defined at *physical* and *data link* layers of the OSI model.[10]

Ethernet does not define any encryption for data which is instead implemented (if at all) higher in the OSI protocol stacks. However, Wi-Fi, in a de-facto recognition of the insecure nature of wireless communications, is typically deployed with *data link* layer encryption. CAN, unfortunately, is not. And, this is important.

4.3 The Vehicle CAN Bus; design and vulnerabilities

The basic CAN packet consists of an 11-bit message identifier (ID) with an eight byte data segment. It is assembled and transmitted onto a low voltage, wired network with devices in a bus topology. Each manufacturer determines the values and meanings of these messages; the only security in the messages is solely due to their obscurity. The message IDs are proprietary to each manufacturer and generally non-public information. The vehicle CAN network assumes that devices on the network are well behaved and without malicious intent. And, in what is a physically hostile environment of temperature extremes, water ingress, and electrical interference, CAN has performed well. The linear (bus) topology has greatly simplified the wiring loom. All said, CAN is inexpensive, robust and works as designed. However, we need to appreciate how this design works in practice if we are to understand the potential vulnerabilities of a CAN network.

[9] When modeling an environment involves interaction with a user (Human Machine Interface) or other system, the user is sometimes referred to as Layer 8, although this is not part of the OSI model.

[10] The *physical* layer defines how the smallest units of data (bits) are physically transmitted. This includes the physical medium, for example, unshielded twisted pair copper wiring, fiber optic cable or specific radio frequencies. This includes defining pins, voltages, signal timing, physical flow control, network topology and the form of network adapters, hubs and repeaters that allows data to stream between two nodes. The *data link* layer defines how data manages in assembled frames, basic flow controls, error checking and payloads.

On the vehicle CAN network:

- *Any device can listen and any device can talk:* CAN packets are broadcast on to the network and available to all nodes; each node decides which packet(s) it finds relevant and often uses the message ID to determine relevance. The publish and all subscribe messaging is beneficial when several ECUs need to know sensor or state data, for instance, vehicle speed. ECUs for the vehicle display can indicate the speed at which the vehicle is travelling while the ECUs controlling the airbags can determine if the minimum velocity has been achieved for deployment in event of an accident.

- *Any device can assert priority:* when networked devices attempt to broadcast at the same time it is said that there is a collision. CAN manages collision detection and arbitration in such a manner that the message with the highest priority is given precedence. The lower the 11-bit message identifier (ID), the greater the priority.

- *Devices communicate without the overhead of encryption or authentication*. Messages are transmitted in the clear and any device is assumed to be from an authorized source.

These characteristics of vehicle CAN networks are a vulnerability:

- Any device on the CAN bus can log *ALL* of the data transmitted on that bus for later analysis and reverse engineering. The data is in the clear and only protected by the obscurity which is, in reality, no protection at all.

- Further enabled by the absence of session encryption, CAN packets can be maliciously injected onto the network, replayed, fuzzed or formed for specific, including man-in-the-middle, attacks.

- Because there is no authentication model, any CAN packet so inserted will be accepted (at face value) as a valid and authorized network message and the sensors, actuators and ECUs on the network will attempt to process them.

- Furthermore, a CAN network can be subjected to a denial of service attack by flooding the network with packets of an arbitrarily high priority (i.e. low message ID) causing other devices to halt transmitting and/ or become overloaded processing arbitrary messages.

- There is no such thing as a read -- or write -- only device; CAN is a multi-master bus.

[PAGE INTENTIONALLY LEFT BLANK]

5 The Ugly: Potential Threats and Exploits

One of the seminal papers we reviewed on the security weaknesses and potential attacks against the CAN and ECU architecture was *Experimental Security Analysis of a Modern Automobile* [A01]. This paper reviewed the results of direct experimental research on two MY 2009 passenger automobiles. There has been additional work and papers by Dr. Charlie Miller and Chris Valasek including *Adventures in Automotive Networks and Control Units* [A03] in which they compromise a 2010 Ford Escape and 2010 Toyota Prius. A second paper by Miller and Valasek, *A Survey of Remote Automotive Attack Surfaces* [A04], published in 2014 for the Blackhat 2014 security conference goes into more detail regarding potential local and remote attack surfaces. It is from these papers which we are able to survey and summarize a great deal of knowledge regarding the potential threats against the CAN, ECU, Sensor, and actuator architecture discussed in previous sections.

The inter ECU CAN communication design is a publish and subscribe model which means that ECUs broadcast messages and then every other ECU on the bus decides what messages it will interpret and act on. This means that there is no control over who listens or sends messages. And, an ECU may relay (bridge) messages to another CAN bus. There is usually a high speed CAN bus for critical drive train operations and a lower speed CAN bus for less time sensitive operations. While one would think that items on the low speed non-critical bus would not be able to access the traffic and ECUs on the high speed critical bus, research has concluded that is not the case. For the sake of simplicity, we shall take a more generalized overview of the network.

A CAN message ID header type identifies the type of message being sent, i.e. speed, brake operation, or any other type of information monitored by sensors or actions taken that need to be coordinated by multiple ECUs. The CAN IDs are usually proprietary to each manufacturer and the information is usually not published as a form of security. That being said, the researchers mentioned above 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. This overall design and function leads to a number of vulnerabilities:

Denial of Service Attack

By flooding the network with a large number of nonsense message traffic it is possible to overwhelm the network completely and stop components from being able to communicate. This type of attack can lead a vehicle to behave unpredictably and could keep a vehicle from functioning all together.

Man in the Middle Attack

Since any ECU can listen and send any message it is possible to reprogram an ECU to listen to a specific message regarding something of interest, say vehicle speed, and then send out a large number of fake messages to drown out the original sender and have ECUs act to the fake message instead. This is possible because components do not check the sender identity.

Diagnostic Packets

While diagnostic functions are good for helping a mechanic and/or car designer test and find problems with vehicles, they can also be accessed for less benign purposes. The diagnostic packets are usually intended to be sent in controlled environments when the vehicle is not in motion (Key On Engine Off, KOEO tests) and can do things to the vehicle which should not be done when operating at speed (such as manipulating braking control). Unfortunately, access to diagnostic functions is possible in some vehicles even while the vehicle is in motion. Depending on the purpose of a hack, there might just be a nice diagnostics function that can be used in way other than originally intended.

ECUs Firmware

If an attacker has physical access to a sample vehicle, it is possible that they can download the firmware through debug access built into the system components. For example, in the *Adventures in Automotive Networks and Control Units* [A03] paper mentioned above, the authors were able to connect to the Parking Assist Module (PAM) ECU using built-in debug connections, freely available software and low cost tools. This gave the authors the ability to download and review the assembly level code which was contained on the ECU. This gave them a great deal of information about the message structures and other intelligence about the CAN network. This can also allow the attacker to "modify" the code and then upload it again to the ECU.

Reprogramming ECUs

In order to allow for software updates and service corrections it is possible to reprogram (also known as flashing or reflashing) or update the code on an ECU once it is in the vehicle. This is "in theory" a protected operation requiring a key exchange, however, most of the seed keys are easily cracked and for many automobiles, they are often already known and published in the car tuning community. This operation is supposed to be prohibited when the car is in motion. Practical testing, however, has shown many manufacturers have not implemented this properly or at all and the researchers above have been able to reflash ECUs while the car was traveling at over 40 mph. Once an ECU can be reflashed, it can essentially be taken over and loaded with any malicious code the attacker may want to run on the CAN network. It is very similar to a hacker taking over a server on your company network. Once the hacker has a nice foot hold on your network to work from, almost anything is possible.

Fuzzing/Packet Injection

Fuzzing is a technique where by a system is sent a sequence of carefully crafted messages to determine how the system behaves. This allows the sender to figure out how a system works without knowing the internals of the system. This can sometimes lead the sender to find ways to make the system do things that it may not have been designed to do by sending message parameters outside of what the original developer was expecting. The researchers above were able to use fuzzing to identify messages for the brakes, engine, lights, door locks, radio, etc. functions and how to structure packets to control these functions. More worrisome part was that they were able to find messages which generated rather unexpected catastrophic results. In one case they found a message to engage a left brake to the point it was resistant to manual

over ride including power cycling and removing the battery until another message was sent to reverse the lockout. They also found a message sequence which would disable the brakes completely and keep them from being engaged while the car was running at 40 mph. Once these messages are determined they can be injected into any similar vehicle to achieve the same results.

Multi-Component Attacks

The previous methods can be combined and/or multiple ECUs can be targeted at the same time to create specific scenarios. Several practical examples have been proven such as controlling the speedometer to show bogus messages or turn it into a clock, turn off all lights (headlights, cabin lights, etc.) while the car was traveling at 40 mph. A simple "self-destruct" was designed for the MY 2009 vehicle in *Experimental Security Analysis of a Modern Automobile* [A01]. The self-destruct 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 be opened manually) thereby trapping the passenger in the vehicle as the engine was then killed. The attack required less than 200 lines of code. Considering that the average high end automobile contains over 100 million lines of code that is a needle in a stack of needles.

While this attack information and examples are concerned with automobiles, we have established through our survey of literature, standards and discussions with leading experts that heavy vehicles have the same vulnerabilities and face the same threats.

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 "spoof" a couple of sensors with bad time data to push a heavy vehicle diesel engine into a DEF limp Home mode. If the OBD for the engine detect an emissions fault, such as no Diesel Exhaust Fluid or a missed service interval, a regulatory requirement forces the engine into a *limp home mode* after a pre-determined interval to force the operator to have the faults fixed. Spoof data on an empty DEF reservoir, and the vehicle will limp within a few hundred miles. Spoof other critical engine sensors and the engine may seek to shut down to protect against catastrophic failure. Such attacks, would have significant economic consequences, especially if it impacted more than one vehicle simultaneously.

A lane keeping system might only need a few bad sensor messages to cause it to take inappropriate action. And, with a heavy vehicle even a small unanticipated change in steering can have catastrophic consequences. Consider the ability by the researchers to lock up a single wheel brake of a car, at speed, applied against a fully loaded heavy vehicle and trailer. A passenger car could possibly recover. It would be far more difficult to recover and control a heavy vehicle due to the physics of such a large and heavy object in motion.

While certainly very bad, these attack scenarios would require physical access to the heavy vehicle; so the risk is very low, right? Well, no. Recall in the previous sections on how we commented on the fact that the radio/entertainment unit was integrated into the CAN network and that most heavy vehicles have a host of other equipment that is connected to the CAN network and the outside world. Okay, well now we have a really big problem because all of this can expose the CAN network remotely. This means that all the attacks that we have talked about in this section could be done remotely, including ECU reflashing, if the attacker can find a way into the vehicle network from afar.

[PAGE INTENTIONALLY LEFT BLANK]

6 Attack Vectors

The most authoritative work on attack vectors we uncovered during our research was a paper titled *Comprehensive Experimental Analysis of Automotive Attack Surfaces* [A02]. This is an early authoritative work referenced by many subsequent researchers. While the paper focuses on passenger cars, we have already demonstrated that heavy vehicles are not significantly different and in some cases even more vulnerable. We have chosen to focus on attacks as they relate to ultimately getting access to the CAN network. Other potential attack vectors such as GPS denial of service, Trojan cargo, etc. are not being considered in this paper.

6.1 Direct Attack Vectors

There are several different avenues to mount a computer based attack against vehicle ECUs and CANs using direct access methods. These may seem trivial and are sometimes dismissed because with direct access to any equipment it is fairly easy to do harm, like cut brake lines and so on, but there are some systematic issues which do warrant exploration.

The first and most obvious is to connect to the vehicles on board diagnostic (OBD-II) port with a laptop or other computer. Another avenue would be a USB memory stick, iPod, or CD-ROM with malicious programs and attempt to attack the vehicle by connecting them through the entertainment system of a vehicle. As a matter of fact, Fiat Chrysler just recently had a major recall relating to a security flaw in the entertainment system in 1.4 million vehicles that allowed hackers to take complete control of a Jeep.[11] Perhaps the most disturbing part of this incident was that Fiat Chrysler did not notify regulators for 18 months. Fiat Chrysler did not consider it a safety defect.[12]

Another effective approach is to utilize the open design of the CAN network and place a rogue ECU directly onto the internal network. This would be the equivalent of installing a backdoor program on a computer which could provide covert and long term access to the vehicle. Given recent advances in Software Defined Radio (SDR)[13] on computer chips, i.e. cellular capabilities without a SIM card, a single ECU could contain a small operating system with remote communication/data capabilities. This would effectively escalate the access from local direct to remote access thereby significantly increasing the effectiveness and flexibility of the attacks already described.

A more complicated, but very effective, approach to compromise multiple vehicles directly is by attacking them in the supply chain. This can be done by inserting malicious code into ECUs or other components prior to delivery to the factory for inclusion in the assembly process. This would be a simple way to introduce systematic vulnerabilities into a large number of vehicles without having to physically manipulate each one. While this may seem a little farfetched, there have been documented instances of this type of attack in “the wild”. Most notably, there was a credit card reader that would -- unbeknownst

[11] See [A05] *Remote Exploitation of an Unaltered Passenger Vehicle* in the References Section of this paper for full details of this hack.

[12] Osborne, Charlie. *Regulators Left in the Dark over Chrysler Security Flaw for 18 Months.* (August 6, 2015) 'Zero Day' on zdnet.com. Retrieved on 19 August 2015 from: http://www.zdnet.com/article/regulators-left-in-dark-over-chrysler-security-flaw-for-18-months/.

[13] Software Defined Radio (SDR) is the system where all pre- broadcast and post receive signal processing such as tuning, (band pass) filtering, mixing, modulation and demodulation, amplification and attenuation are implemented in software instead of hardware.

to the user or credit card processor -- selectively dial out and report (gold card or better) credit card details to a phone number in Pakistan. When investigated, the trail led back to a malicious firmware program in a component being sent to the factory for the credit card reader manufacturer.[14] The vehicle manufacturing process is heavily dependent on 3rd party parts and providers for components from all around the world. A single truck manufacturer has thousands of equipment configuration options that are supported by a vast network of components. It would not be inconceivable or very difficult to attack a supply chain which is so diverse and distributed.[15]

6.2 Remote Attack Vectors

In addition to direct attacks, there are the more attractive remote attack surfaces. This is where access to the CAN network and systems can be done remotely over radio, cellular, or satellite communication networks.

Short Range

First, we have some short distance communication vectors. One short distance communication technology is Bluetooth, which is frequently connected directly to the vehicle to allow pairing of cell phones with the onboard hands free calling features. While the Bluetooth standard is pervasive, it has been known to have the occasional security flaw in implementation. Another is the remote keyless entry which uses encoded digital signals to unlock doors, start the vehicle, etc. which unfortunately are also susceptible to compromise. There was a presentation at Blackhat 2014 where a Software Defined Radio aficionado demonstrated how he was able to crack the remote entry system of his Toyota Prius. Criminal gangs in Europe are believed to load the sometimes sizable SDR equipment into vehicles and then target luxury vehicles. This same type of approach can also be effectively used against RFID technology used for vehicle immobilizers and the proximity “keys” used to start vehicles.

Tire pressure monitoring systems (TPMS) also work over radio frequencies. It has been shown that these frequencies can be identified and the sensor messages forged. Although, forging the TPMS packet may seem unremarkable, if the TPMS ECU itself is compromised, sensor data may be used to trigger a 'logic bomb' hidden in the altered TPMS ECU code that, in turn, launches an attack over the CAN on other systems. This helps illustrate how any device on the CAN network is potentially a malicious actor.

[14] See Reference [A12] *Significant Cyber Incidents Since 2006*, incident 29, October, 2008.

[15] Supply chain issues are most often seen when counterfeit parts enter the market. However, the last few years have seen significant concern over possible back-doors in Chinese technology sold to consumers and government in the US (cyber-espionage).

An interesting fact about today's entertainment systems is that they are directly integrated into the engine computer networks to provide sound and other audio/visual feedback to the driver and passenger. Previously we mentioned that you can attack a vehicle through the entertainment center using a specifically crafted USB memory stick or CD-ROM. Given the frequency with which radio is included, it is also feasible to send this same malicious CAN data via radio signal. Sound farfetched? In July 2015, the NCC Group, a company in Manchester, England reported that it found a way to carry out an attack using the European digital audio broadcasting (DAB) standard.[16] DAB/ DAB+ radios are now included in almost all new cars sold in Europe.[17] Even basic FM radio with RDS-TMC has been demonstrated as vulnerable to attack going back as far as 2007. [A48]

With new contemplated features such as vehicle to vehicle and vehicle to infrastructure interaction to support accident avoidance and platooning, a short range communication system must be employed to allow the vehicles and infrastructure to "talk". How is that communication going to be secured given the nature and diversity of heavy vehicles and infrastructure? How do you keep these signals from being spoofed and/or abused?

Medium Range and Global Access

As if there were not enough attack surfaces, car manufacturers have started to include built-in WiFi with connectivity using 3G and 4G cellular modems and local hotspots so that you can surf the internet while you are in the car. This introduces two different vulnerabilities. You can now access your car by attacking the local WiFi hot spot in your car which is a problem as WiFi is very difficult to secure and weak passwords can potentially be cracked by intercepting ongoing communication[18]. Another problem with this is that it gives your car (through the 3G or 4G cellular connection) it's very own public internet IP address, which can be found and interrogated by anyone on the internet. Given that these are provided and managed centrally by the manufacturer or 3rd party provider, it is probable that the address space would be grouped. This means attackers would be able to identify groups of vehicles, thereby exposing a systematic fleet vulnerability. Refer to [A05] for a practical example.

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.

---

16 SDR is now known to be able to deliver DAB/DAB+.

17 Eventually, DAB (and DAB+) will be the only radio option. Analogue FM transmissions are expected to cease within the EU and the newly freed bandwidth is to be reallocated. However, only Norway has announced actual plans for a switchover in January 2017. The UK has stepped back from a 2015 target and has no firm date, but is generally thought to be working towards 2022.

18 For a primer on cracking WiFi passwords please see: http://null-byte.wonderhowto.com/how-to/hack-wi-fi-cracking-wpa2-psk-passwords-using-aircrack-ng-0148366/

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.

NMFTA Survey Results

In early 2015, NMFTA conducted a survey among their carrier members to determine the type of remote communication systems installed in their vehicles, if any. While the sample size was somewhat limited, the study showed that a clear majority of carriers, over 90%, had remote communication systems in their vehicles. This included a mix of satellite, cellular, satellite and cellular, as well as cellular and GPS integration. At least 36% of the respondents reported that their systems integrate directly with the vehicle computer system and 43% stated that their systems did not. An interesting fact was that 21% did not know if their communication system integrated directly with their engine computer system or not. The survey also showed that there was a wide variety of 3rd party providers for fleet communication and management, not including the integrated telematics from the vehicle manufacturers. This survey demonstrates that the remote attack vector is even more likely for commercial heavy vehicles than personal automobiles and seems to be significantly aided by -- not only the prolific nature of the connectivity, but also by -- the variety of solutions and lack of understanding of the integration by the companies themselves.

7 Potential Threat Actors

An analysis of actual attacks based on Mandiant's 2015 and 2014 M-Trends reports [19] finds that the breakdown of threat actors has remained relatively the same in recent years, but that there has been an increase in attacks on the transportation industry. In 2013, 3% of attacks were directed at the transportation industry but in 2014 it rose to 5%. This is a significant increase; however, the majority of the attacks in 2014 are against traditional business & professional services (17%) and retail (14%).

The objectives of the attacks continue to increase. They now include:

- **Access and propagation** to further other goals such as spam and botnets (networks of compromised computers) from which other attacks can be launched
- **Data theft** either for economic or political advantage such as the OPM hack to get details of people with security clearance
- **Cybercrime** for direct financial gain such as stealing credit card, bogus wire transfer requests, fraudulent bank account transfers and payments, etc.
- **Hacktivism** for publicity, defamation, and furtherance of social and political objectives such as denial of service attacks against companies that are on the "wrong side" of an issue or dumping company data to embarrass companies and their customers
- **Destructive attacks** which are designed to cripple and destroy infrastructure such as the denial of service and infrastructure attacks against certain eastern European countries during the height of tensions with Russia

The perpetrator of an attack may be a single individual, small groups of individuals bonded together for a single cause, criminal gangs seeking profit or even well-funded nation states preparing for cyber warfare. Engine hacking is still new, fairly complex and requires a significant skill set as well as specialized and expensive resources. Due to the size and expense, a heavy vehicle to experiment on is usually out of reach of most individuals and small scale groups and operations.

Therefore, at the moment, the most challenging threats come from Advanced Persistent Threat (APT) actors, such as well funded cyber-criminal organizations and nation states. The line between these actors is often blurred. Criminal gangs are believed to rival some nation states in their skills and sophistication. These gangs may sell their best (zero-day)[20] exploits to nation states to utilize later; and, nation states may help sponsor deniable actions to mask their own role in attacks.

It is from these advanced groups that we see the most immediate problematic threats to the transportation industry. Since truck transportation is such a key and distributed element of national infrastructure, the ability to disrupt or control any significant aspect of it could be very profitable or desirable, especially for ransom or political and military purposes. It would not take much to disrupt the normal flow of goods and services. A few disabled tractor trailers at a port or on a bridge is sufficient to have a dramatic impact on traffic and the flow of goods. Indeed, a single vehicle accident is generally sufficient to disrupt urban commuters on roads operating (at or) near capacity during rush hours.

[19] References [A13] *M-Trends 2014: Beyond the Breach* and [A14] *M-Trends 2015: A View from the Front Lines.*

[20] "Zero Day" vulnerabilities are unknown by (or undisclosed to) the OEM and may be exploited with the OEM having "zero days" to patch the problem.

The ability to disable and hold hostage even a small percentage of heavy vehicles in a fleet or area would provide significant leverage over a company or country. If this ability is combined with the ability to target specific cargo -- such as fuel, explosives, hazardous waste, etc. -- it could very quickly lead to some truly large problems.

8 Threat Impact

In attempting to assess the impact of the risks that we discuss in this paper, we have consulted some prior research in this area. In 2006, the American Trucking Associations (ATA) released a white paper with a basic impact assessment called "When Trucks Stop, America Stops" [A16] which included case study examples of when the borders were clogged during 9/11 due to extra security. Additionally, the Swedish Association of Road Haulage Companies conducted a similar study called "A week without Truck Transport" [A17] in 2009. These studies are focused on the stoppage of all truck delivery services and represent the most extreme case. The conclusion of both studies were similar:

- The impact of a total outage would be felt in the first 24 hours. Industries and businesses that rely heavily on *just in time* delivery -- such as gas/service stations, hospitals, mail, and most modern manufacturing operations -- will start to run short on inventory.
- Within 3 days, food, gasoline, and other basic necessities will start to experience shortages. ATMs will run out of cash. Restaurants will be unable to serve food. Panic buying can be expected.
- Within the first week, basic sanitation services such as garbage collection will be impossible and most city water supplies -- which rely on a steady supply of chemicals to treat water -- will cease to function. Emergency services will be unable to operate effectively due to a lack of fuel and basic supplies. Most automotive traffic will cease due to lack of fuel. Grocery stores will be out of food.

As one might imagine, things get worse from there.

While this may seem somewhat alarmist, recent events such as Hurricane Katrina and Hurricane Sandy showed that the services infrastructure within most urban areas is very fragile. Most households and businesses are ill prepared for even small disruptions in the supply chain. Even a heavy snow storm can cause serious problems in most urban areas. As the case study from ATA showed, during 9/11, those automotive factories that depended on daily deliveries were moved to reduce capacity within 12 to 36 hours of what was just a slow down at (not a shutdown of) the border with Canada. The Center for Automotive Research estimated that the cost was about $60,000 per hour for the assembly plants.

While the scenarios above represent the extreme end of the spectrum, even very minor events can cause serious problems.

- If a malicious cell transponder is placed at a key location such as a port, bridge, or tunnel which was capable of disabling just a few trucks, it could have a significant and far reaching impact.
- If a disgruntled employee was able to use the built in company truck monitoring and control systems to disable (or lockout) even a small portion of the trucks for a single company, the impact to the company itself in terms of lost productivity, revenue, and cost of recovery could be enough to put the company out of business.
- If a malicious actor was able to identify hazardous cargo and take control of just that one vehicle, there could be a major human and environmental disaster.

We have seen that exploits in each of these scenarios have already been demonstrated by security researchers. And, we have seen that these attacks are well within the technical expertise of today's hackers. Malicious groups such as nation states can potentially buy trucks and perform testing in order to prepare for an attack with a low risk of discovery and relative anonymity.

In summary, based on our review of available literature and studies and our understanding of the national infrastructure, there is the potential for significant impacts from even small localized events, not to mention large scale attacks and like scenarios.

It is therefore advisable that we consider the security of heavy vehicle transportation *seriously* and *urgently*. With computer security it is not really a question of "if" as much as it is of "when".

9 Current Security Measures

One might think it reasonably safe to assume that since the media first began reporting in 2010 and 2011 about the vulnerabilities in modern automobiles that there would have been a noticeable, if not significant, hardening of subsequent model years for vehicle cyber security. However, you would be wrong.

- "Security through obscurity" continues to fail. Vehicle networks remain unchanged and unprotected from the vulnerabilities previously reported. Each year, the total cost of reverse engineering vehicle network traffic declines as new hacking tools are developed and prior knowledge is codified and disseminated. Vehicle hacking sessions are a guaranteed draw at cyber security conferences such as Black Hat. *Knowledge wants to be free.*

- "Access denial" through *physical* security has never been a credible deterrent. Locked car doors have never been able to defeat a determined attacker (even for those who wish their intrusion to remain undetected). Regardless, the vehicle network is still accessible without ever having to enter a vehicle. Nor is it possible to 'air gap' the vehicle.

  Manufacturers continue to broaden the available attack surface. Infotainment systems are growing more powerful and better integrated into vehicle functions. With the computing power of a modern laptop -- (and sometimes the operating system of an old one) -- they are bridging internal networks to make this happen. And, these infotainment and manufacturer integrated telematics units are wirelessly connected to the outside world.

  Importantly, the most modern truck and truck tractor engines can be increasingly thought of as having their own IP address. And, as we have seen in the case of some "insurance dongles", consumers and fleets readily plug in devices to their car networks that include wireless communications.

- "Standard Access Controls" remain weak, and, will remain so, as long as the current standards that they legally must implement remain in force. Hence, for access to "protected" ECU functions, the challenge (seed) response (key) space remains at 16 bits and implementation algorithms well known[21]. Research has found that even the few security measures provided for in the standards, have been not been properly implemented by manufacturers. Unfortunately, even when they were, researchers have still been able to access the protected functions of ECUs.

[21] Re-Flashing an ECU is supposed to be a protected function.

Furthermore, manufacturers have -- by their own admission -- been slow to acknowledge cyber security issues as a problem. Nevertheless, it is possible, although we believe highly improbable, that there have been efforts that have made it into production vehicles to harden ECU software from attack. For instance:

- if a manufacturer has a team of "white hat" hackers doing penetration testing of their vehicle models;

- if ECU developers were moving to memory-safe programming languages, formal verification techniques, and "white box" testing to include hacker techniques such as fuzzing inputs; or,

- if OEM "black box" test sets are being extended to verify component and subsystem resistance to firmware hacking and successfully failing into "safe modes" under network-born attacks ...

these efforts would not be discernible to vehicle owners or operators.

However, our review of academic literature on vehicle (cyber) security shows that research remains focused on what *should* or *could* be done in the near 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.

10 Ongoing Hacking Activities

In our research, we have taken a look at some of the "hacks in the wild" reported in the media to see what these attacks can tell us about the scope and nature of actual ongoing hacking activities. This provides us with a sense of how immediate these threats are to heavy vehicles. We have found that actual attacks have been varied and range from the mundane to the stuff of spy novels. Detailed references and information for the hacks can be found in reference sets [A24] through [A47].

Hastings Attack

Some people believe that a 2013 vehicle hack was used to assassinate Michael Hastings, an independent journalist most commonly known for contributing to the downfall and resignation of US General Stanley McChrystal. Hastings was killed in a single car auto accident when his 2013 C-class Mercedes went completely out of control. Based on the available video footage, the vehicle seemed to accelerate through the streets of Los Angles completely out of control. At the time of his death, Hastings was very concerned that someone was targeting him and possibly his vehicle. A cyber security expert and former US National Security Council Special Advisor, Richard Clarke, determined that the accident was consistent with a cyberattack. Clarke stated in an interview with the Huffington Post there is "reason to believe that intelligence agencies for major powers" have the ability to remotely attack and seize control vehicles.[22]

Ramos-Lopez Attack

This 2009 attack was against a subprime auto sales group that installed remote disabling equipment on their vehicles; if a customer did not make the necessary payments, the car would be disabled. In this particular case, a disgruntled former employee, whose access permissions had been terminated, was able to use the credentials of a co-worker to access the company systems and disable around 100 cars[23]. This attack was made possible by bad password management and a lack of two-factor authentication.

Insurance Company Dongles

There have been two interesting instances of problems with the insurance dongles that have been attached to the ODB-II port in cars. Many people have seen the advertisements for the Progressive "snapshot" dongle. It is used to track driver patterns and activity and exchange data via a cellular network allowing the insurance company to fine tune their insurance rate. In 2015, it was revealed that the Progressive dongle had a major security flaw; their device accepted communication from any source, without any real authentication and communicated without encryption[24].

---

[22] [A24] Hogan, Mike. *Was Michael Hastings' Car Hacked? Richard Clarke Says IT's Possible.* Huffington Post. Retrieved on 2 September from http://www.huffingtonpost.com/2013/06/24/michael-hastings-car-hacked_n_3492339.html.

[23] Please see references [A26] and [A27]

[24] [A29] Fox-Brewster, Thomas. *Hacker Says Attacks On 'Insecure' Progressive Insurance Dongle in 2 Million US Cars Could Spawn Road Carnage.* Forbes.Com (January 15, 2015). Retrieved on 19 August 2015 from: http://www.forbes.com/sites/thomasbrewster/2015/01/15/researcher-says-progressive-insurance-dongle-totally-insecure/

A different dongle device tested on a Corvette[25] allowed the hacker to send the cellular modem an SMS message, which was translated to a CAN message that disabled the brakes on the car. This is because, as we have already discussed, the ODB-II port with which the device is integrated sits right on the CAN network. Additionally, researchers were able to use an internet search engine to find additional devices with this particular operating system/manufacturer signature and were able to locate these dongles on the internet. Their trolling for potentially vulnerable targets identified an entire commercial vehicle fleet in Spain.

OEM Telematics

There have been two high profile demonstrated hacks against manufacturer integrated telematics systems including GM, BMW, and others. An overview of some of these can be found in [A31] through [A37]. This has included a DARPA sponsored research project where they were able to compromise and take control of a Chevrolet by coming in via the built-in OnStar system. Miller & Valasek recently demonstrated a weakness in the built-in Uconnect® system affecting a broad range of Fiat Chrysler vehicles which also allowed them to take control of the vehicle[26].

Stuxnet

While not a vehicle hack *per se*, the Stuxnet attack against Iran uranium enrichment centrifuges which was discovered in June 2010 has some interesting applications for a vehicle fleet attack. First of all, it is an example of a very sophisticated state sponsored attack against CAN based infrastructure. CAN networks are not only being used in vehicles, they have a large number of other industrial applications as well. In the case of the Stuxnet attack, the computer communicating with the controllers on the CAN network for the Iranian centrifuges were compromised through a man in the middle attack. This was done by inserting a new software layer between the software that everyone thought was controlling the centrifuges and those libraries actually controlling the equipment. On one side, it instructed the controllers on the network to do things differently than original designed, causing mechanical failures in the centrifuges. On the other side, it reported false readings and settings to the controlling software on the computer making everything appear to be operating normally until well after the centrifuges were irreparably damaged. This type of attack, conducted against an OEM or 3rd party telematics provider could remain hidden for a long period of time and be used to attack a large number of vehicles simultaneously without having to worry about "infecting" every CAN network individually. Please see references [A38] and [A39] for additional analysis regarding the Stuxnet attack.

[25] [A30] Greenberg, Andy. *Hackers Cut a Corvette's Brakes Via a Common Car Gadget.* Wired.Com/ Wired Magazine. Condé Nast. (Published August 11, 2015). Retrieved on 19 August 2015 from: http://www.wired.com/2015/08/hackers-cut-corvettes-brakes-via-common-car-gadget/

[26] Please see [A05] and [A31] through [37] and [LR05]

Globalstar

"Hackers Could Heist Semis by Exploiting This Satellite Flaw,"[27] reads one sensationalized headline reporting the Globalstar hack. However, this was actually not the case. Globalstar is a service/product provider which enables their customers to track high value or important cargo -- such as diamonds, munitions, cash, toxic waste, etc. -- via satellite. When digging into the story it, turns out that the vulnerability did not give anyone access to cargo. However, there was a weakness that, if exploited, could let unauthorized 3rd parties use the tracking functionality to locate the cargo. This involved hackers setting up their own satellite antenna to search for certain kinds of traffic, on certain communication bands. While not enabling someone to take control of a heavy vehicle, the ability to pinpoint valuable cargo is an important intelligence component for some of the threat actors and scenarios discussed in this document.

Ordinary Car Theft

While not as sensational as some of the other stories, there is a new, pervasive problem with automotive thefts. Insurance companies have been baffled by a large number of automobile thefts (the recent examples we found were in London and California) where the perpetrator walks right up to a very expensive high end car, gets in, and then simply drives away. This is apparently being done by thieves and gangs cracking the encryption and security for the key fobs used by the manufacturer to unlock and start cars without a physical key being present. Police are advising the owners of these expensive cars to invest in physical steering wheel locks to help protect their car. Examples and evidence can be found in reference documents [A41] through [A47]. So if you own a nice Range Rover with a key start fob, you may want to stop by the auto store and buy The Club 1000 original steering wheel lock.

[27] [A40] Zetter, Kim. *Hackers Could Heist Semis by Exploiting this Satellite Flaw.* (July 30, 2015). wired.com. Retrieved on 19 August 2015 from http://www.wired.com/2015/07/hackers-heist-semis-exploiting-satellite-flaw/.

[PAGE INTENTIONALLY LEFT BLANK]

11 Current Research Activity

To an important degree, all research into secure and trusted networks, computers and embedded systems will be relevant to *vehicle* cyber security. Trusted, formal programming and development practices are ultimately essential for achieving the goal of a secure transportation infrastructure. However, the freight industry needs research that will protect their vehicles *today*. This is targeted research. And, the community publicly active in this area -- although growing -- is still very small.

Our literature review shows that automotive computer/network security has been an area of academic interest since at least 2002; this was at a time when CAN networking (in conjunction with ODB-II and heavy J1939 standard vehicles) was gaining significant traction, if not dominance, in vehicle architecture. Yet, prior to 2008, we find that vulnerability analysis appears to have been largely theoretical. At least publicly, academics have lead the way and in doing so, have encouraged a growing community of private security analysts. The publicity generated by these 'white hat' hackers has given significant momentum to political awareness of research needs, and inspired some basic legislative proposals, but resulted in very little additional funding.

Some identifiable funding has been provided by the National Science Foundation (NSF) and Defense Advanced Research Projects Agency (DARPA). One notable irony is how small grants in basic research have helped uncover and demonstrate fundamental, and potentially devastating, security flaws common to most vehicle networks.

Automotive manufacturers have committed to an Information Sharing and Analysis Center (ISAC) which should help advance research. Heavy vehicle manufacturers, however, are *not* leaders in this initiative. Regardless, the research activity of vehicle manufacturers only has indirect visibility -- for example through activities in the SAE International (SAE) -- and is tempered by commercial and proprietary considerations and interests.

However, our impression remains that research into heavy vehicle vulnerabilities is fragmented and underfunded at this time.

11.1 Academics, Engineers, Hackers and Security Researchers

The research in the key 2010 [A01] *Experimental Security Analysis of a Modern Automobile* and 2011 [A02] *Comprehensive Experimental Analysis of Automotive Attack Surfaces* papers was funded, in part, by the National Science Foundation (NSF) and Air Force Office of Scientific Research (AFOSR). The authors of these papers demonstrated the extreme vulnerability of the CAN network and the ECUs connected to them. However, the dramatic exploits uncovered in this research were largely dismissed by automotive manufacturers. Still, at least one lonely commenter thought to ask: *Can fleet vehicles be hacked?* [28] Nevertheless, almost all subsequent research has remained conducted on light (passenger) vehicles.

[28] ... concluding that there was no need to worry for the moment, but that in 5 to 10 years, "all bets are off." See Antich, Mike. *Can Fleet Vehicles be Hacked?. HDT Heavy Duty Trucking, truckinginfo.com. (May 27. 2010). Retrieved on 22 July 2015 from:* http://www.truckinginfo.com/blog/market-trends/story/2010/05/can-fleet-vehicles-be-hacked.aspx.

Independent researchers, hackers, have picked up the mantle and continued the journey of exploration. Topics on 'hacking' vehicles have become *de rigeur* at computer security and hardware hacking conferences such as *DefCon, Black Hat, SysCan* and *CounterMeasure*.

- Researchers Miller & Valasek, whose research has, in part, been previously discussed, have presented their findings at several of these conferences.[29] Notably, a significant portion of their work has been funded by the Defense Advanced Research Projects Agency (DARPA).

- The most recent DefCon hosted a *Car Hacking Village*, giving hackers the hands on opportunity to begin exploring vehicle security (and no doubt inspiring vulnerability research we will read about all too soon).

11.2 Battelle: Vehicle Cyber Security as a National Security Discipline

Battelle, with 22,000 employees, is "the world's largest nonprofit research and development organization." *Vehicle Cyber Security* (VCS) is one research domain under the umbrella of Batelle's *Cyber Innovations* sub group in *National Security* research.

The VCS group was a participant in the (2012) one-year NHTSA "Safety Pilot" extensive trialing of V2V and V2I in Ann Arbor, Michigan. For the Pilot, 2,800 vehicles were equipped with a variety of devices from different manufacturers, implementing a mix of connected vehicle ADAS technologies and tested on 73 miles of instrumented roads. Battelle was responsible for 8 (of the 16) heavy commercial / fleet vehicles in this scheme.

Battelle has also developed a form of vehicle Intrusion Detection System (IDS), their NEM Vehicle Network Enforcement Module. The NEM learns normal vehicle network behavior and monitors for anomalies from software or firmware bugs, other system malfunctions or cyber attacks. NEM is reportedly in testing with "several" automotive manufacturers.[30]

The Annual CyberAuto Challenge (CAC) - Recruiting Next Generation Engineers

However, what is probably Battelle's most unique contribution to Vehicle Cyber Security is their annual CyberAuto Challenge (CAC). The CAC brings together "scores" of high school and college students, automotive engineers, scientists, policy makers, representatives of federal agencies (DOT, DOD, DHS), 'white hat' hackers and other security researchers for a week long training and practicum-camp session. This is free of charge to the invited students who are assembled into working groups with security professionals for active sessions in topics such as CAN Bus engineering, forensics, embedded programming, reverse engineering, vehicle attack surfaces and security strategies.

The Third Annual (2014) CyberAuto Challenge generated headlines with the story of a high school student's exploit of a car. The student decided not to wait for the practical end of week session which was to focus on designing and implementing a remote attack on a car. Instead, he went to Radio Shack,

[29] Miller & Valasek papers are references [A03], [A04], [A05] and [A06].

[30] A very high level explanation of the NEM is available at this link: https://www.youtube.com/watch?v=nB0mT8UtTPY&list=UU4NPUPf1eo-FF_acXNKpugw

spent $15 on parts and worked into the night building his own circuit board. By the next morning, he was able to remotely control the windshield wipers, lock and unlock the doors, engage the remote starter and flash the headlights to the beat of the music on his iPhone.

As Dr. Andrew Brown, chief technologist at Delphi Automotive, was quoted: "This kid was 14, ... looked like he was 10" and, industry representatives noted "'There's no way he should have been able to do that". Describing it later, Brown is quoted as saying it was "mind-blowing."

The CAC has had demonstrable success in helping the industry identify and recruit students into the study of automotive cyber security. And, in doing so, the CAC has memorably demonstrated (1) how low the barrier to entry to vehicle hacking can be, and (2) how important it is to recruit (ethical) talent in this area.

11.3 SAE International (SAE)

The SAE International is a critical resource for direct and indirect access to researchers and research projects. SAE has approximately 140,000 members from OEMs, tier 1 suppliers, security consultants, academics, industry associations, specialized and management consultancies, government and other interested parties.

The work of the Global Ground Vehicle Standards[31] group is organized into major categories, including the Motor Vehicle Council (MVC) and the Truck and Bus Council (TBC). The TBC is charged with vehicles 10,000 GVRW (Class 3) and above. Whereas significant MVC activity is extensible to heavy vehicles, the TBC committees and subcommittees focus is on those areas with material differences specifically applicable to heavy vehicles.[32]

For example, the SAE is developing V2V communications standards, notably DSRC, under contract for the NHTSA. This work is initially for light vehicles, but NHTSA is in the process of drafting rules for heavy vehicles. Specifically, in the area of heavy and commercial vehicles, SAE committees are also looking at truck platooning, Lane Departure Warning (SAE J3045) and Forward Collision Avoidance and Mitigation (FCAM) System (SAE J3029) test procedures, ADAS and drive-by-wire issues (e.g. *WIP* SAE J3081: Recommended Practice for Heavy Vehicle Operator Controls Prioritization and Conflict Resolution).

One MVC committee -- the SAE Vehicle Electrical System Security Committee -- is concerned with on board vehicle ECUs that, when manipulated by an attacker, can control or act contrary to occupants' interests. The committee's work includes prevention, detection, identification, defense and mitigation. We understand that the TVC is likely to form a similar committee.

[31] One SAE slide on standards development cites notes that -- in one year -- some 600 committees, involving nearly 9,000 members and 3,000 companies participated in approximately 1,400 meetings on standards development in the area of Global Ground Vehicle Standards.

[32] An interactive organizational chart with statements on committee scope for the Global Ground Vehicles group is available at: http://www.sae.org/standardsdev/groundvehicle/gvorgchart.pdf

SAE is in the process of producing standards such as SAE J3061, a "Cybersecurity Guidebook for Cyber-Physical Systems" and is in the early stages for issuance of a standards of "Best Practices for Cyber Automotive Systems".

However, of special interest is the SAE Commercial Vehicle Engineering Congress (ComVec) which has held sessions specifically focused on Cybersecurity for Commercial Vehicles (CVCS). The first two CVCS sessions were held in October, 2014. Another ComVec CVCS session is scheduled for October, 2015. Panelists are a mix of government, automotive and academic parties.

11.4 Platform and Engine OEMs, Tier 1 Suppliers and Cyber Security Consultancies

The ECUs of any vehicle brought to market are a highly integrated assembly of intellectual property, largely specific to one engine and model configuration. It is not in the obvious interest of manufacturers, their tier 1 suppliers, or even security consultancies to publicly elaborate on the details of their security research.

Visibility into this work is much more likely to come through working groups such as the SAE, symposia such as Embedded Security in Cars (ESCAR) conferences or as a byproduct of academic associations.

What is clear is that political pressure is mounting on OEMs to have credible response to questions about their security practices.[33] And, OEMs increasingly understand that failure to secure their cars, even for non-safety related hacks, still entails significant reputational risks. Pressure from the customer base can also make a difference in guiding OEMs in the right direction. This can be done very effectively by including product security assessments in the product selection criteria for fleet purchases where quantity and volume considerations can be brought to bear.

11.5 Automotive Information Sharing and Analysis Center (Auto-ISAC)

The Alliance of Automobile Manufacturers and Association of Global Automakers is developing an Automotive Information Sharing and Analysis Center (Auto-ISAC). Booz-Allen-Hamilton is leading implementation and association participants include manufacturers who also have heavy vehicle divisions such as Ford, GM, Mercedes-Benz, Mitsubishi Motors, Toyota, Volvo.[34] NHTSA is also a key stakeholder in this initiative. The system is not yet operational but has been reported as likely to go live in late 2015. The SAE is reportedly supporting this project and recent information was released in conjunction with the 2015 Battelle CyberAuto Challenge. Unfortunately, due to the proprietary nature of vulnerabilities, information sharing with the public is likely to be very limited.

The early identification, warning and dissemination of vulnerabilities, exploits and attacks are, together, a critical coordinated service that has been absent in vehicle cyber security research.

---

[33] In September 2014 there were prominent reports that General Motors appointed their first Chief Product Cybersecurity Officer, pulled from their Infotainment divisions (see: https://www.linkedin.com/pub/jeffrey-massimilla/b/31b/180). And, in a similar time frame, it was noted that Ford was looking to recruit Automotive Cyber Security Engineers (see: https://www.linkedin.com/jobs2/view/1823858).

[34] Although no heavy vehicle manufacturing divisions are themselves participants in the ISAC proposal.

11.6 Government Funding and DARPA - High Assurance Cyber Military Systems (HACMS)

As noted, above, important research has been sponsored by the NSF and DARPA. And, as a pattern, we see Department of Defense (e.g. AOFSR and DARPA) and Department of Homeland Security (e.g. DHS Security, Science and Technology Directorate, Cyber Security Division (S&T CSD)) as sponsors and consumers of specifically applicable research.

The Department of Transportation (DOT) is funding a vast array of research in Intelligent Transportation Systems (ITS), and Connected Vehicles technologies. Critically, the National Highway Transportation Safety Agency (NHTSA) has new mandates directly applicable to vehicle cyber security. Yet these are nascent, and even unfunded efforts, as we shall discuss further, below, in considering the regulatory and legislative environment.

Notably, DARPA's Innovation Information Office (I2O) High-Assurance Cyber Military Systems (HACMS) program has been the most comprehensive and visible sponsor of research most likely to be directly applicable to heavy vehicles. Reference [A11] provides an overview of the program structure entitled *HACMS: Making sure you are in control of your vehicle.* HACMS funds programs, projects, researchers and laboratories in an integrated framework, with a structured model for applying solution domain expertise, in differing deployment scenarios. HACMS research has been published in industry forums such as ESCAR.

[PAGE INTENTIONALLY LEFT BLANK]

12 Current Legislative Activity

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 focused on preliminary information gathering and the early development of some consumer based legislation focused on protecting the retail consumer of passenger cars.

On February 11, 2015, Senator Edward J. Markey (D-Mass.) and Richard Blumenthal (D-Conn.) announced new legislation that would direct the National Highway Traffic Safety Administration (NHTSA) and the Federal Trade Commission (FTC) to establish federal standards to address cyber security and data privacy issues in automobiles. Notably absent was any reference to heavy vehicles.

On May 28, 2015 a bi-partisan group from the House of Representatives House and Energy Commerce Committee wrote an open letter to seventeen automobile manufacturers and the NHTSA requesting information on how they were planning on dealing with emerging cybersecurity challenges as vehicles and transportation infrastructure becomes increasingly connected (through v2v and V2I). These were excellent letters. The letters contained a good summary of the issues discussed in this document including more nuanced issues like supply chain attacks; and the terminology was not necessarily focused exclusively on passenger cars. The list of manufacturers to which the letter was sent included seventeen manufacturers of automobiles and the NHTSA. Again, noticeably absent were any manufacturers of heavy vehicles such as International, Kenworth, Volvo, etc. or heavy engine manufacturers like Detroit Diesel and Cummins.

MAP-21 (Moving Ahead for Progress) was a piece of legislation for the multi-year funding of transportation priorities and included $105 billion in funds signed into law in 2012, and becoming effective in 2013. It also included a number of rules and regulations impacting the transportation industry including such things as event-on-board-recorders (EOBRs) on all interstate commercial vehicles, electronic logging of service hours, etc. This massive legislative and budgetary endeavor contains little or no explicit focus on transportation cybersecurity.

It would seem that Rep. Waxman (D – CA) has been trying to get an advanced cyber security program established at NHTSA since around 2010. We found some DOT NHSTA presentations on transportation cyber security from 2011 by Michael Dinning from US DOT Research and Innovative Technology Administration. They were at a very high level which covered many modes including aviation and passenger cars, but they were mostly focused on establishing a program. Our review of NHTSA 2016 budget request shows that NHTSA has requested funding a new program in Vehicle Electronics and Emerging Technologies at $4 million for 2016. This was to cover some research by existing engineers and two new full time employees. This would seem to indicate that the program is in its infancy.

There may be additional classified and unpublished activities and information to which we are not privy but, from what we can gather from public sources, very little if anything is being done to address the cyber security of heavy vehicles.

[PAGE INTENTIONALLY LEFT BLANK]

13 NMFTA Recommendations

Based on the research that NMFTA has conducted, we have developed some recommendations for our members which we believe can help our members reduce and mitigate the risks discussed in this paper. We have also put together some ideas for industry activity to help address these security issues in the medium and long term.

13.1 Protect Your Networks

While the most sensational hacks involve direct remote access and control of the vehicle itself; however, the easier method to gain access is to attack office networks and those computers that are used to communicate with the vehicles. This involves known and proven techniques and exploits for remote access such as malicious websites and email attachments but can also include direct access by a rogue contractor or disgruntled employee. In order to protect the networks and computers that communicate with vehicles, companies should be following basic network and computer security protocols:

- **Separate Networks** - Segregate the networks where computers have remote access to vehicle systems from other more common networks used for conducting routine business like email, browsing the internet, working on office documents, etc.
- **Network Security** – Make sure that you protect your networks that communicate with vehicles with well configured firewalls, intrusion detection/prevention systems (IDS/IPS), as well as vulnerability management tools to help ensure that your environment has the latest patches and is configured properly.
- **Lock Down Internet Access** - Restrict internet access on all systems and computers that communicate with vehicles and consider removing internet browsers, PDF readers, and email clients, etc. These are the most common vectors for attack against traditional networks. If outbound internet access is required, make sure to restrict internet access to a known set of safe destinations.
- **Two Factor Authentication** – Ensure that all systems that give remote access to vehicle communication and features are accessible only via two factor authentication. This prevents password sharing, brute force password attacks, and makes unauthorized access much harder.

Additional information regarding basic sound computer security can found in *Critical Security Controls for Effective Cyber Defense* by the Council on Cyber Security [A23]. The principles contained in this document are not just applicable in protecting your networks; many of these same principles can also be applied to vehicles.

13.2 Protect Your Vehicles

While little can be done to change the vehicle computer design in the short term to deal with the security issues we have been discussing, there are a number of things which members can to do to help reduce the associated risks.

- **Vendor Communication** – Make sure to establish communication and notification avenues with manufacturers and 3rd party product/service integrators to ensure that you are notified of any critical security issues or updates to your equipment and service. If you do not know about a problem, you cannot fix it.
- **Established Maintenance Plans** – Establish documented maintenance plans for the vehicles which include requirements to ensure that the latest firmware and software patches/upgrades are applied to the vehicles systems within 30 days of release.
- **Reduce Attack Surface** – Just because the feature is available does not mean it should be used or enabled unless it is absolutely necessary. Disable and remove unused features that are not critical to the use and functionality of the vehicle. This can help reduce the risk to the vehicle. This is a tried and true method adopted from general best practices for locking down other computer equipment and is a good way to reduce the attack surface.
- **Question New Features and Capabilities** - Question regulatory requirements for new efficiency and safety mandates, new vehicle features from manufacturers, and integrated communication systems from a security perspective. Vendors and agency regulators are always introducing new safety and productivity features, but there seems to be very little concern regarding the underlying computer security implications. Based on our research, we see features such as convoy platooning beginning in 2016,[35] and autonomous heavy vehicles on highways starting this year.[36] Other new advances are just around the corner. Ask yourself, do we really need to be doing this or does enabling this functionality endanger my vehicles, company, or the transportation industry as a whole? How can this regulation requirement/feature/system weaken our vehicle security and how can it be abused? Until we get a better handle on vehicle system security, it is best to take a cautious approach.

13.3 Prepare for the worst

There is a saying in the computer security community that there are only two types of networks. Those who have been hacked and those where the hackers on the network have not yet been found. Given that *hackers have to get lucky only once* -- and those *people protecting computer systems and networks have to be perfect all the time* -- the odds are heavily in the hacker's favor. A security breach is almost inevitable.

[35] Transport Topics. *Platoon Use to Begin in '16 ...: Fleet to Implement System, Peloton CEO Says.* Retrieved on 2 September 2015 from https://www.ttnews.com/articles/printopt.aspx?storyid=39166.

[36] Goodwin, Antuan. *Self-Driving Freightliner Inspiration Rolls Out on Public Roads in Nevada.* [Cnet.com]. (May 6, 2015). Retrieved on 25 June 2015 from http://www.cnet.com/news/freightliner-autonomous-inspiration-truck/.

A standard part of system security is an incident response plan. This plan outlines the process and procedures to follow in the event of an incident. Planning before an event takes place, helps ensure you know how you can recover and is critical to surviving a breach or attack. It is highly recommended that all members immediately start working with the heavy vehicle manufacturers and associated 3rd party providers to develop a plan on how you can recover from a breach and/or attack against heavy vehicle fleets.

As we have covered previously, a large scale attack or incident on the entire transportation community or key transportation points can have a devastating impact. The industry must prepare and be ready to get the trucks moving again in the event that they are compromised.

In the case of heavy vehicles, there are basic and fundamental questions that need to be answered:

- How can we disconnect an affected vehicle from remote communication systems and reload a known good version of all firmware to get the vehicles moving again, even if it is at minimal functionality?
- Is there a switch to disconnect remote connectivity or does it require wire cutters? Is there a field manual for performing the disconnect?
- Who has known good firmware, tools and knowledge to restore compromised components and CAN networks? Can it be done in the field?
- If there are critical ECUs that cannot be recovered, who has parts in inventory and how can we get them into the field?
- If there is an event with one vehicle, how do we warn others so that they can take necessary precautions, e.g. disconnect from the communication system, to limit the impact on the fleet and the industry?

13.4 Develop Heavy Vehicle Counter Measures

While a permanent solution to these issues seems out of reach at the moment, there are some medium term ideas which show promise to mitigate some of the risks. These ideas are well within reach and do not require full automotive lifecycle time frames or cost structures.

When implementing a computer network which is to be connected to the internet, a firewall and usually an intrusion detection (IDS) and intrusion prevention (IPS) system are placed between the internal network and the internet. These systems are essentially autonomous appliances that inspect and control the communication between the network and the internet. The appliances act as a bridge between the two areas. The firewall component blocks messages other than the ones it has been configured to allow. The intrusion detection and prevention appliances look for traffic patterns (signatures) which are outside of what is to be expected in normal operations. When abnormal traffic is identified, the appliance issues alerts and/or blocks the traffic depending on how they have been configured to behave for a specific pattern. This keeps unwanted and malicious traffic from entering the computer network from the internet.

Based on our research, we believe that it is feasible to develop and deploy engine computer firewall and IDS/IPS systems into existing vehicles. There have been basic prototypes of intrusion detection devices built by private individuals such as the device discussed by Miller and Valasek in *A Survey of Remote Automotive Attack Surfaces* [A04]. The SAE International (SAE) have also published some work in this area. See [A19] *CAN Security: Cost-Effective Intrusion Detection for Real-Time Control Systems*. And, it is worth once again highlighting the Batelle NEM IDS discussed in section 11.2, above.

The initial results seem to indicate that there are cost effective methods for developing basic security appliances and attaching them to the CAN network. While such a device would not offer 100% protection or be a "silver bullet" to solve all security problems, it would provide a significant and welcome improvement. Even a basic ability to block certain inbound traffic from remote interfaces to the CAN based on a defined rule set as well as look for known patterns of malicious or out of place traffic would be a large step forward in mitigating the security risks of the current CAN network design. We would urge the members to collaborate with the industry at large as well as manufacturers, academia, industry non-profits, and government agencies to rapidly research and develop this key technology so that it can be deployed into the field as quickly as possible.

Another idea developed during our research was the manufacture of standardized field repair kits. If a particular heavy vehicle is immobilized in a strategic location or in sufficient quantities it could cause serious problems. If the vehicle manufacturers could provide field kits for each make and model of their vehicle, which allow someone to replace key EUCs and CAN components and disconnect it from remote access so that it could be made functional quickly, this would also help mitigate the risk posed by some of the more sever scenarios. These kits would significantly aid in the development of incident response plans and provide the same type of "recover from backup" which the computer industry relies on today to recover from malicious software infections. We would urge the members to collaborate with all interested parties to rapidly develop these types of field kits so that they can be deployed into the field as quickly as possible.

13.5 Educate

One of the first steps in dealing with such a large issue is to educate all the different stakeholders as to the issues and potential impact regarding heavy vehicle cyber security. To that end, we would recommend that members share this paper within their organizations and the industry in general to help everyone understand the nature of the problem so that everyone can start to take the necessary steps to mitigate and ultimately work together to resolve the issue.

13.6 Incorporate Security in OEMs/Vendor Selection

One of the most practical moves our industry can take is to start including security evaluations as part of the product selection criteria. OEMs respond faster and better to market pressure than regulatory or industry standardization pressure. The next time you go out to buy heavy vehicles, start asking them about security. Does this product undergo adversarial security testing? Does it come with a field kit to assist in recovery in the event of a breach? If not, why not? If you are buying 10 or 1000 units, start pushing the concept of vehicle security back up the sales chain. The same goes for all 3rd party providers. Before you buy and install the product, ask them about security.

13.7 Collaborate and Innovate

In order to more thoroughly address heavy vehicle computer security issues, there will need to be transformative changes in the way that they are designed and implemented. There have been several papers written on securing vehicle computer systems, although mostly for personal automotive vehicles. These papers include [A22] *Securing the Automobile: a Comprehensive Approach* from Galois Inc.[37] and [A21] *Five Star Automotive Cyber Security* by I am the Cavalry. There has also been work done by SAE such as [A20] *Securing Connected Vehicles End to End.* We see no reason why these same ideas cannot be applied to heavy vehicles. We recommend that our members work with industry leading manufacturers, academics, and organizations such as the SAE to develop long term product development plans that incorporate security by design from the bottom up and include rigorous adversarial testing and remediation plans.

We would also urge our members to sponsor and support further research and development for CAN and ECU security, either directly or indirectly, and in conjunction with universities, industry partners, manufacturers, non-profits associations, government, etc. A good example would be studies and projects such as those being done at the University of Tulsa and described in their proposal: *A Heavy Vehicle Test Bed for Cyber Security Research* [A10].

13.8 Develop Legislative Initiatives

A problem of this size, scope, and complexity will also require the development legislative initiatives. This includes:

- The development of distinct security standards and regulations for heavy vehicle computer systems. The current automotive legislation being presented is specific to automobiles and heavy commercial vehicles have different complexities and issues.
- Legislative initiatives to curb agency regulatory requirements and mandates that would unintentionally further increase the risks to heavy vehicles. This could take the form of mandatory vehicle security impact assessment to new agency regulations. For example, requiring a mandatory remote kill capability on engines who idle may be a good idea from an environmental perspective, but if implemented without consideration to vehicle system security, it could be disastrous.
- Development of formal government mandatory review periods for the adoption and approval of new leading edge technology such as platooning, V2V systems, autonomous vehicles, etc. to slow down the adaptation of these technologies so that security impact can be determined.

[37] Galois are a participant in the HACMS program.

[PAGE INTENTIONALLY LEFT BLANK]

14 Conclusions

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 previous section of the paper, we have outlined a set of recommendations that we urge the members 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 recommendations section 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. Given the carrier nature of the NMFTA membership and our available resources, it seems that NMFTA is in a position to help facilitate, coordinate, and educate on the criticality of cyber security for heavy vehicles. This undertaking would benefit our members and the transportation community as a whole. This could take the form of organizing meetings for connecting key people inside the various industries to work on the problem. And, possibly sponsoring the necessary research directly -- and in conjunction -- with our members. The one thing that we cannot afford to do is … nothing.

[PAGE INTENTIONALLY LEFT BLANK]

15 Acknowledgments

NMFTA would like to thank Kevin Kenety for his assistance in researching and developing this paper on our behalf. We would like to thank Jeremy Epstein from the National Science Foundation for making introductions to the academic researchers presently leading the way in this field. We would also like to thank Professors Rose Gamble and Jeremy Daily from the University of Tulsa for sharing their knowledge and ideas in the field of heavy vehicle security and answering our many questions. We would also like to thank everyone who had a hand in reviewing and editing this paper. Additionally we would like to thank all the other academics, security professionals, white hat hackers, and hobbyists who have published the information which forms the core of our survey on the state of affairs in this area. Our reference section contains a myriad of worthwhile information, which we have tried our best to cover, that is strongly recommended for those who want a deeper dive into the subject.

[PAGE INTENTIONALLY LEFT BLANK]

16 Annotated References and Guide to Resources

Automotive hacking has become the subject of dozens of conference presentations, hundreds of working groups, briefings, and papers of varying quality, all wrapped in an often hyped and endlessly churned journalistic cycle. While these stories grab our attention, and therefore help to justify assigning resources to examining the issues, a real understanding of the problems, the impact, the community of who is working on these issues, and how one can mitigate risk and promote long term solutions requires examining *primary* research as part of the process of outlining, and writing the white paper.

The NMFTA literature search and resulting survey paper identified academic and industry research into automotive security vulnerabilities dating back to at least 2002, with the first annual conference on Embedded Security in Cars (ESCAR) taking place in Europe in 2003.[38]

Hence, there is a dense body of work available.

However, prior to 2008, vulnerability analysis appears to have been largely theoretical. And, not until seminal research published in 2010 and 2011 did the public begin to understand how the computerization of vehicles and increased external attack surface of wireless interfaces meant that cars were hackable -- cyber physical systems -- with exploitable vulnerabilities.

The group of documents assembled for this package is intended to provide a window into the primary, or otherwise significant, work in this area and provide the basis for better informed discussions and in complement to the NMFTA white paper on Heavy Duty Vehicle Cyber Security.

Notes to the reader are provided for context and to help a reviewer evaluate the merit of them investing time reviewing that specific document.

Each document in this research package is referenced in the format [A##], or similar.

- The [LR##] set is composed of those documents that have been chosen to highlight legislative, political and/or regulatory matters;
- The [VN##] set is composed of those documents that are specific to vehicle networking which are comparatively technical in nature;
- The [A##] set are those documents referenced in the white paper and/or those which are themselves useful resources for further investigation of subjects discussed in the white paper; and,

Some of these documents may also have associated Recorded Media available; subject to limitations on available disk space, several recorded presentations may also be distributed with reference / resource documents. For example, the recorded presentation of research paper [A01] is provided as [A01-RM].

The minimum CORE PACKAGE suggested for review is A01 through A05.

[38] Notably, the first US ESCAR Conference did not take place until 2013.

16.1 The Core Papers Exploring Vehicle Cyber Vulnerabilities

In 2010 and 2011, researchers from the University of California, San Diego (UCSD) and the University of Washington (UW) -- funded , in part, by the National Science Foundation (NSF) and the Air Force Office of Scientific Research (AFOSR) -- released two of the most influential papers [A01] [A02] in automotive network security which are essential reading in their entirety.

[A01] "Experimental Security Analysis of a Modern Automobile" (2010) provides an excellent review of vulnerabilities of Engine Control Units (ECUs), sensors and the Controller Area Network (CAN) which interconnects these components . Highly recommended reading.

> Earlier papers on automotive hacking tended to be more theoretical. This first paper is largely premised on the attacker having *physical access* to the target vehicle, hence the CAN Bus / ODBII port to communicate with ECUs and sensors, and then determining what they could hack.
>
> The authors were able to maliciously bridge subnets, and control many vehicle functions including engine, brakes, heating and cooling, light, instrumentation and more.
>
> They found what little security existed in ECU components was poorly implemented or usually easily circumvented. Even where properly implemented, brute force methods could break the keys. Hence, ECUs were open to firmware attacks, and they even managed to show that an ECU could be re-flashed whilst the vehicle was in motion.
>
> The authors' "CarShark" application was developed to monitor and inject messages onto the CAN Bus and multiple 'composite' attacks demonstrated forcing braking, disabling braking and shutting down the vehicle to prevent restarting and other 'denial of service' attacks.
>
> Importantly, the authors also highlight how any component on the CAN Bus might be compromised through counterfeit or otherwise malicious supply chain attacks introducing other hidden vulnerabilities.
>
> The authors are well aware that, in an era of increasing wireless connectivity in automobiles, that the attack surface is expanding. They were able to demonstrate several hacks of / and through externally facing attack surfaces and vehicle telematics.

K. Koscher, et al ., *Experimental Security Analysis of a Modern Automobile*, published in *IEEE Symposium on Security and Privacy*, IEEE Computer Society, May 2010. Retrieved 22 July 2015 from: http://www.autosec.org/pubs/cars-oakland2010.pdf.

[A02] "Comprehensive Experimental Analyses of Automotive Attack Surfaces" (2011) follows on from the earlier 2010 paper and is perhaps the first systematic and experimental study of the external (and remote) attack surfaces of a car. Highly recommended reading. This is a generalized survey of automobile vulnerabilities extrapolated from theoretical and practical work on a single vehicle model. Miller and Valasek's work in [A04] may be considered a generalization of this work through experimental research into a large number of late model year vehicles.

S Checkoway, et al., *Comprehensive Experimental Analysis of Automotive Attack Surfaces*, released 2011 [any journal publication unknown]. Retrieved 22 July 2015 from: http://www.autosec.org/pubs/cars-usenixsec2011.pdf

From 2013 we see the research into automotive security move away from a more academic grounding and increasingly towards disclosure at 'hacking' and computer security conferences, such as BlackHat, DefCon and CounterMeasure.[39]

[A03] "Adventures in Automotive Networks and Control Units" was authored by Dr Charlie Miller and Chris Valasek[40] in support of their DefCon 21 (July 2013) presentation. The authors provide significant (replicable) detail of how they hacked a model year (MY) 2010 Ford Escape (with Active Park Assist) and a MY 2010 Toyota Prius (with Intelligent Parking Assist, Lane Keep Assist and Pre-Collision System). The level of detail contained in this paper is that of primary (often raw) research. Hence, it is recommended to merely skim the [A03] paper and to gloss over the specifics of the attack. If the reader wishes to examine a specific CAN Bus hack, [A06] is preferred.

Through the CAN Bus the authors were able to disable brakes, disrupt steering control, influence acceleration, kill the engine, pre-tension seat belts, control headlights, door locks and the horn, as well as alter displayed information such as fuel levels (although not all exploits were achievable on both cars). In addition, they were able to extract ECU firmware and reflash ECU's with altered versions capable of sending malicious messages onto the CAN Bus.

> This research also specifically garnered the attention of Senator Ed Markey (D-Massachusetts) who requested information from 20 automotive manufacturers concerning, inter alios, Miller and Valasek's [A03] research. This, and related congressional interest, is discussed in greater detail in the comments on [LR01] through [LR07].
>
> It is also worth noting that this research was funded by a US$ 80,000 DARPA grant (elsewhere reported and not detailed in the paper itself). The level of investment (and skill) required to develop these exploits is well within the resources of organized criminal gangs and national actors.
>
> However, there are significant limitations in the extent of control demonstrated in these vehicles -- the vehicle hacks demonstrated required interfacing a computer laptop to the CAN Bus. And, at the time of their publication, these hacks might be responsibly viewed as proof of concepts instead of exploits expected to be imminently weaponized.
>
> Nevertheless, demonstrations by the authors' of their work for the media are the root source of hundreds of written and dozens of broadcast media reports on car hacking. Much of this work was sensationalized. Yet, proof of concept of remote exploits would imminently follow, many developed by Valasek and Miller who have since become highly visible in the area of vehicle security and hacking.

Miller & Valasek, *Adventures in Automotive Networks and Control Units*, supporting paper to presentations at Defcon 21 (July, 2013), Hackers to Hackers Conference H2HC 2013 (October), and CounterMeasure 2013 (November). Retrieved 22 July 2015 from: http://illmatics.com/car_hacking.pdf.

AVideo of the DefCon presentation at: https://www.youtube.com/watch?v=n70hIu9lcYo.

[39] https://www.blackhat.com/, https://www.defcon.org/ and http://www.countermeasure.ca/.

[40] Biographical and publications information for Valasek available at http://chris.illmatics.com/about.html.

[A04] "A Survey of Remote Automotive Attack Surfaces" is Miller and Valasek's next major published research, made public at the BlackHat (August) 2014 conference in Las Vegas.[41] Once again, much of the paper presents primary (raw) research that need not be examined in detail by the reader. The reader is therefore advised to read from the start of the paper [A04] through to page 23 (inclusive) and then continue from page 87 to the end.

These sections of the paper will present the authors' three stage model for the "Anatomy of a Remote Attack" on vehicle computers: First, gain a point of entry in to the vehicle network. This initial point of entry is unlikely to give immediate access to target (sensitive) ECUs. Second, bridge the penetrated network to gain access to safety critical ECUs. And, third, cause the target ECU to control and compromise vehicle control and function.

> (Stage 1) The paper lists and discusses remote attack surfaces in the modern automobile which might be typically used in the first stage of a remote attack; the authors consider Passive Anti-Theft Systems (PATS), Tire Pressure Monitoring Systems (TPMS), Remote Keyless Entry / Starter (RKE), Bluetooth integration, Radio Data Systems (RDS), and Telematics / Cellular / Wi-Fi extended networks.
>
> (Stage 3) The paper also lists and discusses some of the cyber-physical systems (those with cyber kinetic potential) found in modern cars as *features* which might be compromised in the third phase of a remote attack to effect vehicle control and function. The authors consider Park Assist, Adaptive Cruise Control, Collision Prevention and Lane Keep Assist systems. Each of these features requires ECUs control over steering, acceleration and braking systems.
>
> Naturally, third phase attacks could also target non cyber-physical systems exploiting vulnerabilities previously discussed in CAN Bus devices such as vehicle locking, lights, horn, gauges and other instrumentation.

The Stage 2 attack is non-trivial and the authors' work in surveying some of the detailed differences between manufacturer, model (and potentially model year) automotive network topologies demonstrates a wide variance in the potential 'hackability' of any specific car.

Miller & Valasek, *A Survey of Remote Automotive Attack Surfaces,* supporting paper to BlackHat USA 2014 (August) and DefCon 22. Retrieved 22 July 2015 from: http://illmatics.com/remote%20attack%20surfaces.pdf.

Video of the DefCon presentation at https:/www.youtube.com/watch?v=tnYO4U0h_wY.

[A05] "Remote Exploitation of an Unaltered Passenger Vehicle" is Miller & Valasek's latest work, formally released in August, 2015 immediately following their DefCon presentation of the same title. Having established in [A04] that the Chrysler Jeep was likely to be a good hacking target, they set about attempting to gain remote control over the vehicle purely through unaltered factory installed wireless interfaces. Miller and Valasek identified multiple attack vectors and were able to exploit multiple vulnerabilities in the infotainment system. These included local wireless through which an attacker could compromise nearby vehicles. And, the factory telematics system which ultimately exposed each vehicle to the global Internet allowing an attacker to identify and compromise a vehicle from anywhere in the world.

[41] The conference was attended by NMFTA CTO Urban Jonson and the analysis of remote attack surfaces for passenger vehicles was recognized as a vulnerability also directly applicable to NMFTA member fleet vehicles, (e.g. class 6 and above vehicles which have not been a subject security research)

The introduction to the paper provides an excellent review of the vulnerability of vehicle networks. The introduction is followed by a survey of the vehicle's attack surfaces and how they have previously been successfully exploited follows. However, from page 20, the level of technical detail in the paper increases significantly.

Therefore, it is highly recommended to review this paper [A05] through to page 19. Those readers who wish to continue beyond page 19 will be guided through the process of how Miller and Valasek could have, at will, taken control of critical safety systems of 1.4 million vehicles. The [LR05] article by Andy Greenberg of Wired also provides an excellent view into this work.

Miller & Valasek, *Remote Exploitation of an Unaltered Passenger Vehicle,* (Released August 10, 2015 following DefCon 23 (2015)). Retrieved on 31 August 2015 from: http://illmatics.com/Remote%20Car%20Hacking.pdf.

Video of the DefCon presentation at https://www.youtube.com/watch?v=OobLb1McxnI

16.2 Additional Resources Further Discussing Vehicle Hacking Techniques

[A06] "How to Hack Your Mini Cooper: Reverse Engineering CAN Messages on Passenger Automobiles", research released at DefCon 21 (July 2013), presenting an end-to-end example of how messaging of CAN instruments can be reverse engineered and then sent false data, i.e. 'spoofed', to display arbitrary readings. As proof of concept, the author builds a custom clock with the speedometer displaying the hour (0-120 MPH) and the tachometer the minute (0-6000 RPM).

This paper [A06] is recommended in full only if the reader wish to better understand the actual mechanics of CAN Bus hacking.

Staggs, Jason. *How to Hack Your Mini Cooper: Reverse Engineering CAN Messages on Passenger Automobiles*, Paper supporting presentation at DefCon 21 (2013). Retrieved on 22 July 2015 from: https://www.defcon.org/images/defcon-21/dc-21-presentations/Staggs/DEFCON-21-Staggs-How-to-Hack-Your-Mini-Cooper-WP.pdf.

[A07] "When Firmware Modifications Attack: A Case Study of Embedded Exploitation", a paper based on research done in 2012 in which researchers were able to use the remote firmware update feature of several models of HP LaserJet to make (optionally permanent) changes to the device firmware. The attack was viable against almost all LaserJet models, and Internet scanning identified some 90,000 vulnerable printers which could in turn be used to attack internal networked printers and other devices. The authors contemplated a cyber-kinetic attack where the firmware would cause the printer fuser to overheat and create a fire; however, hardware safety features closed that attack. Firmware could also have been used to 'brick' the devices.

However, the authors were able to demonstrate a much more dangerous attack. Once compromised, the printers are able to serve as a reverse proxy giving the attacker a persistent point of entry into a network.

From discovery of the vulnerability, to full development of the full exploit and payload, the process relied on publicly available vendor information, and took less than two months and less than US$ 2,000 in hardware. This work was also, in part, DARPA and US Air Force funded. This paper [A07] is recommended in full only if the reader wish to better understand a firmware attack.

Cui, Costello and Stolfo, *When Firmware Modifications Attack: A Case Study of Embedded Exploitation, 2013 (research also released in other forms in 2012).* Retrieved on 22 July 2015 from: http://ids.cs.columbia.edu/sites/default/files/ndss-2013.pdf . (DARPA USAF)

[A08] "How Are Thieves Stealing Modern Vehicles?" is a focused and brief paper on the methods being used to gain physical access to, and drivability of, *individual* cars for the purpose of theft. This paper helps answer that first question in vehicle hacking, "how do you get physical access to a vehicle network?". The answer is often through hacking the remote keyless entry (RKE) system. This paper does not concern itself with extrapolating these techniques to more scalable attacks (such as was developed in [A05]). Instead, each method of theft should be considered as an exploit that might later be scaled and weaponized.[42] This paper [A08] is optional reading and is safely skipped.

SBD Consulting, *White Paper: How Are Thieves Stealing Modern Vehicles?* (2012). Retrieved on 22 July 2015 from: http://www.sbd.co.uk/wp-content/uploads/2012/11/2010_12_2288-Whitepaper-on-Electronic-Theft-Tools.pdf

[A09] "Vehicle Electronic Security and 'Hacking' Your Car" is the *Slide Deck* from a presentation prepared by Jeremy Daily, *et al*, for the January, 2014 SAE International (SAE) January, 2014 "Texas Meeting on Car Hacking". This resource is chosen to reinforce technical detail which is presented in narrative form. Professor Daily specializes in heavy truck cash reconstruction using ECU data. Daily is one of the few people we have identified hands on with hacking, ECUs and heavy vehicles. Although there are slides with some technical detail, a quick review of this deck is a useful way to develop an understanding of vehicle hacking. In addition, Daily introduces the concept of "Truck in a Box" (TIB) simulation environments which have been built to allow research into specific configurations of manufacturer (truck and engine) ECUs. We believe that the TIB is an important research approach and for that reason [A09] is suggested reading.

Daily, J. Johnson, J. and Kongs, A., *Vehicle Electronic Security and "Hacking" Your Car,* (Slide Deck from SAE Texas Meeting on Car Hacking). (January 16, 2014). Retrieved on 22 July 2015 from: http://tucrrc.utulsa.edu/Publications/SAE%20Texas%20Meeting%20On%20Car%20Hacking%2016%20Jan%202014.pdf

[42] Several CCTV videos of automotive thefts apparently using wireless hacking tools have recently emerged in insurance forums.

16.3 Resources on Selected Research Programs (Proposed and Active)

[A10] "Heavy Vehicle Test Bed Framework for Cyber Security Research" is the one page summary of a research proposal by University of Tulsa Professors Professor Rose Gamble (a computer scientist, as Principal Investigator) and Professor Jeremy Daily (Co-Investigator, see also [A09] , above). The critical assessments and knowledge breakthroughs we have seen published in resources such as [A01] through [A05] have relied upon external funding. This one page summary [A10] is recommended reading as just one example of a research proposal that will contribute practical understanding in the area of heavy vehicle cyber security.

Heavy Vehicle Test Bed Framework for Cyber Security Research. [Funding Proposal].Rose Gamble, Principal Investigator. Jeremy Daily, et al. Co-Investigators. (August, 2105)

[A11] "High Assurance Cyber Military Systems (HACMS): Making Sure You Are in Control of Your Vehicle" is a *Slide Deck* from a March 2013 presentation given by Dr. Kathleen Fisher, the then DARPA HACMS program manager. DARPA has been a critical sponsor of research into civilian vehicle cyber security, a role quite complementary to the HACMS goals. We recommend that the slide deck [A11] should be quickly skimmed in order to get insight into the scope and complexity of the HACMS program.

Fisher, Kathleen. *High Assurance Cyber Military Systems (HACMS): Making Sure You* Are in Control of Your Vehicle. (Slide Deck). March 20, 2013. Retrieved on 31 August 2015 from: http://www.cyber.umd.edu/sites/default/files/documents/symposium/fisher-HACMS-MD.pdf.

Video of the presentation at https://www.youtube.com/watch?v=3D6jxBDy8k8.

16.4 Resources on Cyber Incidents and Trend Analysis

[A12] "Significant Cyber Incidents Since 2006" is a brief listing of significant cyber incidents maintained by the Center for Strategic and International Studies. When media is constantly reporting hacking attempts and intrusions, historical perspective is easily lost.. The argument that ECU hacking or general vehicle hacking is likely to be beyond the motivation or resources of potentially interested parties is readily refuted. For instance, those who doubt that supply chain and /or firmware attacks are likely should look at incident 29:

> **October 2008.** Police discovered a highly sophisticated supply chain attack where credit card readers made in China and used in UK had a wireless device inserted in them. The device copies a credit card when it is inserted, stores the data and transfers it via WiFi to Lahore, Pakistan. Estimated loss is $50 million or more. The device could collect only certain kinds of cards (such as gold cards), or to go dormant to evade detection.

This paper [A12] is optional reading and is safely skipped.

Center for Strategic and International Studies, *Significant Cyber Incidents Since 2006.* Version as last modified on July 13, 2015. Retrieved on 22 July 2015 from: http://csis.org/files/publication/150714_Significant_Cyber_Events_List.pdf. This list is maintained and updated and newer versions are likely to be found at http://csis.org/program/significant-cyber-events.

[A13] Mandiant, *M-Trends 2014: Beyond the Breach.* Retrieved on 31 August 2015 from: https://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf

[A14] Mandiant, *M-Trends 2015: a View from the Front Lines.* Retrieved on 31 August 2015 from: https://www2.fireeye.com/rs/fireye/images/rpt-m-trends-2015.pdf.

[A13] and [A14] are white papers produced by Mandiant Consulting. These papers are very accessible annual overviews of the cyber threat landscape. Some statistics of note are that in 2014 (2013) the median number of days an attacker was on the network was 205 (229), with the longest time an attacker had been on the network prior to being discovered was approximately 6.25 years (8.17 years). Almost 2/3 of the compromised organizations failed to discover this on their own and learned their network was hacked from an external party. We would hope that the reader of these documents internalize the concept that, in cyber vulnerability, *absence of evidence is not the same thing as evidence of absence*.

In the Mandiant reports, extremely complicated network intrusions are simply explained from the point of system compromise through to the monetarization or other realization of the goals of the attacker. Again, any reader who might doubt the determination, sophistication and/ or level of resources that are employed in every day cyber-attacks would benefit from a review of these documents. We suggest that [A13] and [A14] be at least quickly skimmed.

16.5 Resources on Potential Impacts from Heavy Vehicle (and other Cyber Physical) Hacking

[A15] "The Dawn of Kinetic Cyber" is a 2013 paper presented at the 5th International Conference on Cyber Conflict, organized by the NATO Cooperative Cyber Defense Centre of Excellence (NATO CCD COE).

The vast majority of computer attacks have sought to either obtain or deny information and, are arguably, non-violent in their nature. However, where computers interact with physical devices, we have cyber physical systems (CPS). The modern automobile is, of course, a CPS.

By exploiting vulnerable CPS systems, an attacker's actions are 'Kinetic Cyber' because they are capable of causing indirect and /or indirect physical damage, injury or death. The author argues that the Kinetic Cyber threat "is generally being ignored as unrealistic or alarmist" but is nevertheless being increasingly validated experimentally, operationally in espionage and sabotage, and for profit by criminal gangs. The paper provides a readily accessible overview of CPS/ Kinetic Cyber threats, including the "CarShark" automotive CAN Bus hacks introduced in references above [A01]. However, this paper [A15] is not necessary reading for anyone already generally familiar with the CPS/ Cyber Kinetic treats.

Applegate, Lt. Col. Scott D, *The Dawn of Kinetic Cyber*. (June, 2013). Presentation paper for the 5th International Conference on Cyber Conflict (CyCon), Retrieved 22 July 2015 from: https://ccdcoe.org/cycon/2013/proceedings/d2r1s4_applegate.pdf

The criticality of national freight, distribution and logistics infrastructure is a key area of study for policy research institutes, military and government agencies concerned with national security issues and can be expected to have been 'war gamed' in some detail. However, the importance of keeping trucks on the road is likely to be overlooked by the average citizen.

For example, increased border controls following the 9/11 attacks lead to temporary shut downs of automotive manufacturing plants in Michigan relying upon just-in-time component delivery from Canada. Disruption to road infrastructure following hurricane Katrina meant trucks with relief supplies could not get where they were needed. Both events demonstrate how road freight is an essential component to responding to national emergencies. As a consequence, industry associations and academics around the world have conducted 'what if' - 'impact' studies as public relations exercises to educate the public about a possible "truckpocalypse".[43]

These papers are provided as reference should an NMFTA associate desire to have materials at hand to help educate someone unfamiliar with the strategic importance of the industry. Otherwise, A16 and [A17] need not be reviewed.

[A16] "When Trucks Stop, America Stops", released by the American Trucking Associations in 2006, is a summary analysis.

American Trucking Associations, *When Trucks Stop, America Stops*, (2006). Retrieved on 22 July 2015 from: http://www.trucking.org/ATA%20Docs/What%20We%20Do/Image%20and%20Outreach%20Programs/When%20Trucks%20Stop%20America%20Stops.pdf .

[43] The term was evidently first coined by publisher Randall-Reilly.

[A17] "A Week without Truck Transport: Four Regions in Sweden", released by the Swedish Association of Road Haulage Companies in 2009.

Swedish Association of Road Haulage Companies (Sveriges Åkeriföretag), *A week without Truck Transport: Four Regions in Sweden,* (2009) Retrieved on 22 July 2015 from: https://www.iru.org/cms-filesystem-action?file=mix-publications/A-Week-without-Truck_full.pdf. Note, a slide presentation summarizing this paper prepared by the International Road Transport Union (IRU) delegation to the European Union may be found at https://www.iru.org/cms-filesystem-action?file=mix-publications/week-without-trucks.pdf.

16.6 Security Papers: Cyber Security for Vehicles, CAN Security, and Related Recommendations

[A18] "Security Threats to Automotive CAN networks -- Practical Examples and Selected Short-Term Countermeasures", was originally published in 2008 and is cited by the UCSD/UW team in their 2010 [A01] and 2011 [A02] papers as one of the few applied analyses of car hacking. In our review, we found the paper to be a *unique body of work* analyzing automotive exploits in a systematic CERT (Computer Emergency Response Team) derived taxonomy / model. The lead author Tobias Hoppe[44] has recently earned his doctorate based on a dissertation on 'prevention, detection and response' to automotive malware. Due to the complexity and density of this paper, reading this paper [A18] is currently only recommended to computer security staff with an interest in CERT modeling.

Hoppe, Klitx & Dittman, *Security Threats to Automotive CAN Networks -- Practical Examples and Selected Short-term Countermeasures*. Originally published in SAFECOMP (2008). Online version released 17 July 2010. Retrieved on 22 July 2015 from: http://www.cse.msu.edu/~cse435/Handouts/CSE435-Security-Automotive/CAN-Security-CounterMeasures.pdf

[A19] "CAN Security: Cost-Effective Intrusion Detection for Real-Time Control Systems" is a 2014 paper which explores how an Intrusion Detection System (IDS) might be reasonably deployed in vehicle CAN networks considering that the life-cycle of ECU components may be decades. The authors' core proposal is that IDS implemented in the gateways between CAN network segments would have significant capability to detect, and then limit the impact of, network 'spoofing' attacks which sent messages outside of the statistically (or explicitly specified) expected pattern for periodic data. [A19] is a comparatively technical paper and is only recommended reading for computer security staff with an interest in IDS.

Otsuka, S., Ishigooka, T., Oishi, Y., and Sasazawa, K., *CAN Security: Cost-Effective Intrusion Detection for Real-Time Control Systems*, SAE Technical Paper 2014-01-0340, 2014, doi:10.4271/2014-01-0340. Available for purchase from: http://papers.sae.org/2014-01-0340/.

[A20] "Securing Connected Vehicles from End to End" is a 2014 paper which considers the problem of the expanding wireless attack surface for vehicles is not keeping pace with a strategy for securing the automobile, including such potentially processor intensive and dynamic tasks as detecting -- and protecting from- malware. The authors open with an excellent survey of vehicle-specific cyber security issues. And, the core contribution of the paper is to utilize the connectivity of the vehicle to integrate cloud-based resources in the process of securing the vehicle. [A20] is a comparatively technical paper and is only recommended reading for computer security staff.

Zhang, T., Antunes, H., and Aggarwal, S., *Securing Connected Vehicles End to End*, SAE Technical Paper 2014-01-0300, 2014, doi:10.4271/2014-01-0300. Available for purchase from: http://papers.sae.org/2014-01-0300/.

[44] Information on DR Ing Tobias Hoppe: http://wwwiti.cs.uni-magdeburg.de/~choppe/

[A21] "Five Star Automotive Cyber Security" is another document focused recommendations or automotive cyber security (instead of demonstrating hacking) released by a group called "I am the Cavalry" at DefCon 22 in 2014. The "Cavalry" grew out of DefCon 21 (2013) and BSides in Las Vegas as a group of technology experts (hackers) who want to "*ensure technologies with the potential to impact public safety and human life are worthy of our trust".* Whereas Miller and Valasek's are often sought out when the threat needs to be highlighted, this paper is finding citation from researchers looking for recommendations on what to do about the threat.

The paper's recommendations are (summarized) as follows in a series of questions:

- *Safety by Design:* Do you have a published attestation of your Secure Development Lifecycle ... including adversarial testing for your products and your supply chain?
- *Third Party Collaboration:* Do you have a published Coordinated Disclosure policy inviting the assistance of third party (white hat) researchers acting in good faith?
- *Evidence Capture:* Do your vehicle systems provide tamper evident, forensically-sound logging and evidence capture to facilitate safety investigations?
- *Security Updates:* Can your vehicles be securely updated in a prompt and agile manner?
- *Segmentation and Isolation:* Do you have a published attestation of the physical and logical isolation measures implemented to segregate critical from non-critical systems?

This paper [A21] is recommended reading.

I Am the Cavalry, *Five Start Automotive Safety Framework,* a paper initially released 14 August 2014 (w/ Defcon 2014), and version retried February 2015 on 22 July 2015 from: https://www.iamthecavalry.org/wp-content/uploads/2014/08/Five-Star-Automotive-Cyber-Safety-February-2015.pdf.

[A22] "Securing the Automobile: a Comprehensive Approach" is the best single paper so far identified which focuses on automotive cyber security. The paper was written by employees of a Galois Inc, a commercial firm specializing in formal programming languages and embedded systems. This paper, like so many others, was part funded by DARPA and, in passing, references domain specific languages and environments developed by Galois and the authors in work on the DARPA High Assurance Cyber Military Systems. Although there is detail here in specific programming and development recommendations, this is actually a very comprehensive paper covering basics such as insider threats through to hardware trojans and supply chain risks.

The paper was presented at the (US) Embedded Security in Cars Conference (ESCAR) in May 2015 and this paper [A22] is highly recommended reading.

Pike, Sharp, Tullsen and Hickey (of Galois, Inc), *Securing the Automobile: a Comprehensive Approach,* (June 3, 2015), a paper initially presented at the (US) Embedded Security in Cars (ESCAR) Conference, May 2015. Retrieved on 22 July 2015 from: http://www.galois.com/~leepike/pike-car-security.pdf

16.7 Reference Document on Security Controls for Cyber Defense (Not Vehicle Specific)

[A23] "The Critical Security Controls for Effective Cyber Defense" is a publication of the Council on Cyber Security (CCS). The CCS is an intensely practical organization focused on, as they put it, cutting through the "fog of more" that comes from "chasing each new attack".

> "The activities ensure that the Critical Security Controls are not just another list of good things to do, but a prioritized, highly focused set of actions that have a community-wide support network to make them implementable, usable, scalable, and compliant with all industry or government security requirements."

[A23] this is an extensive document with which security professionals should be familiar but which the general reader can skip.

Council on Cyber Security, *The Critical Security Controls for Effective Cyber Defense* Version 5.1. Retrieved on 21 August 2015 from: http://www.cisecurity.org/documents/CSC-MASTER-VER5.1-10.7.2014.pdf.

16.8 References for Ongoing Hacking Activities

The following references provide a great overview of some the more interesting hacks that are in the news today. [A24] through [37] and [A41] through [A47] are mostly short news stories and blog entries. They are not overly technical generally and as such are recommended reading. [A38] and [A39] are very technical and can be skipped by the general reader. [A40] can be safely skipped.

Hastings Attack

[A24] Hogan, Mike. *Was Michael Hastings' Car Hacked? Richard Clarke Says It's Possible.* Huffington Post. (June 26, 2013). Retrieved on 2 September 2015 from: http://www.huffingtonpost.com/2013/06/24/michael-hastings-car-hacked_n_3492339.html.

[A25] Wallace, Benjamin. *Who Killed Michael Hastings?.* NYMag.com/ New York Magazine. (June 26, 2013). Retrieved on 26 August 2015 from: http://nymag.com/news/features/michael-hastings-2013-11/.

Ramos-Lopez

[A26] Hoffman, Gary. *Pay Up or Your Car Engine Will Stop.* CNN.Com. (April 17, 2009). Retrieved on 13 July 2015 from: http://edition.cnn.com/2009/LIVING/wayoflife/04/17/aa.bills.shut.engine.down/.

[A27] Poulsen, Kevin. *Hacker Disables More than 100 Cars Remotely.* Wired.com/ Wired Magazine. Condé Nast. (March 17, 2010). Retrieved on 19 August 2015 from: http://www.wired.com/2010/03/hacker-bricks-cars/.

Insurance Company Dongles

[A28] Fox-Brewster, Thomas. *Zubie: This Car Safety Tool 'Could Have Given Hackers Control of Your Vehicle'.*. Forbes.Com (November 7, 2014). Retrieved on 19 August 2015 from: http://www.forbes.com/sites/thomasbrewster/2014/11/07/car-safety-tool-could-have-given-hackers-control-of-your-vehicle/.

[A29] Fox-Brewster, Thomas. *Hacker Says Attacks On 'Insecure' Progressive Insurance Dongle in 2 Million US Cars Could Spawn Road Carnage.* Forbes.Com (January 15, 2015). Retrieved on 19 August 2015 from: http://www.forbes.com/sites/thomasbrewster/2015/01/15/researcher-says-progressive-insurance-dongle-totally-insecure/.

[A30] Greenberg, Andy. *Hackers Cut a Corvette's Brakes Via a Common Car Gadget.* Wired.Com/ Wired Magazine. Condé Nast. (Published August 11, 2015). Retrieved on 19 August 2015 from: http://www.wired.com/2015/08/hackers-cut-corvettes-brakes-via-common-car-gadget/.

OEM Telematics

[A31] Anthony, Sebastian. *Tesla's Model S Can Be Located, Unlocked, and Burglarized with a Simple Hack.* April 1, 2015). Retrieved on 8 July 2015 from: http://www.extremetech.com/extreme/179556-teslas-model-s-can-be-located-unlocked-and-burglarized-with-a-simple-hack.

[A32] Lehmann, Keith. *BMW Hack Exposes Connected Car Vulnerabilities.* Connected Car Council. (February 6, 2015). Retrieved on 29 June 2015 from: http://www.cthreereport.com/bmw-hack-exposes-connected-car-vulnerabilities/.

[A33] SBD Consultancy. *BMW ConnectedDrive Vulnerability Analysis.* (July 22, 2015). Retrieved on 29 June 2015 from: http://www.sbd.co.uk/bmw-connecteddrive-vulnerability-analysis/.

[A34] Valiance, Chris. *Car Hack Uses Digital-Radio Broadcasts to Seize Control.* BBC.co.uk. (July 22, 2015). Retrieved on 19 August 2015 from: http://www.bbc.co.uk/news/technology-33622298.

[A35] Whittaker, Zack. *Why Chrysler's Car Hack 'Fix' Is Staggeringly Stupid.* ZDnet.com. (July 27, 2015). Retrieved on 19 August 2015 from: http://www.zdnet.com/article/chryslers-response-to-car-hack-was-slow-and-incredibly-stupid/.

[A36] Osborne, Charlie. *OwnStar: Unlock and Track ANY GM OnStar Connected Car for $100.* ZDnet.com. (July 30, 2015). Retrieved on 19 August 2015 from: http://www.zdnet.com/article/ownstar-the-gm-onstar-connected-cars-worst-security-nightmare/.

[A37] Osborne, Charlie. *Regulators Left in Dark Over Chrysler Security Flaw for 18 Months.* ZDnet.com. (August 6, 2015). Retrieved on 19 August 2015 from: http://www.zdnet.com/article/regulators-left-in-dark-over-chrysler-security-flaw-for-18-months/.

Stuxnet

[A38] Byres, Eric J. *Cyber Security and The Pipeline Control System.* Pipeline & Gas Journal. Pages 58-59. (February 2009). Retrieved on 17 September 2015 from: https://www.tofinosecurity.com/sites/default/files/Cyber_Security_and_The_Pipeline_PGJ_Feb_2009.pdf.

[A39] De Falco, LTC Marco. *Stuxnet Facts Report. A Technical and Strategic Analysis.* NATO Cooperative Cyber Defense Centre of Excellence (NATO CCD COE). (Published 2012). Retrieved on 17 September 2015 from: https://ccdcoe.org/multimedia/stuxnet-facts-report-technical-and-strategic-analysis.html (landing page) and report: https://ccdcoe.org/sites/default/files/multimedia/pdf/Falco2012_StuxnetFactsReport.pdf.

Globalstar

[A40] Zetter, Kim. *Hackers Could Heist Semis by Exploiting This Satellite Flaw.* Wired.Com/ Wired Magazine. Condé Nast. (July 30, 2015). Retrieved on 19 August 2015 from: http://www.wired.com/2015/07/hackers-heist-semis-exploiting-satellite-flaw/.

Ordinary Car Theft

[A41] Zetter, Kim. *Researchers Crack Keeloq Code for Car Keys.* Wired.Com/ Wired Magazine. Condé Nast. (August 24, 2007). Retrieved on 17 September 2015 from: http://www.wired.com/2007/08/researchers-cra/.

[A42] Naone, Erica. *Car Theft by Antenna.* MIT Technology Review. (January 6, 2022). Retrieved on 8 July 2015 from: http://www.technologyreview.com/news/422298/car-theft-by-antenna/.

[A43] O'Carroll, Lisa. *Scientist banned from revealing codes used to start luxury cars: High court imposes injunction on Flavio Garcia, who has cracked [Megamos Crypto] security system of cars including Porsches and Bentleys*. (July 26, 2013). Retrieved on 17 September 2015 from: http://www.theguardian.com/technology/2013/jul/26/scientist-banned-revealing-codes-cars.

[A44] Verdult, Garcia & Ege. *Dismantling Megamos Crypto: Wireless Lockpicking a Vehicle Immobilizer.* (Intended for Publication at USENIX Conference, August 2013 ; Suppressed by Court Order). Retrieved on 17 September 2015 from: https://www.usenix.org/sites/default/files/sec15_supplement.pdf.

[A45] Dryfhout, Brian. *Thieves Caught on Camera Using Mystery Device to Unlock Vehicles.* National Insurance Crime Bureau (Blob). (March 11, 2015). Retrieved on 8 July 2015 from: http://www.nicbblog.org/2015/03/11/thieves-caught-on-camera-using-mystery-device-to-unlock-vehicles/. See also embedded video at: https://www.youtube.com/watch?v=oqYJi6DV21A.

[A46] Dryfhout, Brian. *Caught on Camera: Electronic Device Used to Unlock Truck.* National Insurance Crime Bureau (Blob). (June 9, 2015). Retrieved on 8 July 2015 from: http://www.nicbblog.org/2015/06/09/caught-on-camera-electronic-device-used-to-unlock-truck/. See also embedded video at: http://www.kmph.com/category/170789/video-landing-page?autoStart=true&topVideoCatNo=default&clipId=11579656.

[A47] Metropolitan Police. *Drivers Urged to Protect Vehicles Against Keyless Theft.*. (February 3, 2015). Retrieved on 8 July 2015 from: http://content.met.police.uk/News/Drivers-urged-to-protect-vehicles-against-keyless-theft/1400029791185/1257246745756.

Other

[A48] Barisani, Andrea and Bianco, Daniele. Hijacking RDS-TMC Traffic Information signal (Blackhat August 1- 2, 2007). Retrieved on 29 October 2015 from: https://www.blackhat.com/presentations/bh-usa-07/Barisani_and_Bianco/Presentation/bh-usa-07-barisani_and_bianco.pdf and http://dev.inversepath.com/download/rds/blackhat_df-whitepaper.pdf

16.9 [LR] Set of Legislative, Political and Regulatory Resources

Although a logical extension of the UCSD / University of Washington 2010 / 2011 work of [A01] [A02], Miller and Valasek's 2013 "Adventures in Automotive Networks and Control Units" [A03] resulted in significantly more media attention than the preceding works and also caught the attention of Senator Edward J Markey (D-Massachusetts).

Markey used his office to write to 20 major automobile manufacturers with a detailed series of questions on how the address cyber security and privacy issues in their vehicles, announced this action with a press release [LR01], and made the letters publicly available. The letters ask a series of questions about how manufacturers prevent, detect and respond to cyber incidents and how they intend to use data from telematics units.

The press [LR01] release may be skipped; however, as an exemplar of one of those letters [LR02] the Letter to Volvo Cars of North America is very highly recommended reading.

[LR01] Senator Edward J Markey (D-Massachusetts), Press Release, *As Wireless Technology Becomes Standard, Markey Queries Car Companies about Security, Privacy.* (December 2, 2013). Retrieved on 22 July 2015 from: http://www.markey.senate.gov/news/press-releases/as-wireless-technology-becomes-standard-markey-queries-car-companies-about-security-privacy.

[LR02] Markey, Senator Edward J., [*Letter to Volvo Cars of North America]*, (December 2, 2013). Retrieved on 22 July 2015 from: http://www.markey.senate.gov/imo/media/doc/2013-12-2_Volvo.pdf.

Approximately 15 months after querying those 20 automobile manufacturers, Markey released a paper [LR03] based on those responses received. Some of the conclusions drawn in the paper were that 100% cars have a potentially exploitable wireless attack surface; most manufacturers are unaware and/ or unable to report on past hacking incidents; security measures to prevent remote access to vehicle electronics are haphazard; and only two (of the respondent) automobile manufacturers were able to describe capabilities to diagnose or meaningfully respond in real time to network intrusions; and, that the report further notes that the responses to network intrusion lacked certain credibility.

The "Tracking and Hacking" [LR03] paper was released in the run up to Senate Commerce Committee hearings on "The Internet of Things" where Senators Markey and Blumenthal intended to introduce the "Security and Privacy in Your Car Act of 2015" or "SPY Car Act".

The [LR03] Tracking & Hacking report and the [LR03] press release should be quickly skimmed.

[LR03] Senator Edward J Markey (D-Massachusetts), (February 2015), *Tracking & Hacking: Security and Privacy Gaps Put American Drivers at Risk*. Retrieved on 22 July 2015 from: http://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf.

[LR04] Senator Edward J Markey (D-Massachusetts), Press Release, *Markey, Blumenthal To Introduce Legislation to Protect Drivers from Auto Security and Privacy Vulnerabilities with Standards and "Cyber Dashboard".* (February 11, 2013). Retrieved on 22 July 2015 from: http://www.markey.senate.gov/news/press-releases/markey-blumenthal-to-introduce-legislation-to-protect-drivers-from-auto-security-and-privacy-vulnerabilities-with-standards-and-cyber-dashboard.

[LR05] Greenberg, Andy. *Hackers Remotely Kill a Jeep on the Highway -- With Me in It.* Wired Magazine. Condé Nast. (Published 21 July 2015). Retrieved on 18 August 2015 from: http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

[FN] [Distribution packs may include both web pdf download and MS Word capture of text]

[LR06] Senator Edward J Markey (D-Massachusetts), Press Release, *Sens. Markey, Blumenthal Introduce Legislation to Protect Drivers from Auto Security, Privacy Risks with Standards & "Cyber Dashboard" Rating System.* (July 21, 2015). Retrieved on 22 July 2015 from: http://www.markey.senate.gov/news/press-releases/sens-markey-blumenthal-introduce-legislation-to-protect-drivers-from-auto-security-privacy-risks-with-standards-and-cyber-dashboard-rating-system.

[LR07] On July 21, 2015, Markey did introduce the SPY Car Act [LR07], which was announced in press release [LR06]. These releases were coordinated with the release of an article [LR05] by Wired reporter Andy Greenberg on Miller and Valasek's ongoing works { [A04] and the then yet to be published [A05] }. The [LR05] article is highly recommended reading. The press release [LR06] need not be reviewed.

The press release announcing the introduction of the SPY Car Act summarizes the legislation as, requiring that wireless access points in cars be "protected" against hacking attacks and "evaluated" using penetration testing; collected information be "appropriately" secured and encrypted to prevent unauthorized access; and, that automotive manufacturers or "third-party" feature providers be able to detect, report and respond to real-time hacking events.

In addition, the Act would "call for new cars to be evaluated by a rating system—a 'cyber dashboard'—that informs consumers about how well the vehicle protects drivers beyond those minimum standards. This information will be displayed on the label of all new vehicles – just as fuel economy is today."

There is very little substance in this proposed legislation. A review of the Act [LR07] is not recommended.

United States. Cong. Senate, *Security and Privacy in Your Car Act (SPY Car Act,* 114th Cong. 1st sess. S. 1806. Washington. GPO. Introduced on July 21, 2015. Sponsors Markey and Blumenthal. Retrieved on 18 August 2015 from: https://www.congress.gov/114/bills/s1806/BILLS-114s1806is.pdf.

[Track Legislation Here: https://www.congress.gov/bill/114th-congress/senate-bill/1806]

[LR08] The Chairman and Ranking Member of the US House of Representatives Committee on Energy and Commerce, et al., [*Committee Leaders Seek Information on Auto Cybersecurity]*, *Press Release,* (May 28, 2015). Retrieved on 24 July 2105 from: http://energycommerce.house.gov/press-release/committee-leaders-seek-information-auto-cybersecurity.

[FN] [Links to all letters can be found here: http://energycommerce.house.gov/letter/letters-nhtsa-and-automobile-manufacturers-regarding-auto-cybersecurity

[LR09] The Chairman and Ranking Member of the US House of Representatives Committee on Energy and Commerce, et al., [*Letter to Administrator NHTSA],* (May 28, 2015*).* Retrieved on 24 July 2105 from: http://energycommerce.house.gov/sites/republicans.energycommerce.house.gov/files/114/Letters/20150528NHTSA.pdf.

[LR10] The Chairman and Ranking Member of the US House of Representatives Committee on Energy and Commerce, et al., [*Letter to Volvo Cars North America],* (May 28, 2015*).* Retrieved on 24 July 2105 from: http://energycommerce.house.gov/sites/republicans.energycommerce.house.gov/files/114/Letters/20150528Volvo.pdf.

On May 28, 2015, the House of Representatives Committee on Energy and Commerce publicized their own investigation of automotive cyber security. The press release [LR08] from committee chairman Fred Upton's office need not be reviewed.

However, the letters to NHTSA [LR09] and the automobile manufacturers [LR10] are highly recommended reading. These letters demonstrate a greater understanding of vehicle cyber security issues than evidenced in [LR02]; the questions themselves are important to understanding how legislators are starting to grapple with this serious issue and how the responsibility of manufacturers (to be proactive) is contrasted with the actions of regulators (which are typically reactive).

16.10 [VN] Set of TECHNICAL Resources on CAN, J1939 and related

[VN01] "Diagnostics and Prognostics for Military and Heavy Vehicles" (2004) is one of the very rare papers to consider military and/or heavy vehicle networks. This paper covers the *"who, what, where, when why and how "* of vehicle networks. Some of the information of standard protocols is now dated with respect to new vehicles (although it is certainly still applicable to many vehicles still on the road). Nevertheless, this paper [VN01] presents one of the most accessible narrative overviews of the topic and is recommended reading.

Boys, Robert, *Diagnostics and Prognostics for Military and Heavy Vehicles.* A paper presented at the National Defense Industrial Association, 4th Intelligent Vehicle Systems Symposium, (June, 2004). Retrieved on 22 July 2015 from: http://www.dgtech.com/pdfs/techpapers/ndia.pdf.

[VN02] "Standards and 'Coopetition" provides an accessible narrative of how standards have evolved to meet the needs of heavy vehicles. The content is complementary to [VN01] and [VN02] is therefore also recommended reading.

SAE International, *Standards and 'Coopetition'.* SAE Off Highway Engineer Magazine, October 2008, pp66-69. Retrieved on 2 September 2015 from: http://www.dgtech.com/pdfs/IndustryNews/hdutystandards_dgtech1008.pdf.

[VN03] Boys, Robert. *CAN: Controller Area Network Introduction and Primer.* Dearborn Group Technology (September, 2004). Retrieved on 22 July 2015 from: http://www.dgtech.com/pdfs/techpapers/ndia.pdf.

[VN04] SAE International, *The SAE J1939 Communications Network: An overview of the J1939 family of standards and how they are used.* SAE Off Highway Engineer Magazine, October 2008, pp66-69. Retrieved on 2 September 2015 from: http://www.sae.org/misc/pdfs/J1939.pdf.

[VN05] SAE International. [Web listing of the Core J1939 Standards, Related Standards and Tools]. Retrieved on 2 September 2015 from: http://www.sae.org/standardsdev/groundvehicle/j1939a.htm.

[VN06] Vector Informatik GmbH, *Networking Heavy-Duty Vehicles Bases on SAE J1939*. (Technical Article, Last Revised September, 2008). Retrieved on 2 September 2015 from: http://vector.com/portal/medien/cmc/press/PON/J1939_ElektronikAutomotive_200809_PressArticle_EN.pdf.

[VN07] Vector Informatik GmbH, *Introduction to J1939.* (Application Note, April 27, 2010). Retrieved on 2 September 2015 from: http://vector.com/portal/medien/cmc/application_notes/AN-ION-1-3100_Introduction_to_J1939.pdf.

[VN03] through [VN07] references provide accessible technical detail in narrative form on the CAN (OSI Layer 1 & Layer 2) standard protocol and the J1939 family of standards that incorporates CAN and implements network (OSI Layer 3) and application (OSI layer 7) logic. Relevant information from [VN03] should already be familiar to the reader. [VN04] is recommended reading. [VN05], [VN06] and [VN07] provide additional, optional detail.

[VN08] Craig, Jeff. *Comparison of Automotive and J1939 Diagnostics.* [Vector Informatik GmbH] (Presentation slides). (October, 2008). Retrieved on 2 September 2015 from: http://www.testing-expo.com/usa/08conf/pdfs/day_1/15_VectorCANtech_Jeff%20Craig.pdf.

[VN09] Craig, Jeff. *Comparison of J1939 & ISO 150031.* [Vector Informatik GmbH] (Presentation slides). (September, 2009). Retrieved on 22 August 2015 from: http://www.sae.org/events/training/symposia/obd/presentations/2009/d2jeffreycraig.pdf.

The [VN08] and [VN09] references present various mapping of past, present and future (*work in progress/ proposed*) standards behind ODB-II (light vehicles) with J1939 (medium and heavy duty trucks) and J1939 with ISO 15031 (primarily for light vehicles). His includes network, messaging, physical OBD ports and ECU access (diagnostics and reprogramming). The work done by the author of these references has been an important resource in our analysis for this paper. Due to the complexity and summary presentation, these resources [VN08] and [VN09] are not recommended for the general reader.

[VN10] "Vehicle Networks: CAN-based Higher Layer Protocols" is a slide deck from a university lecture on vehicle networks. CAN, as an OSI Layer 1 and 2 (physical and data link) standard, is used to transport many different Higher Layer Protocols (HLP) to implement (Layer 7) applications. This point has been made elsewhere in both the paper and other [VN##] references. However, [VN10] does help reinforce the idea of HLP over CAN and references vehicle network communication standards not discussed in any significant detail in this paper whilst doing so. Further review of this document [VN11] is not recommended for the general reader.

Strang, Thomas; Röckl, Matthias; *Vehicle Networks: CAN-based Higher Layer Protocols.*(Slide / Lecture on Vehicle Networks 2008/9). Retrieved on 2 September 2015 from: http://www.sti-innsbruck.at/sites/default/files/courses/fileadmin/documents/vn-ws0809/03-vn-CAN-HLP.pdf.

[VN11] *FMS [Fleet Management Standard]-Standard Description Version 03*. (September 14, 2012). The FMS is a standard developed to isolate, at least in part, the internal CAN bus from telematics devices. FMS was developed by European manufacturers Daimler, Man, Scania, Volvo, Renault, Iveco, DAF and VDL. Implementation is unclear. At one level FMS appears to be a gateway, translating high level messages between the vehicle CAN bus and the FMS connector to which telematics devices should be attached.

Page 13 of the document concerns J1939 communications. We could not conclusively determine from this document, but it appears that FMS can enable, block or selectively permit messages passing to and from the J1939 bus. Initially we believed that FMS vehicles might have a reduced attack surface. However, current instinct is that the differential is minor. Further review of this document [VN11] is not recommended for the general reader.

FMS [Fleet Management Standard]-Standard Description Version 03. (September 14, 2012). Retrieved on 22 July 2015 from: http://www.fms-standard.com/Truck/down_load/fms_document_ver03_vers_14_09_2012.pdf .

[VN12] Hodac, Ivan. *Subject: CAN bus connection.* (Brussels, 14 October 2004). [Unsigned Letter from European automotive and truck manufacturers association ((ACEA) Secretary General Hodac]. This document is the first we have identified as highlighting the potentially serious problems of allowing devices to connect to the CAN bus. And, it happens to also be specific to heavy trucks.

> *... electronic systems in ... trucks ... govern most of the functionalities. ... the main European truck manufacturers ... have agreed a common standard (FMS-Standard) for the communication between the truck electronics and on-board computers used to retrieve ... data [from the vehicle electronics].*
>
> *... Direct connection to the CAN bus ... is not allowed ... could be extremely dangerous .. interfere with functionality of truck systems, for example engine or brakes.*
>
> *... the truck manufacturer shall not be subject to product liability arising from any direct CAN bus connection made by a third party.*

The above quotes contain the relevant information from [VN12]. No further review of this document [VN12] is necessary.

Hodac, Ivan. *Subject: CAN bus connection.* (Brussels, 14 October 2004). [Unsigned Letter from European automotive and truck manufacturers association ((ACEA) Secretary General Hodac] [Published on Fleet Management System Official Web Site in context that suggests the letter was issued]. Retrieved on 22 July 2015 from: http://www.fms-standard.com/Bus/down_load/letter_acea.pdf.

[VN13] WWH-OBD - made simple. World Wide Harmonized OBD refers to the ongoing efforts to define global standards for OBD communications. As we have seen in these previous resources and this paper, the vehicle networks and the legislated OBD requirements tend to evolve cooperatively. The i*n process* work requested by the United Nations for a relevant global Technical Regulation (GTR) is to be specified as the ISO 27145 standard. ISO 27145 will incorporate standards we have not actively discussed such as Uniform Diagnostic Services (UDS) and diagnostics over Internet Prototol (IP) networks. Cyber security can only be effective if it is integrated at the start of a design cycle. We do not know to what degree these future standards will respect that design imperative. No further review of this document [VN13] is necessary.

Vector Informatik GmbH, *WWH-OBD - made simple.* (Technical Article, September, 2012). Retrieved on 22 July 2015 from: http://vector.com/portal/medien/cmc/application_notes/AN-ION-1-3100_Introduction_to_J1939.pdf.