Medium and Heavy Duty Electric Vehicle and Charging Infrastructure Cyber Security Baseline Reference Document

May 30, 2018
Version 1.2.1

Prepared by

National Motor Freight Traffic Association, Inc.
1001 N. Fairfax Street
Suite 600
Alexandria, Virginia 22314

GRIMM
2001 6st Street S
Arlington, Virginia 22204

USDOT/Volpe Center
Advanced Vehicle Technology Division
55 Broadway
Cambridge, MA 02142

U.S. Department of Transportation
John A. Volpe National Transportation Systems Center

Disclaimers

Permission is hereby granted, free of charge, to any person obtaining a copy of this work, to make fair use of this work, specifically to copy this work for limited and transformative purposes, limited to commenting upon, or criticizing this work, and to permit persons to whom the work is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the work and that the above copyright notice(s) is referenced in derivative works.

Except as contained in this notice, the name of National Motor Freight Traffic Association, Inc. shall not be used in advertising or otherwise to promote the sale, use or other dealings in this work without prior written authorization of National Motor Freight Traffic Association, Inc.

THIS WORK IS PROVIDED BY NATIONAL MOTOR FREIGHT TRAFFIC ASSOCIATION, INC. "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL NATIONAL MOTOR FREIGHT TRAFFIC ASSOCIATION, INC. BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS WORK, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The information contained in this document is subject to change without notice. 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.

This report was prepared as an account of work sponsored by National Motor Freight Traffic Association, Inc. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

Trademarks

ClassIT, NMFC, SCAC, and National Motor Freight Classification are registered trademarks of the National Motor Freight Traffic Association, Inc. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

[PAGE INTENTIONALLY LEFT BLANK]

TABLE OF CONTENTS

[PAGE INTENTIONALLY LEFT BLANK]

1 Introduction

1.1 The Beginning

NMFTA is a nonprofit membership organization headquartered at 1001 North Fairfax Street, Suite 600, Alexandria, VA 22314. Its membership is comprised of more than 500 motor carriers operating in interstate, intrastate, and foreign commerce primarily specializing in the transportation of less-than-truckload (LTL) quantities of freight. NMFTA's mission is to promote, advance and improve the welfare and interest of its members and the motor carrier industry in general. NMFTA presents its members' positions in relevant judicial, regulatory and legislative proceedings. NMFTA's members operates fleets ranging in size from just a few vehicles to thousands of straight trucks, tractor, and trailers. The NMFTA Heavy Vehicle Cyber Security Program takes an active industry role in vehicle cyber security to ensure the safety and operations of our member's fleets.

On November 29-30, 2017, the U.S. Department of Energy's (DOE) Office of Policy (OP), in collaboration with DOE's Vehicle Technology Office (VTO), the U.S. Department of Homeland Security's (DHS) Science and Technology Directorate (S&T) Cyber Security Division (CSD), and the U.S. Department of Transportation's (U.S. DOT) John A. Volpe National Transportation Systems Center (Volpe) held a technical meeting on key aspects of electric vehicle (EV) and electric vehicle supply equipment (EVSE) cyber security with a large group of stake holders across multiple industries.

One of the problems identified during the meeting was the lack of a practical baseline document to educate all of the disparate stakeholders and interested parties on each other's domains and cyber security issues and concerns. An additional issue was understanding of and representation from the heavy vehicle industry that has different use cases and concerns for electric vehicles, especially Class 7 and 8 trucks. The usage patterns and requirements for commercial heavy trucks are very different from automotive. Another highlight from the meeting was discovering the need to explore current and future research for cyber security principles, risks/threats, and best practices for electric vehicles and electric vehicle charging stations.

1.2 Document Objectives

Motor freight transportation is a critical industry that keeps many other industries and modern conveniences of life working. The effects and risks of compromise at a large scale of the motor freight industry can cause widespread systemic and societal issues. To highlight a few examples: gas stations wouldn't be able to provide gas; grocery stores wouldn't be able to provide goods; clean water would become unavailable in large cities if the water treatment chemicals upon which they rely stop flowing. It is therefore important for us all to seriously consider the security of the motor freight transportation industry when considering the electrification of heavy vehicles.

This paper will attempt to provide a baseline reference document for understanding the issues surrounding electric heavy vehicle cyber security. The scope of this paper includes vehicles, charging stations and their ties to utility companies, and Building Energy Management Systems (BEMS). We have gathered information from many sources, including interviewing companies with established processes, and discussions with research and development groups on the progression of technology with respect to cyber security in this industry. This document also provides as survey of existing security measures, ongoing research and standards development, and attempts to identify topics that need to be

addressed by future work as well as to provide some common sense recommendations on how to improve the current security posture.

There is a significant existing body of work in many of the individual areas covered within this paper. Rather than re-present this information in its entirety to a reader who is already familiar with the subject, we have assumed a baseline of knowledge from which to expand. Attached as appendices to this document are the ***DOE/DHS/DOT Volpe Technical Meeting on Electric Vehicle and Charging Station Cybersecurity Report*** and ***A Survey of Heavy Vehicle Cyber Security*** by National Motor Freight Traffic Association, Inc. These documents are provided as a reference and for a deeper dive on certain topics.

1.3 Heavy Vehicle Cyber Security Overview

The heavy trucking industry is in a period of great technological shift. Mechanical devices in heavy trucks are being supplemented and replaced by integrated Electronic Control Units (ECUs). These ECUs are networked together using a Controller Area Network Bus (CAN bus), which allows them to communicate with each other. These ECUs help the vehicle run more efficiently, and one family of sensors known as Advanced Driver Assistance Systems (ADAS) are enabling automation and active safety functionality. Additionally, freight carriers are augmenting their heavy vehicles with new communications systems, known as telematics, to enhance fleet management capabilities. New technologies such as telematics and ADAS are leading to a safer, cleaner, and more efficient trucking industry. However, these new technologies also come with cyber security risks such as the ability of an attacker to access critical vehicle systems through an unsecure telematics device. Heavy trucks are especially vulnerable to internal network attacks due to the commonality of their internal network communications. The J1939 communications standard for heavy trucks was created to allow the many components from different manufacturers found in the modern heavy truck to work together. Security researchers are increasingly interested in light passenger vehicle and heavy vehicle cyber security; over the past few years these vehicles have become highly publicized targets.

Heavy Vehicles today are complex machines that contain multiple Embedded ECUs, networks to support these units, and a host of external interfaces, both wired and wireless. Wired interfaces to the heavy vehicle most often includes an on-board diagnostic port, but also includes USB, Compact Disk (CD), and SD cards. Wireless interfaces can include Bluetooth, Wi-Fi, Proprietary Radio Frequency (RF) networks, Dedicated Short Range Communications (DSRC), Near Field Communications (NFC), Global System for Mobile Communications (GSM)/Code Division Multiple Access (CDMA), Satellite Communications, and cellular (3G, 4G, LTE, etc.). The wireless interfaces can be used to support features such as telematics for scheduling, navigation, diagnostics, etc. and the Tire Pressure Monitoring System (TPMS). Other systems that will be appearing in the near future will be Vehicle to Vehicle (V2V) communications and communication with the world around it (V2X), and in the not too distant future, autonomous driving. These new systems promise to offer tremendous benefits for efficiency, comfort, and driving safety. The continuing trend in vehicle architecture is a shift from an isolated closed loop structure to more and more open systems which communicate with the world outside of the vehicle.

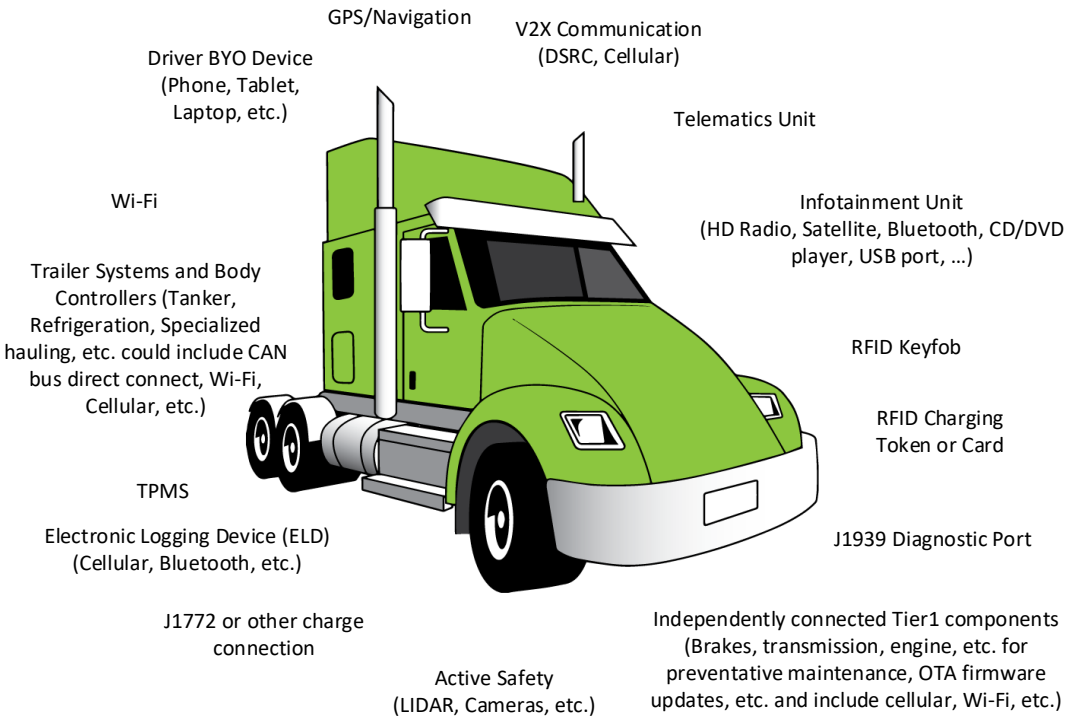


Figure 1 – Heavy Vehicle Communications

Increasing feature sets, interconnectedness with internal and external networks and increasing complexity can also introduce security vulnerabilities that may be exploitable by various adversaries such as "script kiddies"[1], dishonest drivers, criminals/terrorists, corporate espionage, nation states and even the vehicle's owner.

In road transportation scenarios of the not too distant future, breaches made to the security of heavy vehicle information or functions could lead to possible issues for all stakeholders in these four main areas:

Unwanted or unauthorized acquisition of data pertaining to:

- Vehicle or driver activities (e.g. location of vehicle, vehicle routes, navigation destination, etc.)
- Vehicle or driver identity data
- Vehicle cargo manifests and destinations
- Vehicle tuning settings and other carrier specific vehicle data
- Vehicle or sub-system design and implementation (i.e. OEM/supplier proprietary data)

Unwanted or Unauthorized commercial transactions or access to vehicle and cargo

[1] "Script Kiddie" is a term used for unskilled attackers who rely on programs or scripts written by others

Operational interference with:

- On-board non-safety vehicle systems (e.g. infotainment, HVAC, ELD, etc.)
- Telematics communications that may have non-safety impacts on the operational performance of vehicles
- Telematics communications that may have non-safety impacts on vehicle
- Over-the-air firmware updates of both critical and non-critical onboard systems

Safety interference with on-board vehicle systems or telematics communications that may have impact on the safe operation of vehicles

It is important to remember that when a cyber-system is compromised, it still may provide a usable function, even though that function is not the expected one. Compromise of vehicle cyber-controlled systems can occur in many ways, including deliberate cyber security attacks, owners of the system changing default parameters, physical damage to network components, or radio frequency interference.

1.2 Emergence of Electric Vehicles (EVs)

Electric Vehicles (EV) and Plug-In Hybrid Vehicles (PHV) are alternatives to traditional Internal Combustion Engine (ICE) vehicles. Analysis from Bloomberg New Energy Finance suggests that EVs could account for half of all new cars sold by 2040.[2] According to *Global EV Outlook 2017* by the International Energy Agency (IEA), in 2015 the global EV stock had surpassed 1 million vehicles. In 2016, with a growth rate of 60%, that number increased to more than 2 million EVs. This trend continued in 2017 with global sales again reaching above 1 million vehicles, and the market is forecasted to continue along the current growth trajectory. With hundreds of thousands of EVs on the roads in the United States, they are becoming a significant part of the transportation and mobility industry.

During the last few decades, the environmental impact of the petroleum-based transportation infrastructure, along with the fear of peak oil, has led to renewed interest in an electric transportation infrastructure. EVs differ from fossil fuel-powered vehicles in that the electricity they consume can be generated from a wide range of sources, including fossil fuels, nuclear power, and renewable sources such as solar, wind and tidal power or any combination of those. A key advantage of hybrid or plug-in EVs is regenerative braking: the capability to recover energy normally lost during braking as electricity is stored in the on-board battery.

New registrations of EVs hit a new record in 2016, with over 750K worldwide. With a 29% market share, Norway has incontestably achieved the most successful deployment of EVs in terms of market share, globally. It is followed by the Netherlands, with a 6.4% electric car market share, and Sweden with 3.4%. The People's Republic of China, France and the United Kingdom all have electric vehicle market shares close to 1.5%. In 2016, China was by far the largest electric car market, accounting for more than 40% of the EVs sold in the world and more than double the amount sold in the United States.

[2] [T23] Shankleman, Jess, *The Electric Car Revolution Is Accelerating*, Bloomberg News, (06 July 2017). Retrieved 04 May 2018 from https://www.bloomberg.com/news/articles/2017-07-06/the-electric-car-revolution-is-accelerating

1.3 Electric Truck Market

Manufacturers are showing a renewed focus on bringing commercially viable MD/HDEV to market. Fleets have shown interest in the benefits of electrified trucks because of the potential for lower operational costs. However, the ROI has not been proven in many use cases due to the high upfront costs of electrified powertrains and the need to select the right application of the technology. Pressure from governments to reduce pollutants related to diesel fuel combustion and tackle greenhouse gas emissions is pushing manufacturers to invest in developing electrified trucks while low emission zones are driving fleets to replace diesel trucks with cleaner options. The MD/HDEV market has lagged behind the bus market in electric powertrain adoption, but has the potential for growth once the total cost benefits of MD/HDEV ownership can be demonstrated.

In the United States, more than 6% of greenhouse gas emissions emitted in 2015 were from medium duty and heavy duty trucking. Transportation, including trucking, was responsible for 14% of emissions globally in 2010. Because trucks need so much hauling power, they have eluded electrification until recently. A battery that could pull significant weight would itself be too hefty and too expensive, but, improvements in battery technology are paying off in reducing both size and cost. Already buoying passenger car sales, "*the trend is now boosting the EV truck market*", says Lisa Jerram, a principal research analyst for Navigant Research. Electric technology for big, heavy vehicles has also received a boost from smog adverse city governments' investments in electric buses. According to a recent report by Jerram, the number of hybrid-electric and MD/HDEV is set to grow almost 25% annually, from 1% of the market in 2017 to 7% in 2027, a jump from about 40,000 MD/HDEV worldwide to 371,000. China's BYD already has MD/HDEV on the road, while Daimler Mitsubishi's FUSO is expected to be rolling soon. Smaller companies, such as Arrival (UK), Chanje (U.S., China), E_FORCE (Switzerland), Tevva Motors (UK), and Workhorse (U.S.), have launched MD/HDEV in local markets, David Alexander, research director of UK-based Truck Technology Ltd. says, and major truck companies such as Volvo, Scania, MAN (VW) and Navistar are testing prototype MD/HDEV, aiming to bring them to market by 2020.[3]

As for MD/HDEV cyber security concerns, MD/HDEV and their Charging Infrastructure are vulnerable (like their light-passenger EV counterparts), but the kinetic safety impacts (i.e. higher weight) of MD/HDEV crashes is an area of cyber security concern that the DOE/DOT needs to focus on.

1.4 EV Charging Infrastructure and Extreme Fast Charging (xFC)

Technavio's market research analyst predicts the global electric vehicle charger market to grow at a compound annual growth rate (CAGR) of more than 29% during the forecast period of 2016-2020. Attractive incentives for EV chargers and the purchase of EVs are also expected to boost the sales of EVs and attract original equipment manufacturers (OEMs) and private organizations to invest in the development of EV charging infrastructure. Emerging trends such as wireless charging are expected to aid the market growth in the coming years. Wireless technology has become an area of interest for the EV and plug-in hybrid vehicle (PHEV) manufacturers because of its convenience and reduced powering up times. It also helps manufacturers differentiate their products. Wireless charging also facilitates

[3] [C16] Gies, Erica, *Electric Trucks Begin Reporting for Duty, Quietly and Without All the Fumes*, InsideClimateNews, (18 December 2017). Retrieved 03 May 2018 from https://insideclimatenews.org/news/18122017/electric-truck-urban-package-delivery-ups-tesla-semi-daimler-byd-china-battery

"charging on the go". For instance, in Gumi, South Korea, electric buses are charged through in-road wireless chargers.

Today's major EVSE vendors, like ABB, ChargePoint, and others are designing and building charging stations for MD/HDEV that require higher power levels in the 300kW to 1M Megawatts (MWs) range. High power charging events could have an impact on the electric grid stability and reliability, and there are obvious cyber security concerns.

Extreme Fast Chargers (xFC) will be transferring 300kW- 1MWatts. Medium and heavy duty electrified vehicles, especially over-the-road tractor-trailers, will likely require a charging infrastructure with charge rates of 1MW or higher. These vehicles will have significantly larger batteries than light-duty passenger EVs and require much longer ranges. With power transfer rates of 1MW and higher, it is anticipated that automated charging, whether conductive or inductive, will be required to eliminate safety concerns with vehicle operators handling the recharging equipment. Power levels over 100kW will likely not be inductive due to the levels of losses. It will likely be conductive, but it is not clear at this time how that will be transferred. ChargePoint in collaboration with Uber recently announced a prototype 1MW connector. It is aimed initially at the VTOL aircraft charging application but could be used for heavy vehicle charging. Since the vehicles themselves are still in the development stage, charging equipment manufacturers may be reluctant to invest in the research needed to develop the hardware and control systems that will be required for these 1MW+ chargers.

1.5 Electric Bus Market

Electric Buses operate with a SAE 1939 CAN bus, so they have similar cyber security vulnerabilities to MD/HD trucks. Technavio's market research analyst predicts that the global electric bus market will grow at a CAGR of close to 27% (in terms of units shipped) during the forecast period of 2016-2020. The global electric bus market is primarily dominated by five major vendors who continually compete to gain maximum market share. Key vendors in the market are: New Flyer, Volvo, Novabus, Gillig, BYD, Ebus, Proterra, Wuzhoulong and Yutong. One of the key focus areas for electric bus OEMs is working with state and city government agencies. For example, Seattle's Metro Transit has ordered 120 electric buses, which is the largest purchase of its kind in the nation to date. Metro Transit released a plan to transition its entire fleet to electric buses by 2034.[4] The market is also characterized by rapid innovation and the development of advanced buses to meet the needs of specific regions.[5]

[4] [T20] Gannon, Rob, *With some all-electric buses, Metro Transit rides into the future*, The Seattle Times, (02 October 2017). Retrieved 03 May 2018 from https://www.seattletimes.com/opinion/with-some-all-electric-buses-metro-transit-rides-into-the-future/

[5] [T21] Technavio, *Global Electric Bus Market 2016-2020*, published by Technavio, (April 2016). Retrieved 03 May 2018 from https://www.technavio.com/report/global-automotive-manufacturing-electric-bus-market?utm_source=T5&utm_medium=BW&utm_campaign=Media

1.6 Cyber Security Considerations for MD/HDEV

In addition to the traditional components encountered in Internal Combustion Engines (ICEs) vehicle, such as the Controller Area Network (CAN), telematics, infotainment, RF, cellular communications, TPMS, GPS, etc., MD/HDEV present several "unique" challenges in regards to cyber security. Unlike their traditional counterparts, when an MD/HDEV refuels they are both physically and electronically connected to and exchange information with Electric Vehicle Supply Equipment (EVSE), which in many cases is also connected to the Power Grid and may be connected to a BEMS, and these are all connected to the Internet. While there are standards for the communications between the vehicle and the grid, such as SAE J2836, "*Use Cases for Communication Between Plug-in Vehicles and the Utility Grid*"[6], and SAE 2931/7, "*Security for Plug-In Electric Vehicle Communications*"[7]. IEC/ISO 15118 is a competing standard that is also worth reviewing. Further work is needed to ensure that the cyber security integrity of both the EVSE and the MD/HDEV are not compromised.

Mr. Hina Chaudhry, who supports the SAE J2931-7 Security for Plug-In Electric Vehicle Communications Standard Committee stated: *"The most important element to test are EVSEs and the network that will carry the communications (e.g. demand response, price charging, authentication and authorization) between EVSE, utility and other connected devices like CEMS, smart meters, etc. If the malware/attacks can be propagated from one node to other node (e.g. EVSE), it will be matter of time before all the nodes are compromised. It will be early at this stage, but inclusion of Advanced Persistent Threat (APT) from State Actors/Nations should be considered as well."*

Listed below are some attacks that pertain to MD/HDEVs:

- **MITM (Man In the Middle) attack at charging station** - Attacker inserts themselves between the MD/HDEV and the EVSE leading to possible tracking issues, monetary issues, and other privacy issues
- **Money from credit card fraud** at charging station
    - The charging cycle does not last the full amount of time paid for
    - The charger is spoofed into providing free service
    - The charger sends credit card information to unauthorized party
- **Privacy/tracking issues** with using EVSEs linked into Smart Grid
- **Intentional overcharging of batteries** via a cyber security attack causing possible severe damage to batteries/EV and surroundings
- **Intentional discharging of batteries** causing the MD/HDEV being taken out of service/degrading range
- **Denial of Service (DoS) attack at EVSEs** - Taking vehicles out of service if unable to re-charge

[6] [P08] Hybrid Committee, *Use Cases for Communication Between Plug-in Vehicles and the Utility Grid*, SAE International, Standard J2836/1, (08 April 2010). Retrieved 02 May 2018 from https://www.sae.org/standards/content/j2836/1_201004/

[7] [P09] Hybrid Committee, *Security for Plug-In Electric Vehicle Communications*, SAE International, Standard J2931/7, (15 February 2018). Retrieved 02 May 2018 from https://www.sae.org/standards/content/j2931/7_201802/

- **A malware infected EV** - a vehicular "Typhoid Mary" which passes its malware to other MD/HDEVs via the EVSE
- **Malware infected MD/HDEV** that passes onboard malware through an EVSE to the Smart Grid or networked EVSEs
- **Rapid cycling of heavy loads** to the grid through multiple compromised EVSEs to cause grid failure

1.7 The Evolving Electric Truck

Electrically powered trucks were popular in the early days of commercial self-propelled vehicles (see Figure 2). Quiet operation, ease of use, low maintenance, and tremendous torque that was instantaneously available were the hallmarks of those early vehicles. However, tremendous battery weights, limited range, and long charging times eventually doomed these pioneers.

Figure 2 - Electric Truck circa 1911

Photo credit: Theoldmotor.com

With the advent of new battery technologies combined with super-efficient electric motors and computerized power management systems that addressed the range and charging issues of their predecessors, a new generation of electrically powered trucks are taking to the roads. For some examples of MD/HDEVs see [T07] and [T12].

1.8 MD/HDEV Business Drivers

Cost of Ownership

Manufacturers are showing a renewed focus on bringing commercially viable MD/HDEVs to market. One of the factors in the upswing of MD/HDEVs is the total cost of ownership (TCO). As MD/HDEVs become more mainstream with purchasers being able to select battery size, charging capacity, and other options, the initial cost of an MD/HDEV will come to reflect a broader market as will the infrastructure costs to support the HEV. A 2017 study by Bernd Heid, et al. states that the earliest TCO breakeven point will be seen in the medium average daily distance use case. For an in-depth look at the study on TCOs for MD/HDEVs, see [T11].

Emergence of MD/HDEV Charging Technology

The increase in technology driven aspects of the MD/HDEV, such as Extreme Fast Chargers (xFC) that drastically reduce charging time, new developments in battery technology that allow for greater power density and control electronics will require more sophisticated ECUs throughout the entire EV environment. This is not just on the MD/HDEVs, but also EVSE and BEMS equipment. MD/HDEVs, especially over-the-road tractor-trailers, will likely require a charging infrastructure with charge rates of 1MW or higher. These vehicles will have significantly larger batteries than light duty passenger EVs and require much longer ranges than the 400 kW charging provided by xFC chargers can support.

Emissions

Pressure from governments to reduce pollutants related to diesel fuel combustion and tackle greenhouse gas emissions is pushing manufacturers to invest in developing electrified trucks while low emissions zones are driving fleets to replace diesel trucks with cleaner options. As emissions regulations tighten, especially in urban areas, the lack of typical ICE emissions from an MD/HDEV will allow the MD/HDEV to operate without emissions imposed constraints and/or extra fees. While these types of regulations have not appeared in the US, they are starting to be employed in Europe. In 2008, the London Low Emission Zone (LEZ), which covers most of greater London, was established to reduce the emissions from diesel powered commercial vehicles. Vehicles that do not meet the low emission standards are charged a fee (currently £200 for an HV per day) to operate in the zone. To read more about the LEZ see [T13].

1.9 Electrification Transformation Impacting the Heavy Trucking Market

Businesses and consumers are switching from fossil-fueled vehicles to electric or hybrid vehicles due to benefits that include lower emissions, better fuel efficiency, and over time, lower costs. Electric motors are also found in forklifts, 4-wheelers, and even heavy trucks and super trucks. According to electric automotive enterprise Proterra, the company has already sold 512 buses across 29 states. In addition, UPS has agreed to purchase an initial 50 all-electric truck fleet, with plans of serious growth in 2019. According to UPS, "*there will be a deployment of a 'larger fleet' in 2019 and beyond*. *There's a lot of work to be done since UPS has approximately 35,000 diesel or gasoline trucks on the road*."[8]

1.9.1 Potential MD/HDEV and Charging Infrastructure Cyber Security Impacts

The emergence of MD/HDEV and their associated charging infrastructure will require the US trucking industry to develop mitigations and/or countermeasures and take strategic actions that are unique to the all-electric environment. Listed below are some of the top MD/HDEV cyber security challenges:

Supporting Infrastructure

There will be a need for supporting infrastructure consisting of equipment and software specific to MD/HDEVs, such as EVSEs and interfaces to BEMS, all of which are unique to MD/HDEVs and will need to be considered from a cyber security point of view. In addition, the EV environment extends beyond the confines of the MD/HDEV and facility to the power grid itself.

The "Last Mile"

One of the early areas where MD/HDEVs will become popular is the" last mile," which is known to be the most inefficient and expensive transportation leg, costing upwards of 30% of the total delivery costs. J. Schultz of Logistics Management stated that "*e-commerce sales are expected to reach $2.4 trillion by 2018 and the demand for last mile logistics will grow with that trend*". LTL carriers fill the need for "last mile" services and will be on the frontlines of MD/HDEV adoption. In order to accomplish this, they may need to use multiple charging stations scattered along their routes to avoid having to return to recharge. Each of these stations represents a cyber-attack surface; for example, if the stations are all networked together an attacker could cause largescale outages on the network.

The MD/HDEV and Autonomy

While there is not yet a clear requirement for autonomy, many experts see the MD/HDEV platform as an entry point for advanced platooning and autonomous functionality. In a recent issue of FleetOwner, John Larkin stated "*The key, will be linking electric propulsion with autonomous vehicles. Environmentalists and cost mavens alike may both support MD/HDEV, particularly if they are paired with driverless technology.*"[9] There are numerous articles on the advent of autonomous and platooning vehicles, a few of these are referenced in [T14] through [T18].

---

[8] [T12] Carey, Nick, *UPS partners with Workhorse to build electric delivery vans*, Reuters.com, (22 February 2018). Retrieved 02 May 2018 from https://www.reuters.com/article/us-ups-workhorse-group/ups-partners-with-workhorse-to-build-electric-delivery-vans-idUSKCN1G61S7#_blank

[9] [T22] Kilcarr, Sean, *Navigating the many challenges facing trucking*, FleetOwner.com, (18 April 2017). Retrieved 03 May 2018 from http://www.fleetowner.com/blog/navigating-many-challenges-facing-trucking

The importance of a strong cyber security posture in the areas of platooning and autonomous operation cannot be stressed enough. The same vulnerabilities that exist for ICE HVs and MD/HDEVs will be present, as well as any new attack surfaces created by the addition of platooning and autonomous technologies.

Cyber Security Attacks on Charging and Battery Infrastructure

As the technology for MD/HDEVs (especially Class 7 and 8) matures, the size of the batteries and power rates will substantially increase with a corresponding increase in the power consumption and output of MD/HDEV EVSEs. Today's DCFC Level 3 chargers provide 50-350 KWs and new Extreme Fast Chargers (xFC) will provide 400 kWs or more. However, due to physical limitations of the battery plates the battery voltage will need to be raised to 800 volts allowing for lower (approximately ½) charging current requirements. These higher voltage and current draws will allow an attacker to multiply the effects of any attempt to disrupt the grid through malicious manipulation of the xFC. In addition, an attacker could attempt to cause an xFC to apply more power than an attached non-xFC rated vehicle could handle. For an in-depth report on xFC gap analysis conducted by the DOE, see [T19].

Other Emerging Industry Electrification Markets

Forklifts (manual and robotic), electric powertrains for MD/HDEVs, light inspection vehicles, etc., are also areas for cyber concern. As advances in technology appear in one sector of EVs, they will be incorporated throughout the entire sector. A cyber security attack that renders a facility's forklifts inoperable can be a major event affecting the ability to load and offload trucks. As facilities add/upgrade to their non-truck electrically powered assets, they need to be aware of the cyber security posture of their EVSE. The same related cyber security issues cited in this report for MD/HDEVs are applicable to this level of equipment.

2 Background

Electric vehicles represent a dramatic change to how energy moves around the power-grid, including where loads are connected to the grid and where/when they draw energy from the power-grid. EVSEs represent a relatively new and high-powered load. Each of these components have a specific and different attack-surface, and when pieced together, some of the components can even be used to attack other components. More specifically, communication between the EVs and EVSEs present an interesting attack-surface, particularly since the communication either uses wireless technologies or CAN. Further concerns involve threats to the power-grid due to the action of numerous charging stations and EVs.

2.1 Vehicle Systems Overview (EVs)

ECUs and Control

Electric and Hybrid Vehicles are some of the most advanced vehicles in production today. Like all modern production vehicles, EVs are made up of Electronic Control Units (ECUs), which are simply a computer system that senses, interprets, or controls an aspect of the vehicle. Some ECUs control power-train and charging, and are thus considered safety-critical. Other ECUs provide In-Vehicle Infotainment (IVI) and Telematics functions. The difference between these two types of ECUs is significant: most safety-critical ECUs run a "raw" firmware, meaning the firmware is purpose-built from the ground up. Telematics and IVI ECUs provide higher level functionality, and most often use a high-level Operating System, such as QNX, Linux, Android, or Apple's IOS. This difference affects the way they engage the rest of the vehicle, the ways to attack them, and the ease of finding exploitable bugs.

CAN, LIN and Ethernet (J1939)

EV ECUs work collaboratively in networks and communicate using one of several core network protocols. The most common protocol in use in all vehicles today is called Controller Area Network (CAN). CAN as implemented in vehicles is a differential-signaling bus-type network. It is very resilient to electrical noise, and allows many different peer ECUs to communicate over one set of wires. EVs and other light duty vehicles use a few other communications protocols, most of which are Master/Slave in nature (i.e. one ECU controls several others), such as Local Interconnect Network (LIN).

CAN has been standardized in the heavy truck/machinery industries as SAE J1939, which is basically extended CAN with specific messages and interactions. Typical CAN bus speeds are 125kbps, 250kbps, and 500kbps.

CAN frames can only carry up to 8 data bytes per frame but have low latency which makes it suitable for control systems. In comparison, Ethernet frames carry up to 1514 bytes per frame. In order to overcome this obvious weakness, International Organization for Standardization (ISO) created a standard known as ISO-TP (its formal name is ISO 15765-2), which allows numerous CAN frames to be grouped together to create messages up to 4096 bytes in length. These messages rely on multiple smaller CAN frames, which allow the bus to be used by other ECUs while sending the larger message.

Infotainment and Telematics

Nearly all EVs provide In-Vehicle Infotainment (IVI) and Telematics. IVI systems provide enjoyable traveling experience, including radio and other music playing capabilities, as well as movies and vehicle navigation. IVI and telematics system -- running high level operating systems -- are the most complex, the most connected, and the most well understood ECUs in a vehicle. They represent the most fruitful first level attack-surfaces when considering how to hack a vehicle. IVI systems will often support Wi-Fi,

Bluetooth, and other wireless communications. Telematics systems typically provide Internet over cellular LTE or satellite, which is connected to via both CAN and a Wi-Fi network provided by the Telematics unit. In some vehicles, IVI and Telematics functionality are wrapped into one ECU or set of ECUs. In other vehicles, they are separated, and IVI systems connect to the Telematics-provided Wi-Fi.

Unified Diagnostic Services (UDS)

For many reasons, including emissions control, modern vehicles all must provide Unified Diagnostics Services (UDS). UDS is a standardized mechanism to access and control various aspects of each ECU (only required on power-train ECUs, but UDS is found in many other ECUs as well). UDS provides the ability to modify an ECU's configuration (how a transmission works, how brakes behave, how suspension functions), allow firmware updates, and many other functions including arbitrary reading and writing to ECU internal memory. UDS defines challenge-response authentication messages for diagnostics tools to authenticate before allowing read/write to important system data (including firmware update).

SAE J2534

To allow local mechanics (not just dealerships that are tied to OEMs) to perform diagnostics and firmware updates, SAE standardized the diagnostics physical and datalink layers in a standard called SAE J2534. This standard allows one piece of hardware to provide UDS interface to ECUs from multiple makes and models, keeping the costs lower for small repair shops. J2534 is currently one of the key attack vectors used by attackers to compromise ECUs on the CAN bus.

Security Gateways and Data Diodes

To provide a degree of security in vehicles using CAN messaging, OEMs are segregating ECUs into different CAN buses, connected by a Security Gateway. Some Security Gateways are simply provided between the OBD-II or J1939 diagnostic ports and the rest of the vehicle. Others sit between each different CAN bus and provide security filtering and potentially intrusion detection between networks. This approach allows higher value power-train ECUs to be segregated from riskier IVI and Telematics ECUs, because ECUs, that are more likely to be hacked, often have no need to send "Turn the Steering Wheel" or other important messages.

Insurance companies have started providing discounts to drivers willing to share driving data by plugging in an LTE-connected dongle into the OBD-II port. This dongle transmits speed and acceleration data, along with other data points, back to the insurance company for evaluation. This allows real feedback to the insurance company indicating how much risk is involved in underwriting a given driver.

This new trend, as well as new regulation that requires Electronic Logging Devices (ELDs) for many heavy vehicles, has led to a great deal of attention to security devices known as Data Diodes. Data Diodes allow traffic to traverse in one direction, but not return traffic. These devices allow ELDs and insurance dongles to gather CAN messages, but not transmit them. Data Diodes in theory provide significant protection. However, because CAN cannot be easily turned into a unidirectional communication path, Data Diodes need be tested to ensure efficacy.

Other Security Mechanisms

Automotive security mechanisms have become an active arena for business opportunities. While some existing IT technologies are not applicable, some interesting security mechanisms have been introduced into the automotive space:

Differential Power Analysis is being used to identify individual code-block execution, hoping to identify malicious code patterns once an attacker has taken control of an ECU. While promising, this technology doesn't currently exist in a production ECU, and the question of how well it works in a noisy electrical environment, such as a vehicle, has yet to be proven.

ECU CAN transceiver filtering provides a way for an ECU to provide CAN message white-listing capabilities. This approach is often used to block outbound CAN messages (so the ECU itself won't allow itself to send non-approved messages). While that's polite, if an attacker controls the ECU, that code is often able to be circumvented.

Stakeholders, Culture, and Regulatory Concerns

The automotive industry is largely made up of consumers, OEM's, Suppliers, US Department of Transportation (US DOT) including National Highway Traffic Safety Agency (NHTSA) and many associations and standards bodies such as SAE International (formerly Society of Automotive Engineers) and International Standards Organization (ISO).

> **OEMs** - OEMs are better known as Automotive and Truck manufacturers, for example: Daimler, PACCAR, Navistar, Ford, General Motors, and Chrysler. OEM's are actually "system integrators," issuing design specifications to suppliers who actually build ECUs and subsystems.
>
> **Suppliers** - Work with OEM specifications to build ECUs and other devices and subsystems. The largest suppliers are known as Tier 1 Suppliers.
>
> **NHTSA** - organization within US Department of Transportation responsible for the safety of vehicles on US roadways. Officially responsible for creating and enforcing safety regulations.
>
> **FMCSA –**the Federal Motor Carrier Safety Administration (FMCSA), which is an organization within US DOT and their primary mission is to reduce crashes, injuries and fatalities involving large trucks and buses.

While not regulated in the same way as the Electrical Industry, the automotive industry has a unique culture and set of constraints. In addition to safety regulations and oversight from USDOT/NHTSA, the automotive industry is heavily influenced by two assumed entitlements: "Right to Repair" and "Right to Modify."

The “Right to Repair” comes from a law in Massachusetts that protects the ability of independent garages and vehicles owners to perform maintenance and repairs on vehicles. While this law was ratified in 2012, several similar bills have been proposed in the US Congress since 2001. To date, no US legislation has been ratified, although the Massachusetts law has carried an undertone throughout the US automotive market, such that garages throughout the nation benefit from the outcomes of the law.

Heavy duty vehicles are not covered under the light duty ecosystem. In 2015, the Commercial Vehicle Solutions Network (CVSN) and the Truck and Engine Manufacturers Association (EMA), together with the Equipment and Tool Institute (ETT), the Auto Care Association (AutoCare), and Heavy Duty Aftermarket Canada announced the signing of a “Memorandum of Understanding” (MOU) providing access to heavy duty service information in order to allow fleet owners and operators to service their heavy trucks at the repair shop of their choosing.

The "Right to Modify" is not a law, but rather an expectation by a significant segment of the automotive community that modify vehicles. Reasons for modifying vehicles vary, but typically range from personalization to performance enhancements. So-called "Modders" expect to be allowed to modify a given vehicle with permission from the owner alone - not the OEM or a legislative body. Technological enhancements, including security enhancements, can hinder this ability.

2.2 Charging Stations (EVSEs)

Compared to the power grid and the automotive industry, EVSE is a relatively new technology space. One vendor built well over half the current identified US deployments.[10] Vendors in this space include ABB, ChargePoint, Tesla, Blink Network, EVgo Network, SemaCharge Network, Greenlots, OpConnect, AeroVironment Network, and EV Connect. While most EVSEs have cloud based controlled platforms, some in the industry are moving towards OCPP 1.6, direct uplink into the network operator.

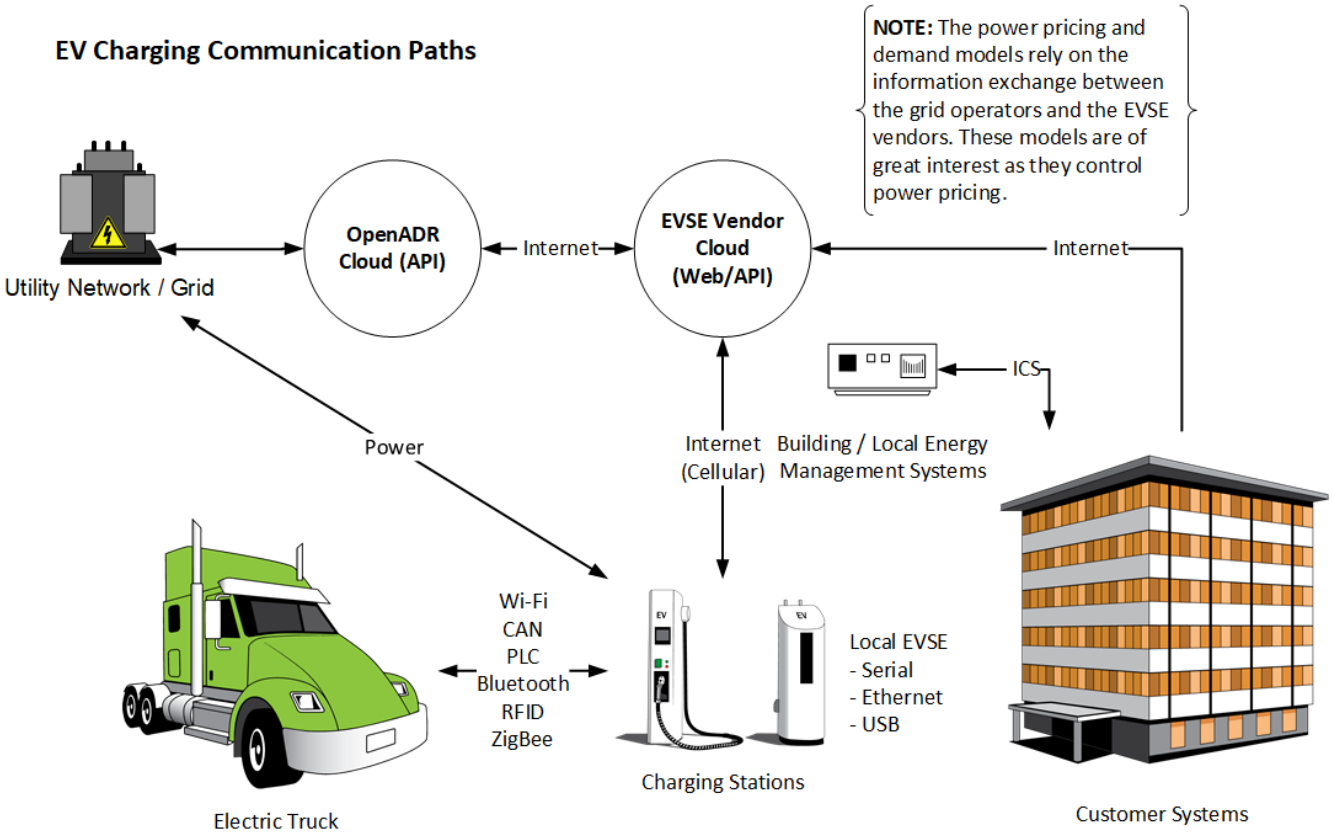


Figure 3 - EV Charging Communication Path Overview

[10] [C14] Wood, E., et al., *National Plug-In Electric Vehicle Infrastructure Analysis*, Office of Energy Efficiency & Renewable Energy, (September 2017). Retrieved 02 May 2018 from https://www.nrel.gov/docs/fy17osti/69031.pdf

High Power, Ranging From 240VAC/30A (US) to 600VDC@400Amps

Many different charging stations exist, ranging from simple residential chargers to commercial chargers that are intended to be used like gas-pumps. Similarly, power available ranges from 240VAC at 16 amps up to 500VDC at up to 125 amps. The value of using Alternating Current (AC) is diminished at higher voltages as power conversion units are heavier, more costly, and throw off more heat, so the industry has migrated to Direct Current (DC) for high power charging.

Types and Modes

When talking about EVSEs, you often hear the terms "Type 2" or "Mode 4". The "Type" refers to the type of connector the EVSE uses to connect to a vehicle. The “Mode” refers to the type of charging voltage and current used.

Four Modes are defined in IEC 61851-1 (and again referenced in IEC 62196-1), each with a different set of electrical characteristics:

Mode 1 - Supports "passive" AC connection of up to 16 amps, basically plugging the battery directly into the AC mains at either 240V Single Phase or 480V Three-Phase.

Mode 2 - Specifies AC but increases the amps to a maximum 32 amps at either 250V (1P) or 400V (3P) and requires the EVSE provide additional functionality like vehicle-detection and over-charge/over-temp protections and safe-wiring protections.

Mode 3 - Builds on Mode 2 and can provide backwards compatibility with Mode 2 vehicles at 32A, but includes active vehicle communication and an increase to 250 amps max.

Mode 4 - Direct Current (DC) using an active connection and allows up to 600VDC at up to 400 amps.

There are currently five different types of connectors (aka "couplers") world-wide, as described in the standard IEC 62196. [11]

Type 1 - Defined in SAE J1772 and included in IEC 62196-2, is a Single-Phase connector and is prevalent in North America.

Figure 4 - Type 1 J1772 Connector

[11] [C01] Wikipedia contributors, *IEC 62196*, In Wikipedia, The Free Encyclopedia, (Last revised 23 April 2018). Retrieved on 26 April 2018 from https://en.wikipedia.org/wiki/IEC_62196

Type 2 - Defined in VDE-AR-E 2623-2-2 and included in IEC 62196-2, is a Single- and Three-Phase connector and has a footprint worldwide.

Figure 5 - Type 2 Connector

Type 3 - Maintained by the EV PlugAlliance, is the first plug with safety-shutters over the electrodes, also providing Single- and Three-Phase connections. This is not a commonly used standard.

Type 4 - Defined in JEVS G105-1993, is a fast charge coupler, known by its industry name CHAdeMO, and is widely used in Japan and Europe. Type 4 couplers use CAN-bus for signaling.

Figure 6 - Type 4 Connector

Combined Charging System (CCS) – This is an attempt to corral all connectors into two: Combo1 for US and Combo2 for Europe. These combined connectors will offer room for Type 1 or Type 2 (respectively) AC wires as well as two DC wires allowing up to 500A. CCS further includes PowerLine Carrier (PLC) signaling for communication between EV and EVSE.[12]

[12] [C02] evcStation, *EV Chargers*, (n.d.). Retreived on 26 April 2018 from http://www.evcstation.com/index.php/extras/ev-chargers

Figure 7 - CCS Connectors

SAE J1772 Signaling

All coupler Types use J1772 signaling except Type 4 (which uses CAN-bus) and CCS (which uses PowerLine Carrier, or PLC). J1772 signaling uses resistance and a 1 KHz square-wave signal to ensure low- or no power is applied to the charging wires unless a vehicle is connected. J1772 is a little more complex but can be compared to the Android and iPhone charging systems, which use resistance and a little intelligence to detect the presence of a system to charge as well as what level of charging to provide. Type 4 and CCS use more active communication methods that provide greater charging functionality as well as additional attack surface. The same signaling is also defined in IEC 81851-1 (Ed3).

CHAdeMO vs. CCS

Type 4 couplers (CHAdeMO) were the first entry to the DC Fast Charging space, providing CAN communications and high power fast DC charging. Current limits for CHAdeMO are 500VDC at up to 125A (soon to be 200A). Unfortunately, CHAdeMO does not support AC charging, so vehicles supporting CHAdeMO must support two different couplers to ensure flexible and easy charging.

CCS, created by the J1772 committee, simply took the J1772 Type 1 connector and added two large pins for DC voltage, also adding PLC support for more intelligent communication between the EVSE and vehicle.

Interesting note, CHAdeMO uses CAN-bus, the most common communications protocol between vehicle systems, while CCS uses PLC, a communications protocol common within some SmartGrid systems (as prescribed in Vehicle to Grid standard ISO 15118).[13]

Wired Charging vs. Wireless Charging

Most deployed charging stations to date use physical wiring to connect the charger to the vehicle, much like a gas pump with a gas-powered vehicle. As EVs and EVSEs mature, ease of charging has become a greater factor, and wireless charging standards have come to light. SAE released J2934 in November 2017, defining wireless charging for up to 11kW charging. For reference, the majority of wired commercial chargers only deliver 3kW.

Wireless chargers provide power through low frequency RF emissions, much like wireless cell-phone chargers and battery-less RFID door key access but at a much greater power level. In addition to the

[13] [C03] Herron, David, *Range Confidence: Charge Fast, Drive Far, with your Electric Car*, GreenTransportation.com, (2016-2017). Retrieved 26 April 2018 from https://greentransportation.info/ev-charging/range-confidence/chap8-tech/ev-dc-fast-charging-standards-chademo-ccs-sae-combo-tesla-supercharger-etc.html

actual power emission, wireless chargers also must communicate with the vehicle for many reasons: The charger needs to know when to begin and stop charging, and it needs to know who to bill. This communication is accomplished using a low power communications mechanism such as Zigbee or Wi-Fi.

Wireless charging would be an important addition to autonomous vehicles. For example, an autonomous taxi will be able to recharge without manual interaction to connect the charger. SAE International is presently working on J2954, which provides recommended practices for wireless charging of light duty plug-in electric vehicles (PEVs).[14] Further references and/or examples can be found in [C04] and [C05].

Embedded Systems

Not unlike other cyber physical systems, EVSEs are composed of embedded systems with a number of electronics components and one or more microcontrollers that handle control of the charging circuits as well as communication with all external systems. For cyber security purposes, the microcontrollers and network communication are the most interesting parts. Interaction with these microcontrollers can be accomplished through several means. Physically removing the panel of the charger is the first method, revealing network components, embedded communications buses, console and debugging ports, and possibly direct access to device storage. The second method is through the charging control protocol, such as CAN, PLC, or the wireless mechanisms used for wireless charging. The third method is to attack the Internet connection or building network interface using standard IP networking or Wi-Fi attacks. Much of the same knowledge required to attack the vehicle transfers to attacking the EVSE.

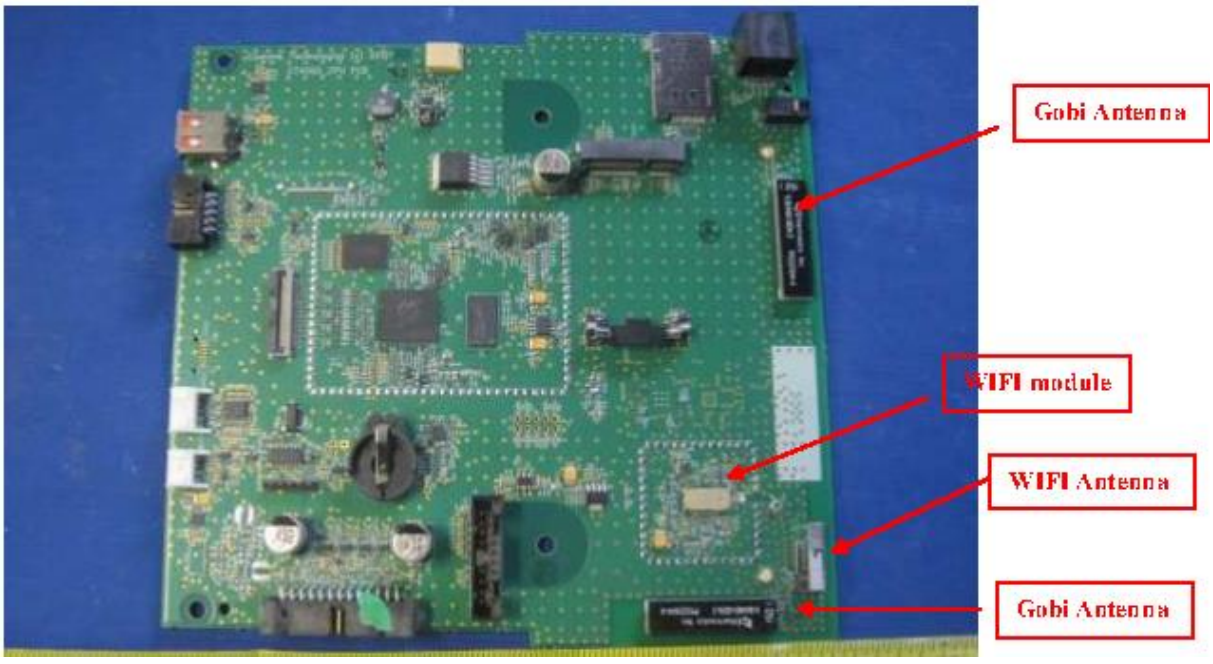


Figure 8 - Sample EVSE communication board

[14] [C36] Wireless Power Transfer for Light-Duty Plug-In/Electric Vehicles and Alignment Methodology (J2954), SAE International, WIP, https://www.sae.org/standards/content/j2954/

Communication with BEMS and BES systems

EVSEs have to communicate with other systems to coordinate power consumption and billing, as well as other information. To coordinate all this information, networked EVSEs use a communications protocol to speak with a network management system, which coordinates the other aspects. Currently many protocols exist for this type of communication. US companies have primarily created and marketed their own protocol, while the Europe appears to be standardized mainly on a protocol called Open Charge Point Protocol (OCPP). While similar in name to the leading EVSE vendor, ChargePoint, they are not directly related. OCPP was originally started by the E-Laad foundation in the Netherlands, but has since included work from many of the vendors who support it (including ChargePoint, Inc. located in Campbell, CA, which could make the term a little confusing). In many localities, the EVSE is known as a "Charge Point," which is the real reason behind the name.

Building Energy Management Systems (BEMS) are networked energy management systems responsible for accessing, tracking, and controlling the energy usage within a building or set of buildings. These include control/data management for Heating, Ventilation and Cooling (HVAC) systems and other systems that draw or generate energy. Adding EVSE control to BEMS could make the BEMS qualify as what the industry terms an "EVSE Aggregator," which is a system that controls charging and discharging of plugged in EVs.

Protections

EVSEs currently have limited known specific cyber protections available, but there are significant protections available to connected embedded systems. All connected systems benefit from proper segmentation and firewalling. EVSEs should not be reachable from the Internet or other untrusted networks, including a corporate network. Embedded systems can benefit from physical protections, anti-tamper options, as well as proper protection of debug ports and serial consoles. All embedded systems should use strong authentication/authorization with sizable passwords help for any communications with the unit, as well as strong encryption.

Cultural Impact

EVSEs are a very powerful impact for change in modern society. As EVSEs are deployed to more roadways, the marketability of EVs increases. Some companies are finding EVSEs to be a strong draw for employees. Engineering firms, such as defense contractor Raytheon, are finding that engineers are the most likely customers for EVs and that providing easy EV charging is attractive to those potential employees.[15]

[15] [C10] Marino, Frank, *Raytheon Provides ChargePoint Smart EV Charging for Employees*, ChargePoint, (2017). Retrieved 11 November 2017 from https://www.chargepoint.com/files/customerstories/cs-raytheon.pdf

2.3 Power Grid Systems (BES)

The Bulk Electric System (BES), aka the Power Grid, is a combination of electrical components that generate, transport, and distribute power to end customers.[16] Large chunks of the BES are modular regional power grids, which can be disconnected from others as necessary. In fact, within a regional power grid, cables that carry power throughout an area can be disconnected from other parts of the grid or connected in different ways. This can happen at "substations" or simply along the cable using what's called a "recloser" or sectionalizer, or a physical disconnection point. This multiply-connected nature of the real cables allows different parts of the grid to be rewired quickly to route power around downed power lines or malfunctioning line equipment.

Generation, Transmission, and Distribution are broken into different business types, often fulfilled by different companies. For example, Consumers Energy of Michigan, until recently, only provided Generation and Distribution, but relied upon other companies for Transmission services.

Power Generation

Without Power Generation, a power grid is powerless. Generators take many forms, including coal plants, natural gas plants, nuclear plants, wind generation, solar panels, and hydro-electric. Residential power generation include gasoline generators and propane generators. Wind and solar power can also be used, and in some cases, can provide power back to the electric grid.

Transmission, Distribution, and Substations

The "transmission network" is a specific term within the BES, indicating the infrastructure that carries large amounts of energy from generation sites to an electrical substation. Transmission lines carry high-voltage electricity of 115 kilovolts (KV) or more because high voltage transmission loses less energy over long distances than lower voltages. Transmission lines are typically 3-phase power, but occasionally can carry single-phase AC. For very long distances (hundreds of miles), high-voltage DC (HVDC) current is used because at those long distances DC is more efficient.

Substations are locations, often either housed in a building or simply surrounded by chain-link fence, that provide a number of services, such as:

- Change voltage from one level to another
- Regulate voltage to compensate for system voltage changes
- Switch transmission and distribution circuits into and out of the grid system
- Measure electric power qualities flowing in the circuits
- Connect communication signals to the circuits
- Eliminate lightning and other electrical surges from the system
- Connect electric generation plants to the system
- Make interconnections between the electric systems of more than one utility
- Control reactive kilovolt-amperes supplied to and the flow of reactive kilovolt-amperes in the circuits

[16] [P11] NERC, *Bulk Electric System Definition Reference Document*, North American Electric Reliability Corporation, (n.d.). Retrieved 04 May 2018 from https://www.nerc.com/pa/RAPA/BES%20DL/bes_phase2_reference_document_20140325_final_clean.pdf

Transmission substations can step-up voltage received from local generation voltage using large power transformers to high voltage (HV) in the range of 69kV to 230kV, extra high voltage (EHV) ranging from 345kV to 765kV, or ultra-high voltage (UHV) from 1100kV-1500kV, depending on the customer's needs. These are called "Step-Up Transmission Substations". Additionally, a Step-Up Substation can step up voltage from generation level to HVDC, typically at 250kV, 400kV, or 500kV.

"Step-Down Transmission Substations" inversely reduces higher voltages from long-distance transmission lines to a subtransmission voltage, typically 69kV, for feeding of Distribution substations.

The "distribution network" is used to carry electricity to end customers. Distribution includes the power systems starting at Distribution substations and ending at the on premise Power Meter.

The Control System

So far, we've been discussing only the power-aspects of the power grid. However, in order to maintain these high-power networks, low-power Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems are deployed throughout the grid, which control and monitor the power networks, and make changes as necessary to maintain a stable power grid.

The power grid has to fluctuate and adjust to our usage patterns. Otherwise a brown-out would occur each time a freezer compressor, water pump or furnace fan started. A brown-out is where the usage over-uses energy and reserve electricity is used up before additional generation can be "connected" to feed it. Brown-outs are when the lights dim, the TV flickers or turns off, the clocks reset, and the fire-alarms beep. They are extremely rare due to intelligent use of ICS and SCADA systems. Generators supply power to the grid and we use the power at a different rate. To provide a stable power grid, utilities "spin up" generators to handle additional load, deploy capacitor banks and other systems to handle additional power when we stop using so much, and provide that power back when we use more... and occasionally shut down or spin up additional generation to cope with peak demand. Many complex calculations are made daily to provide us stable power so our computer systems stay running consistently and the TV doesn't flicker. Typically, we barely notice when significant changes to power usage occur. Regulatory bodies put fine-tuned restrictions on performance of ICS to ensure rapid response to energy demands don't cause significant problems, and it has worked fairly well for decades.

In 2003, the Northeastern US experienced a notable power outage affecting numerous states all the way from the East Coast into the Great Plains. This outage was caused by numerous factors and failures in managing the control systems correctly, and a few small events caused cascading failures, where different segments of the power grid failed because control systems did not disconnect healthy portions of the grid from failing segments. People died from this outage. Many man-hours went into investigating how/why the outage occurred and the culture of the power industry has been significantly shaped by this and similar events.[17]

Advanced Metering Infrastructure (AMI) is a combination of so-called "Smart Meters" and support communications infrastructure which allow these Smart Meters to communicate with the Utility systems. AMI is part of the Distribution part of the BES. Because of ARRA funding and a great deal of attention to the "new thing," AMI systems received significant design attention to security and more verification than their aging cousins, ICS and SCADA systems which control much of Distribution, Transmission, and Generation systems.

[17] [P12] Minkel, JR, *The 2003 Northeast Blackout – Five Years Later*, ScientificAmerican.com, (13 August 2008). Retrieved 14 May 2018 from https://www.scientificamerican.com/article/2003-blackout-five-years-later/

Costly Guys in Trucks - and Tools They Carry

Over the years, meter reading and end-user power control have been a costly part of the energy business, and subsequently an area of research to find cost-reduction options. Each time a utility "rolls a truck" it costs them at minimum $500 (budgeting numbers). This means that to turn off power to a residence or apartment, to configure and troubleshoot a meter, to handle any issues that come up, the cost starts at $500. For high turn-over areas such as apartments near colleges, the cost to "connect" and "disconnect" can gets expensive very quickly.

In order to troubleshoot and reconfigure meters and substation equipment, these technicians often carry laptops with specialized software to interact with meters and ICS in substations. Utilities and vendors have been encouraged to provide limited-access cryptographic keys for these tools, in order to limit the damage if they are stolen.

For this reason, many AMI Smart Meters include an electromagnetic "disconnect switch" allowing the utility to enable and disable power at a given location without a technician visiting the site. Unfortunately, this disconnect switch also dramatically increases the risk of Smart Meter compromise. A compromised meter can connect and disconnect power load from the grid at will. A few thousand compromised Smart Meters can connect and disconnect a great deal of energy load at once in a synchronized fashion. We will cover this more in subsequent sections of the paper.

Peak Load, Capacitor Banks, and Spinning Reserve

Utility companies develop their energy generation/management plans based on "peak load," or the amount of energy used at the most energy-active time for a given area. If these plans cannot provide enough energy during peak usage, the utility must revamp them and possibly add more generation, and/or negotiate on the energy market for other organizations to provide the necessary additional generation.

Spinning reserve is any back-up energy production capacity that can be made available to a transmission system with ten minutes' notice and can operate continuously for at least two hours once it is brought online.[18] Utilities also use systems known as capacitor banks to act as an energy buffer, storing energy when load is lower than generation, and providing it back to the grid as need requires. These capacitor banks can be quite costly and difficult to source quickly and represent one of the greater risks of instability in the event of attack on the power grid.

ICS / SCADA

The power grid relies heavily on ICS, particularly ICS devices combined together into a SCADA system, which allow operators to gather information, identify and respond to alerts, and exert control throughout the grid. The most common ICS devices found throughout the grid fall into two categories: Programmable Logic Controllers (PLCs) and Remote Terminal Units (RTUs). The differences between the two categories are largely based on where the majority of the logic/programming lies. PLCs are programmable, meaning much of the logic / decision-making happens at the PLC, as a distributed computing component. RTUs provide significant control when deployed in the field, however the majority of their functionality is to provide terminal access to the control center (think: telnet or dumb terminal session); the logic remains elsewhere.

[18] [C13] "Spinning reserve, non-spinning reserve", In *Energy Dictionary*, (n.d.). Retrieved on 25 April 2018 from: https://www.energyvortex.com/energydictionary/spinning_reserve__non_spinning_reserve.html

Demand Response / Load Control

Smart Meters enable a great deal of control, influence, and empowerment in the Distribution network. To influence power load during peak usage, the industry has been leveraging two complementary technologies: Load Control and Demand Response.

Load Control is when a utility gets permission from customers to exert some control over high-energy devices in the residence, such as air conditioning (AC), and provides credit to the customer's bill in compensation. Typically, a utility will cycle a customer's AC off 15 minutes out of every hour. While not terribly noticeable to one customer, with enough customers in an area participating in the program, utilities gain significant stability improvements.

Demand Response is a different approach to provide similar stability but grant more control to the customers. Instead of controlling anything within the customer's premises, the utility provides customers information on increased pricing for energy. A customer consumes this information and will typically use a programmed home-management system to adjust usage. While similar in nature to Load Control, Demand Response requires Time-Of-Use (TOU) billing (where energy costs different amounts based on time of day) and requires the customer to take action on the information. This approach puts the customers in control of their own energy usage with a more natural curtailment strategy. Customers are encouraged to simply do what's in their best interest. However, without the direct control, utilities are at the mercy of customers participating in the program, and prediction models get much more complicated.

Optical Ports, Mesh Nets, Cellular, ISDN, Leased Lines

SCADA, ICS, and Smart Meters all require significant communication to be effective. This equipment is deployed at generation plants, substations and on customer's premises, with varying requirements on connectivity. Utilities use many different technology types to stay in contact with their equipment. For some devices, utilities still make use of older technologies like ISDN (digital dial-up). Many Smart Meter rollouts and substations make use of cellular, and possibly mesh networks using proprietary FHSS radios. Many substations use leased lines which are virtually a hard wire connection back to the utility, although often the hardware takes a few twists and turns along the way and at least goes through the local telco.

In addition to remote communications, Smart Meters make heavy use of optical communications to a local tool. This optical port, defined in ANSI C12.18, allows a utility to program and configure power meters.

Energy Market

One of the biggest surprises to most consumers is that a diverse energy market exists, where sources with power generating plants/sites sell their energy, and utilities bid and purchase energy as necessary.

FERC / NERC / PUC / PSC

The Energy regulatory space is quite complex, with both federal and state-focused influences dictating how power is generated, transported, and distributed.

At the federal level, the Federal Energy Regulatory Commission (FERC) is the "big stick" agency, ensuring minimum safe-guards and best practices are used to protect our critical infrastructure. FERC makes use of Critical Infrastructure Protection (CIP) standards created by the North American Electric Reliability Corporation (NERC) to enforce these best practices. NERC has created seven different iterations/versions of the CIP standards to evolve with the industry and its understanding and ability to deploy intelligent security systems. While NERC-CIP standards are not sufficient for ensuring "cyber

security," they are a good step towards it. No standard is able to ensure that an organization understands and cares about the cyber security of its systems. However, utilities are certainly incentivized to comply with NERC-CIP, as fines for non-compliance can be up to $1M per day of non-compliance.

At the state level, Public Services Commissions (PSC), aka Public Utilities Commissions (PUC), ensure the customers are protected. These organizations have the ability to set electricity rates to consumers. Meanwhile, PSCs and PUCs are working hard to understand the cyber security aspects of the power grid (and other utilities) to ensure they provide for proper rate increases. This is for utilities to deploy important cyber security protections and replace horribly insecure systems with better options.

IOU, Muni's, and Co-ops

Power Utilities can be broken into three primary categories: Investor Owned Utilities (IOUs), Municipal power companies (referred to as Muni's), and Co-operatives (Co-ops). The geographical and monetary footprint of these different types of utilities plays into attack surface and ability to pay for cyber security. Numerous IOU power companies have spent significant amounts to provide/share security research, capabilities, and best practices to the less-endowed utilities because they understand that the grid is all shared; exploitation of a small power company can have dramatic impact on all surrounding utilities.

Power Grid Standards

The power grid has many ISO, IEC, and ANSI standards. Some of the more interesting standards that determine much of the cyber security landscape in the power grid are:

- DNP (IEEE 1815)
- Syncrophaser Standards (IEEE C37.118.1)
- IEC 61850
- IEEE 802.15.4g
- ANSI C12.22/.18/.19
- OpenADR 2.0b

There are many others as well. A full review of all power grid standards is outside the scope of this paper but more information can be found at: https://www.nist.gov/programs-projects/smart-grid-national-coordination/standards-information-resources-nist-and-sgip

2.4 Building/Local Energy Management Systems (BEMS/LEMS)

A building management system (BMS) or a building automation system (BAS) provides computer-based controls over a buildings mechanical and electrical systems such as heating, cooling, lighting, fire systems, security systems, etc. Building energy (BEMS) or local energy management systems (LEMS) specifically control the energy systems and usage of buildings to make energy usage more efficient, e.g. turning off lights, adjusting temperature for work hours, and so on. The systems themselves are specific examples of industrial control systems (ICS) and are also known as supervisory control and data acquisition (SCADA) systems. As is the case with most computer-based systems the building and local energy management solutions are frequently connected to the outside world via direct or cellular internet connectivity to allow for management, alerts, and general communication.

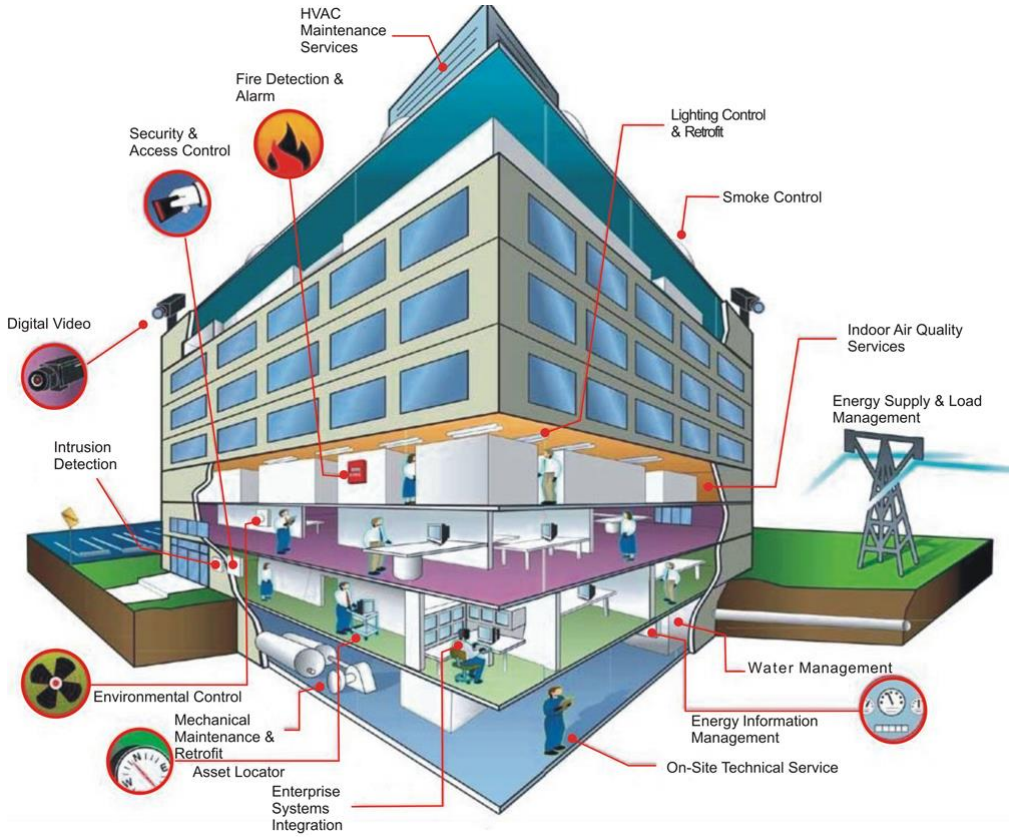


Figure 9 - Building Management System[19]

These systems, when networked together regionally with other intelligent energy systems, such as advanced metering infrastructure, play a significant role as part of the core of the "smart grid" as it is still being realized. The energy management systems are able to dynamically adjust loads based on feedback from the utility. This allows the utility to balance loads on their power grid.

[19] Image from https://blog.econocom.com/en/blog/smartbuilding-and-bms-a-little-glossary/

Control energy usage for buildings, is responsible for 32% of all energy and 40% of primary energy in most IEA countries. Therefore, the aggregate efficiencies that can be captured via a building or local energy management system can be quite substantial.[20]

Research from the Pacific Northwest National Laboratory (PNNL) has shown that when J1772 charging stations can be managed by a local energy management system capable of coordinating charging of vehicles, efficiency is improved by reducing the peak load by 26%, thereby producing less stress on the local power grid.

Our research has shown that most EVSE providers provide a cloud-based control and reporting platform with some level of both customer and utility grid integration. EVSEs are primarily configured to communicate directly with these cloud-based systems. While B(L)EMS systems can add efficiency, this level of integration does not seem to be widely deployed. We do, however, believe that this implementation scenario is not far off given the efficiencies that can be achieved.

It is important to recognize that ICS and SCADA systems are usually designed to be closed systems and as such, the internal cyber security inside the network is usually weak or not implemented at all due to performance and latency requirements. The global connectivity trend is now pushing these systems into contact with the Internet introducing significant cyber security concerns. If building and local energy management systems are added to the connectivity equation for EVSE operation, it is very important to consider the cyber security implications that these systems will bring into the mix.

[20] [BE02] Marmaras, C., Javed, A., Rana, O., and Cipcigan, L., *A Cloud-Based Energy Management System for Building Managers*, ICE '17 Companion Proceedings of the 8th ACM/SPEC on International Conference on Performance Engineering Companion 22-26 April 2017, pp 61-66, doi: 10.1145/3053600.3053613. Retrieved 27 April 2018 from https://research.spec.org/icpe_proceedings/2017/companion/p61.pdf

3 Freight Traffic and Fleet Specific Use Cases

A truck can be described as a vehicle designed with the primary intention of carrying non-passenger loads. In the context of this paper, we are primarily discussing commercial motor freight vehicles that are subject to the Federal Motor Vehicle Safety Regulations. These are vehicles having a gross combined weight rating (GCWR) or gross vehicle weight rating (GVWR) of 10,001 or more pounds.

Trucking is a regulated industry. On an interstate level, the Federal Motor Carrier Safety Administration (FMCSA) regulates the safety aspects of trucking. Companies that operate commercial vehicles with a gross vehicle weight of 10,001 pounds or greater in interstate commerce must register for a USDOT Number. Some states also require registration for a USDOT Number for motor carriers that operate solely in intrastate commerce. Also, commercial interstate and intrastate hazardous materials carriers who haul types and quantities of such goods requiring a safety permit must register for a USDOT Number.

Freight carrying trucks come in a number of standard configurations in the United States. Single units containing both the power unit and cargo space are called straight trucks. Vehicles that separate the power unit from the cargo carrying unit are referred to as tractor trailers. Standard truck configurations, such as these, can operate in all 50 states if they have a gross vehicle weight (GVW) of up to 80,000 pounds. States that had greater maximum vehicle weights before the 80,000 GVW limit went into effect in 1974 were allowed to retain them.

Truck operators can be defined as private carriers and for-hire carriers. A private carrier transports its own cargo, usually as part of a business that produces, uses, sells and/or buys the cargo that is being hauled.[21] A for-hire motor carrier transports goods owned by others for compensation.

Some industry analysts predict aggressive adoption of electric trucking options, pointing to new market entrants and the availability of state-based incentive packages. A number of states are offering financial incentives, including tax credits, for lowering the costs of acquiring MD/HDEVs.[22] Based on our research we have found that there are a number of issues that may slow or inhibit the adoption of MD/HDEVs. Most of these issues stem from how the trucks are deployed and used in commercial operations. Outside of environmental and fuel cost concerns, there are some real potential benefits of MD/HDEVs, such as the reduction in engine complexity which could improve operational uptime and reduce maintenance/operating costs. Modern diesel truck engines have about 16,000 parts. This creates a complex maintenance and supply chain situation. The comparatively simple electric motor has the possibility to dramatically reduce the number of components and simplify maintenance and operations.

[21] [T08] FMCSA, *What is a private motor carrier?* , Federal Motor Carrier Safety Administration, (02 December 2014). Retrieved 27 April 2018 from https://ask.fmcsa.dot.gov/app/answers/detail/a_id/247

[22] [T09] O'Dell, John, *California Readies $398-million Green Truck Incentive Package*, Trucks.com, (11 December 2017). Retrieved 27 April 2018 from https://www.trucks.com/2017/12/11/california-green-truck-incentive-package/

3.1 Motor Freight Operations

There are many forms of trucking operations. These different operations generally utilize their equipment differently. The major for-hire segments are truckload, less-than-truckload, parcel/courier, hazardous materials and specialized hauls, household goods, and intermodal. Many large companies operate multiple types of trucking operations.

Truckload, or TL carriers, generally handle shipments ranging from 10,000 to 48,000 pounds that originate from a single shipper and are destined to a single consignee. Because of the nature of their operations, truckload carriers usually utilize tractor trailers and generally do not operate terminals. They frequently do not have scheduled operations on regular routes. Examples of TL carriers would be J.B. Hunt Transport, Werner Enterprises, and Schneider National Carriers.

Less-than-truckload, or LTL carriers, generally handle shipments that range from 150 to 10,000 pounds. LTL carriers operate terminals to consolidate and deconsolidate shipments. They often operate on regular routes and on schedules. In contrast to TL carriers, it is normal for LTL carriers to have freight from many different shippers on each vehicle at the same time. Freight is usually picked up in the afternoon by a driver with a straight truck or tractor trailer who is dispatched from a terminal and makes many stops before returning to the terminal. The freight is then unloaded and sorted at the terminal, loaded on a line-haul trailer, and driven overnight to another terminal where the freight is unloaded and either placed on another truck for delivery or further consolidated and loaded on another truck for shipment to another terminal. Freight destined for delivery usually is loaded on a straight truck or tractor trailer for local delivery in the morning. LTL carriers often utilize separate vehicles for line-haul operations between terminals and pick-up and delivery activities, although this can vary depending on freight volumes and equipment availability. Examples of LTL carriers are ABF Freight System, Old Dominion Freight Line, Ward Trucking, Estes Express Lines, and YRC Freight.

Parcel carriers or couriers primarily handle small shipments of individual packages up to 150 pounds. Like LTL carriers, they operate terminal systems to consolidate and deconsolidate shipments. The primary carriers in this segment of the industry are UPS, FedEx, and the United States Postal Service. These operators utilize small vehicles to pick-up and deliver packages and they use large vehicles, often tractor trailers, to run line-haul operations.

Hazardous materials and specialized carriers operate a wide variety of equipment with or without trailers. Bulk liquids and gasses are handled in tank trucks that can be used to transport chemicals, fuels and food-grade commodities, such as milk and cooking oils. This category of carriers also handles large quantity shipments of dry products, such as flour, salt, fertilizers, feeds and grains. Some carriers utilize flatbed trailers to transport machinery and large vehicles or specialized trailers to transport automobiles. Others carriers specialize in transporting oversize and overweight commodities on special trailers or aggregates in dump vehicles.

Household goods carriers transport the personal effects of homeowners. These carriers utilize straight trucks and/or tractor trailers to pick-up and deliver household goods, either to the homeowner's new location or to a storage warehouse. Examples of household goods carriers are Allied Van Lines, Mayflower Van Lines, and United Van Lines.

Intermodal carriers transport containers to and from rail yards and ports. These carriers utilize special trailer chassis that are built to handle standard sized containers.

3.2 Commercial Fleets

According to the Owner-Operator Independent Drivers Association (OOIDA), the majority of the trucking sector - ninety percent - is comprised of individual or small business owners (defined as ownership of "ten or less trucks").[23] OOIDA estimates group numbers to be about 350,000 carriers nationwide. In this model, the driver of the long-distance truck is also the owner and primary business contact, negotiating rates and service terms with shippers that require trucks for successful delivery of goods and services.

About half of total truck shipments by tonnage are made by operators of private fleets. These are businesses such as manufacturers, distributors, and retailers that utilize their trucks to pick-up and deliver their own goods. They operate every type of equipment from light duty vehicles, straight trucks to tractor-trailers. Private fleets often operate in specific service areas on fixed routes and schedules. 75% of private fleets hauls are less than 500 miles, with an average haul distance of 71 miles. Examples include food service companies that supply restaurants, beverage companies that distribute soft drinks and beer, grocery stores such as Safeway, and other retailers such as Walmart and Target. Most utilities operate their own fleets of work trucks to service their operations. Some of the larger private fleets that have van style equipment hold for-hire operating authority to be able to utilize their vehicles for backhauls.[24]

Vehicle Usage

Vehicle usage varies greatly among truck operators. Truckload carriers most often use long trailers up to 53 feet in length. While some shipments occur with regular frequency between the same origins and destinations, much of their operations are irregular and result in the vehicle rarely being out of service at regular intervals and locations.

Depending on freight volumes at different locations, some LTL carriers may utilize the same tractor to perform pick-up and delivery during the day and line-haul operations at night. Other LTL carriers may do the opposite and have specific equipment dedicated to each type of service. If local operations require vehicles to go into dense cities, the carriers may often use straight trucks or short 28-foot trailers for pickup and delivery. They may also use smaller equipment for residential deliveries where it may be difficult to turn a tractor and 53-foot trailer. Equipment may be shuffled as needed to accommodate maintenance, repairs and service demands.

Many hazardous materials carriers operate from fixed locations, such as tank farms or other similar locations, where the cargo is stored until it is ready for delivery.

---

[23] [T01] Owner-Operator Independent Drivers Association, *Trucking Facts*, OOIDA, (n.d.). Retrieved 03 May 2018 from https://www.ooida.com/MediaCenter/trucking-facts.asp

[24] [T24] Burks, S. V., Belzer, M., Kwan, Q., Pratt, S., Shackelford, S., *Trucking 101: An Industry Primer*, Transportation Research Board, Transportation Research Circular Number E-C146, (December 2010). Retrieved 04 May 2018 from http://onlinepubs.trb.org/onlinepubs/circulars/ec146.pdf

Light Automotive

In contrast to many trucking operations, light-duty vehicles such as automobiles, vans and pickup trucks, are most frequently used for commuting, or traveling for business or short trips. They are often parked at the owner's place of residence or work for long periods. If the infrastructure is available, this makes charging easy to facilitate.

Battery Weight vs. Freight Capacity

The weight of the batteries in MD/HDEV may limit the carrying capacity of the vehicle. For an MD/HDEV to be competitive with a diesel-powered truck, it needs to have roughly the same carrying capacity. As previously stated, the maximum federal gross vehicle weight is 80,000 pounds. The average tractor trailer combination weighs 32,000 pounds. That leaves 48,000 pounds for freight to be loaded in the trailer. Elon Musk recently announced that Tesla will begin production of an electric Class 8 truck in 2019. Musk has not yet announced how much the vehicle will weigh. Independent analysts estimate a two ton or 4000-pound premium for the MD/HDEV.[25] This means that the freight load is reduced by the same amount which results in an operational loss. This is an even greater issue for container freight, which is usually loaded up to, and sometimes in excess of, the maximum allowed freight.

3.3 NMFTA Electric Vehicle Surveys

In January of 2018, NMFTA conducted an informal survey among our less than truckload (LTL) motor freight carrier members to determine both practical usage scenarios for MD/HDEV and usage of electric forklifts. NMFTA received replies from many LTL carriers of different sizes and geographic locations. While NMFTA did not receive a multitude of responses, we believe that the answers are representative of our membership. The details of both surveys can be found in Appendix A and B of this document.

Electric Vehicle Usage

NMFTA did not see wide adoption of MD/HDEV nor do they see serious consideration for this among their members at the time of this paper. From the survey, we were able to determine that the ability to accurately gauge operating costs, range, load capacity, and maintenance/operational impact are key to adoption. From the survey participant's perspective, there is not enough readily available real-world data on the emerging MD/HDEV. More research needs to be conducted on how the MD/HDEV perform in a real-world environment and in various operating capacities. Additionally, given the large batteries required to power Class 8 electric trucks charge time and range are also going to be key factors for adoption. While rapid charging technology is being developed that might be able to improve charge times, there are also operating safety and capacity concerns due to the higher charging rates.

[25] [T10] Turpen, Aaron, *Tesla Semi truck's battery pack and overall weight explored*, Teslarati.com, (24 February 2018). Retrieved 27 April 2018 from https://www.teslarati.com/how-much-tesla-semi-truck-battery-pack-weigh/

Electric Forklift Usage

NMFTA chose electric forklifts as an indicator of adoption as well as to identify issues or concerns that might arise in the adoption of Class 8 MD/HDEV. Out of the 13 respondents, only three use electric forklifts within their operations, with a total of 42 electric forklifts in use. Though unclear how many other electric vehicles are being supported by these charging stations, these 3 respondents operate 46 charging stations. Only one of the three companies' forklifts communicate with the charging stations. The one respondent that does have communication between the forklift and charging station noted that it is not "advanced communication." None of the current forklift owners utilize the Internet connected capabilities of the charging stations, this reduces the risk of a coordinated attack against charging stations greatly.

Battery and vehicle maintenance seem to be an issue with the electric forklifts including lack of qualified technicians and safe handling for battery maintenance. Serious consideration must be given to how fleet operators can safely maintain the larger batteries on Class 8 electric vehicles. The lack of qualified technicians to work on Class 8 electric vehicles could be a major obstacle to successful adoption as it could increase operational costs.

3.4 Vehicle Charging Requirements

There is a significant difference in vehicle charging requirements between commercial heavy vehicles and light automotive due to both the nature of the business and regulations.

Motor Freight Traffic

When operating a hub and spoke LTL freight operation or running freight in general, the time required to traverse the legs of the runs are very important. In most cases, the freight on the truck can be thought of as passengers on an airplane who all have connecting flights. If one truck stops or is delayed all the connections will be impacted. If an electric heavy truck only has an operational range of 300 miles, compared to 600 miles for a traditional truck, significant operational problems will rise. The operator would need to shorten the local pickup and drop off routes. If they are running a long-distance haul they may need to add another day to the trip. This costs more money and slows down service times and may cause missed connections. Another complicating factor is the federally set hours of service regulations administered by FMCSA. If the driver has to stop and take an extended break to recharge the vehicle it may have an adverse effect on his available driving hours due to the various driving window and rest requirements.

Fleet Requirements

The electric vehicle charging model traditionally considered pertains to light automotive. This is where the owner drives their car back to their house, plugs into a traditional residential electric grid, and it charges overnight. The charge time is assumed to be relatively unimportant, as they have time to charge it overnight at home or during the day at work while the vehicle is not in motion and the utilities have time to coordinate and balance the grid load. A significant amount of time is being spent trying to figure out how to coordinate the charging of these vehicles so that a large number does not adversely impact the grid.

Fleet requirements are very different from the above-mentioned charging use case. Fleets can have thousands of vehicles that all need to be charged in a very short period of time. In some operations the equipment is in almost constant use by different drivers. Heavy trucks are very expensive assets and operators are constantly trying to increase operational up time and utilization. When trucks are not moving, they are not making money. In the NMFTA survey, there are fleet operators who operate over 5000 trucks with potential charging windows of only a few hours. To limit potential operational impediments, charging times must be able to compete with traditional diesel fill-ups. You can fill a truck at 40 gal/min which is approximately 292 miles per minute of charge. This is a fairly significant technical hurdle.

To lower costs for the operator, trucks are often multi-tasked reducing the number of trucks in operation. This means a truck may be doing a long line-haul one day and short pickup/drop off local deliveries the next. The interchangeability of tasks for trucks are a key to their successful utilization. Therefore, a truck designed to do only one type of task will have limited value and reduced adaptation.

Practical Loads

The NMFTA survey found that if larger LTL fleet operators deployed MD/HDEVs, they would need between 10 to 100 charging stations at each terminal with the ability to use all of them at the same time to recharge the vehicles within an hour. Given the load and distance requirements of MD/HDEV they would have to have significantly larger batteries then those found in existing passenger cars. This means that there would be significant grid load issues at these facilities. To handle these load issues there would need to be real time communication between the MD/HDEV and the charging infrastructure to control the load.

Existing Infrastructure

The existing electrical infrastructure at most terminals would not support the load requirements described in the above section. Even if the service at the locations could be upgraded, it is not clear the existing capabilities of the local grid in these geographically dispersed areas would have enough capacity to supply the necessary power. Having to install power producing equipment and/or large batteries locally to handle load issues would further add to the operational costs, and in most cases would not be practical.

Due to the dangers of the charging rates that would be required, this would also necessitate the use of fully automated “hands off” charging technologies. That would introduce additional logistical and installation complications. Most freight terminals are not designed to accommodate additional large infrastructure. Further, large trucks, in general, are much harder to maneuver, especially once one or more trailers are attached.

3.5 Summary

When considering the electrification of heavy vehicles, it is important to understand the specific use cases and operational concerns of heavy vehicle fleet operators. These use cases and concerns differ substantially from those of light personal automotive usage and operational concerns. The reduced acceptable downtime for vehicles, as well as, the overall battery size and capacity, creates some significant technical and logistical hurdles.

4 Vehicle Cyber Security Vulnerability Overview

Vulnerabilities are weaknesses in a given system that, when exploited, provide some level of control to an attacker, and potentially destructive outcomes. Vulnerabilities can be weaknesses introduced by insecure ***design*** or faulty ***implementation***. Vulnerabilities most frequently exist at boundaries of responsibility, and stem from any number of flawed assumptions. For example, most buffer overflow vulnerabilities (the original "remote code-execution" bug), are caused by either a developer thinking that she is not responsible for making sure library calls (such as strncpy, memcpy, strcat, etc…) will not write past the allocated destination memory buffer. She believes the library call will take care of those details, and because the code works as tested, the bug is pushed into production. Meanwhile, the quality assurance people and the developer's boss assume the developer is managing her memory buffers appropriately. This example is common, and it indicates multiple *assumptions* and *breaks in responsibility* that allowed an *implementation* vulnerability to be deployed into production code.

Attackers work very hard to identify vulnerabilities that can provide them code-execution, or other desirable (pronounce "un-de-sIr-abel" by security professionals) capabilities. The extent to which attackers will go to find vulnerabilities simply boggles the minds of most security-minded developers and managers. These decision-makers falsely assume certain boundaries on an attacker's technical ability and tenacity. This allows exploitable vulnerabilities to be shipped and subsequently discovered by dedicated attackers.

When discussing software vulnerabilities, vulnerability discovery, and exploitation, it is important to point out that software exploits leverage programming code they are able to cause the processor to execute (or "tickle"). Whether a design or implementation bug, the vulnerable programming code, running on a target device, is leveraged by an attacker to accomplish some end-goal. Sometimes, especially in design bugs, the vulnerability is not what the code does, but what it does not do (e.g. validating authentication and authorization before providing privileged access). Other times, the code simply does something that is meaningful to an attacker (e.g. reading an unbounded amount of data from the attacker into a fixed-length buffer). The skilled attacker digs into the code with eyes wide open. While fuzzing (aka Robustness Testing) is a favored practice to trigger bugs quickly, the skilled attacker is a Reverse Engineer first. Attackers know what to look for, how to look for it, and the best attackers know what to look for **not** being in the code.

Attackers don't only attack software/firmware. One of the primary attack surfaces for embedded systems is often the hardware. Many valuable goals can be achieved by leveraging specifics of hardware, laws of physics, and assumptions of hardware security; such goals can include improved reverse-engineering, reusing hardware to attack other systems, and gaining access to firmware and/or secrets that can be leveraged to compromise numerous systems remotely.

In addition to software and hardware vulnerabilities, many systems fall prey to insecure configuration. While the systems are designed and implemented in code reasonably well, the deployment of the system was done without reasonable consideration for security. For example, deploying an embedded device with Secure Shell (SSH) is not typically considered insecure, so long as the system is regularly patched and maintained. However, if every system of that make/model includes a privileged user with the same 4-letter password, this combination becomes a **huge** vulnerability. This kind of vulnerability can be discovered using firmware analysis, hardware attacks to gain access to a running system, or simply insider knowledge.

It is important that we **not** underestimate attackers' capabilities, nor be lulled by the idea that hacks only happen in the laboratory.

4.1 Attack Distance Profiles

Before discussing ways to attack the various systems, let's first talk about Attack Distance Profiles, or the distance from which an attacker can exploit a system. Three distance profiles are worth considering when discussing attack vectors: Remote, Proximity, and Local.

Local – The attacker can touch the target device. This could be the outside or inside of a vehicle, the inside or outside of an EVSE unit, the inside or outside of a building or substation, but the attacker must touch the target.

Proximity – The attacker can use a short-range RF signal such as Wi-Fi, Bluetooth, Zigbee, DSRC, NFC, or proprietary wireless. This profile can get muddy with mesh network-capable technology like Zigbee, or other wireless communications technologies that may be attached to a relay/gateway which makes it a "remote" profile. However, those are bigger attack variables, and for the purposes of this paper, this designation will be based on the attack vector technology. Simply keep in mind that virtually any Proximity attack may be relayed through a larger network and possibly connected to the Internet. However, the technology itself has some limited range of effectiveness.

Remote – The attacker is able to launch the attack over the Internet or some similarly large network (such as HAM Radio networks set up with relays and/or High Frequency, or HF, radio bands). Because Proximity technologies can be connected to these larger networks, this designation will be considered "network-connected" technologies for the purposes of this paper.

4.2 Electric Vehicle Attack Surface

Each of the components this paper focuses on have unique designs and attack vectors. These attack vectors define the ways attackers will interact with vulnerable systems and code. EVs are the epitome of touch-points, broken into the three Distance Profiles:

4.2.1 Local

Local Hardware Attacks

ECU's are embedded systems wrapped in rugged casings. Beneath the casings, attackers are likely to find many ways to gain access (through JTAG or serial consoles) to the microcontrollers which control the ECU, inspect and/or modify data in external flash/EEPROM chips, and inspect/modify data as it traverses buses on the printed circuit board (PCB). These and many other hardware hacking techniques can be employed while a vehicle is being serviced, and potentially over night while the owner sleeps.

CAN Bus

Electronic Control Units (ECUs) within the vehicle communicate over several wired communications mechanisms, most notably CAN. These wires are typically accessible from several places, such as the wheel-wells, mirrors, tail-lights, and the OBD2 port. In addition to standard automotive communication, CAN is the protocol used by several EVSEs to provide intelligent charging services.

Unfortunately, CAN traffic is largely considered beyond the scope of securing. There is no current way to prove what system sent a message on a CAN bus network. This allows compromised systems to easily spoof messages they should not be sending.

Power Line Carrier

Another standard protocol used for intelligent charging is known as Power Line Carrier (PLC), not to be confused with Programmable Logic Controllers mentioned with regards to ICS. Used for sending data over high power wires in technologies such as HomeLink as well as by power utilities, PLC represents a fairly untapped ability for abuse. In addition to EVSEs, PLC is also used by heavy trucks to connect systems such as the rig to a trailer, thus making this connection available outside of the vehicle.

4.2.2 Proximity

Wi-Fi & Bluetooth

Beyond the "functional" network, In-Vehicle Infotainment and Telematics systems often provide Wi-Fi and Bluetooth connectivity for entertainment, hands-free calling, and Internet connectivity. While Wi-Fi and Bluetooth have received significant security scrutiny over the years, the design of Bluetooth has been found to be less than ideal for security, and embedded Wi-Fi implementations are often less mature than Infrastructure equipment that powers most business.

In addition, for the past several years, BlueBorne vulnerabilities have existed in most Bluetooth stacks, and because updates occur seldom or never, many Bluetooth systems are still vulnerable.

With a good directional antenna setup, Wi-Fi and Bluetooth signals can be attacked from up to a mile away or more. In fact, many competitions have been run to determine just how far a Wi-Fi connection can be pushed. In 2005, a team at the Defcon Wi-Fi "Shoot-out" competition was able to conduct standard communications at 125 miles!

TPMS

In 2007, when the US automotive market started mandating Tire Pressure Management Sensors (TPMS) to monitor air pressure in the tires, they could not have known that they were introducing a new Cyber Attack Surface. The TPMS signaling is currently limited in scope, and software to handle this data is trivial to write securely, these signals tend to be directly processed by important ECUs, such as the Body Control Module (BCM), which frequently also serves as a gateway between CAN networks and controls most non-engine functions.

TPMS sensors, while not required to use radio signals/RF (some even use the sound of tire tread from the wheel wells), normally use a small part of the Industrial, Scientific, and Medical (ISM) bands around 315MHz or 433MHz. These lower frequencies allow better frequency propagation than Wi-Fi, allowing it to cut through walls better. Regardless of the power levels of the TPMS sensors, an attacker can use amplification and powerful antennas to increase attack distance considerably.

Remote Keyless Entry/Passive Key

Another use of RF below the gigahertz range is Remote Keyless Entry (RKE) systems and Passive Key/Proximity Key/Intelligent Access systems. RKE systems have been deployed for decades to allow remote door lock/unlock, alarm control, and remote start; the chance of you driving a modern car without RKE is minimal. Passive Key fobs allow the car to sense that the owner of the vehicle is sitting in the car, and automatically allows the car to start, and even allows the car doors to automatically unlock when the handle is touched. RKE and Passive Key both also use the ISM band spectrum, generally in the 315MHz and 433MHz ranges. Passive Key also often uses an RFID signal around 125kHz to sense the presence of the key without expending too much energy over time.

While the protocol complexity for these systems is fairly low, it is possible that routines handling the data may be found to corrupt memory and allow for Remote Code Execution (RCE). Alternately, these protocols have been implemented very poorly in numerous cases over the years, allowing an attacker to exercise the control these technologies were designed to provide only to the owner.

Zigbee

Modern EVs are moving toward wireless communication to control charging and billing, and the Secure Energy Profile 2 (SEP2) for Zigbee is being promoted and being used in limited trials[26]. Zigbee is a powerful mesh-networking protocol that sits on top of an IEEE 802.15.4 network interface providing a complex set of network services, and is often used by Smart Meters to provide the “Home Area Network” or HAN.

Zigbee software stacks are generally available, but often modified to suit a particular purpose. Exploitable bugs may be found in both the standard software stacks as well as the modifications/adaptations used to build a particular vehicle. Misconfigurations can also be leveraged to exploit a Zigbee-attached system.[27]

[26] [C37] Communication for Smart Charging of Plug-in Electric Vehicles using Smart Energy Profile 2.0 (J2847), SAE International, 05 November 2013, https://www.sae.org/standards/content/j2847/1_201311/

[27] [H40] *Hacking Zigbee Devices with Attify Zigbee Framework*, blog.attify.com, (24 April 2014). Retrieved 04 May 2018 from https://blog.attify.com/hack-iot-devices-zigbee-sniffing-exploitation/

DSRC

Dedicated Short Range Communications (DSRC) is commonly considered the way of the future for connected vehicles, providing ad-hoc interconnectivity between vehicles and the infrastructure surrounding them. This concept is referred to as Vehicle to Everything (V2X). DSRC allows relatively short-range communications between one vehicle and another vehicle, or DSRC road-side units which provide access to information and services pertaining to the roadways.

Technologically, DSRC is basically a modified Wi-Fi communication system running in "ad-hoc networking" mode (which was prevalent when Wi-Fi was first standardized). DSRC is designed to influence the vehicle based on signals received from other vehicles and infrastructure. This means that attacks can take many forms, including "as-designed" attacks where existing V2X messages are sent to cause chaos for the driver, and possibly influence the power-train systems. Additionally, attacks on the code implementing DSRC can be attacked to potentially provide Remote Code Execution (RCE)… i.e. The attacker's code executes on the DSRC systems within receiving vehicles.

4.2.3 Remote

Telematics / Internet

The Telematics and In-Vehicle Infotainment (IVI) systems utilize remotely accessible networking, most often the Internet. Some vehicles provide Telematics as a separate function from IVI, others join them in the same system. But whatever the arrangement, both utilize the Internet for service, often allowing traffic from the Internet to directly interact with services offered on the units. Even if restricted to a particular cellular carrier's network, an attacker can simply tether their attack tools to a cell phone running on that carrier's network.

These systems are the most connected, the most complex, and the well-understood platforms to the common hacker. This makes them the sweet-spot for attack. Often these systems will provide access to the Internet as well as Bluetooth and Wi-Fi services. The most widely publicized and notorious car-hacks to date have used the Internet as the initial attack vector.

5G/CV2X

A competitor to DSRC as V2X technology is 5G, specifically by the 5G Automotive Association (5GAA). They refer to this technology as Cellular V2X (CV2X), and endeavor to provide 5G Internet and potentially mesh networking to vehicles using 5G cellular. While generally similar in nature to previously mentioned items, like Internet and DSRC, this technology war represents more fodder for attack, as efforts focus on additional functionality and completion.

Corporate Compromise

Because OEMs have considerable control over the vehicles for telematics and CAN bus control (or whichever communications medium is used), an OEM's infrastructure is a high value target. While some have taken great pains to divide networks that provide email access and those which can issue vehicular commands, the actual security of such networks is not well understood and we are required to trust the OEM. Business Email Compromise (BEC), Email Program/Viewer Exploitation, and Spear Phishing with malicious attachments are common attack vectors, in addition to browser compromise and server compromise. Once the initial systems are controlled, an attacker pivots and begins finding new systems to compromise, which may provide access to the desired target (in our case, vehicular control messaging).

4.3 EVSE Attack Surface

Local Hardware Exploits

One significant attack vector, and likely the first step in reverse-engineering and launching an attack is through touching the hardware. Ideal for an attacker would be some external interface, such as USB or other serial interface, which can be leveraged to gain a foothold and potentially gain code execution access to the unit. This opportunity is ideal because an attack may be generated that allows an EVSE to be compromised while appearing to charge the attacker's vehicle. An attacker will also likely, at least initially, want to get access to the electronics behind the casing/panels. Behind the panels an attacker is likely to find specialized access to the microcontroller, storage, data buses, and network connectivity. This access can be leveraged to allow significant compromise. The attacker may also obtain full firmware from the EVSE, allowing offline analysis to discover potentially remotely exploitable vulnerabilities.

Wi-Fi

Many EVSEs communicate with each other and allow configuration and control through a Wi-Fi network interface. Wi-Fi has numerous known attacks that may prove successful if not configured securely, potentially allowing an attacker to participate in the Wi-Fi network and talk directly to the EVSE or perform Man-In-The-Middle attacks on it. In addition to known attacks, such as Passphrase Cracking/Guessing, and leveraging MITM attacks, the code controlling the Wi-Fi interface may also be found to have vulnerabilities, potentially allowing an attacker to gain code-execution on the EVSE without touching it. [28]

Zigbee

As with the EV, the Zigbee interface also provides significant attack surface for EVSEs which support Zigbee communications with the vehicle. Attacks on Zigbee can be performed from a significant distance, likely allowing for anonymous compromise of the EVSE.

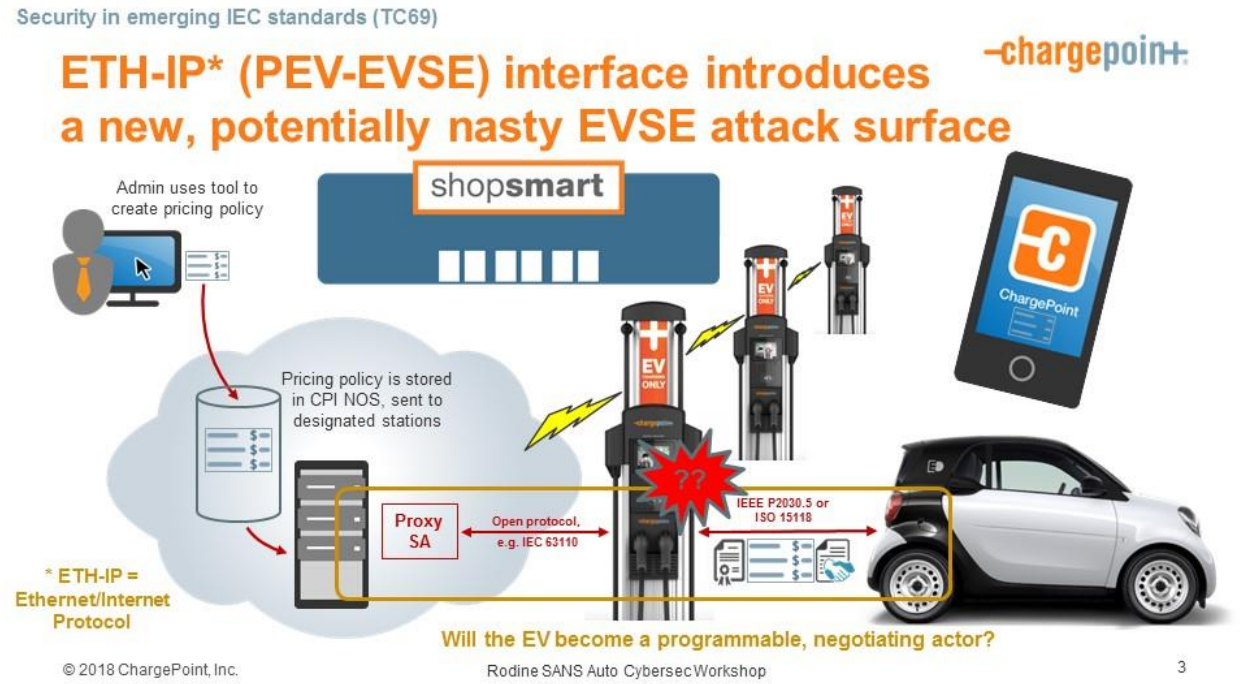
[28] [H41] Wright, Joshua, *How Attackers Exploit Modern, "Secure" Wireless Networks,* blogs.sans.org, (13 October 2010). *Retrieved 04 May 2018 from* https://blogs.sans.org/pen-testing/files/2011/11/Wright-ExploitModernWlan-Webcast-20111013.pdf

Internet / OCPP

Nearly all EVSEs communicate over the Internet back to a vendor portal, either with hardwired Ethernet, Wi-Fi, or Cellular connections. Cellular connections may be attacked using some form of an IMSI-Catcher, or similar tool.[29] Wi-Fi connections may be compromised using the same mechanisms previously discussed. Ethernet-attached systems may fall victim to MITM attacks or direct access against the EVSEs provided services. In Ethernet scenarios, access to the Ethernet may be as easy as finding the right jack in an access panel.

Vehicle-To-Grid Interfaces

The TCP/IP vehicle to grid interface presents the potential of a significant attack surface. Figure 10 illustrates the area of interface concern. One of the current protocols being used for DC Fast Charging (DCFC) is DIN SPEC 70121:2014 *"Electromobility - Digital communication between a D.C. EV charging station and an electric vehicle for control of D.C. charging in the Combined Charging System"*. This protocol has security issues including no requirements to the secured communication via Transport Layer Security (TLS), no digital certificates, and no XML based digital signatures meaning that the authenticity and integrity of data cannot be ensured. A second popular standard, ISO 15118 "Road Vehicles -- Vehicle To Grid Communication Interface," while providing for security, has not received any independent analysis. Without a standardized scalable solution for the EVSE industry, manufacturers are left to their own devices with varying rates of success and many cybersecurity unknowns.



Slide used with permission of ChargePoint

Figure 10 - EVSE Interface Vulnerabilities

[29] [H32] Uttmark, Michael, *LYE IMSI Catcher*, Hackaday.com, (30 May 2017). Retrieved 10 May 2018 from https://hackaday.com/2017/05/30/lte-imsi-catcher/

Corporate Compromise

EVSEs are not simply vulnerable where deployed. They also rely heavily on a vendor portal or an API that provides access to EVSE owners and aggregators. Such interfaces can exercise significant control over the EVSEs, including how much power they can provide through the charging cables, as well as firmware updates. The systems and networks used to support EVSE deployments could be leveraged to cause significant harm to the Bulk Electric Systems, as well as potentially countless vehicles.

4.4 Power Grid Attack Surface

The power grid has its own set of security issues that have been the subject of many reviews. There is significant additional information on this subject, including congressional research.[30]

AMI

AMI networks consist of hundreds to thousands of Smart Meters networked either with mesh networking technologies with a cellular (or leased line) uplink, or direct cellular connection to the utility for each Smart Meter. The AMI network is potentially vulnerable to attack by physically compromising a Smart Meter and using it to communicate to the rest of the network and the AMI Head End (which controls all the meters and collects information from them). Another method of attack on the AMI network is to gain access as an additional device on the network. Sometimes this only requires understanding the hopping pattern and sync method for new meters. Knowing cryptographic mechanisms and secrets is helpful, which may potentially be obtainable by "borrowing" a Smart Meter from someone else's house (you don't steal your own, right?). Once on the network, it is possible to discover a vulnerability in the meters, which allows for a Meter Worm[31], through which hundreds or more meters could collectively shed load all at once (i.e. shut off homes, so that energy is no longer being used). By rapidly cycling the grid load enough (powering on and off the customers' premises), the power grid can be destabilized and potentially cause certain components to malfunction. The effect is well demonstrated, though not using aggregated Smart Meters, through the Aurora[32] attacks where Idaho National Labs was able to make a generator smoke and shake using a simple cyber-attack to rapidly modify load. Another valuable target to compromise is the AMI Head End, the computer system(s) at the Utility that control all the Smart Meters. Head Ends have access to all cryptographic keys and the ability and authority to control every Smart Meter. Similar to the worm scenario, this system has the ability to cause massive fluctuations to the power grid, potentially causing serious harm.

Substation Comms Systems and SCADA equipment

Substations have valuable control systems that manage energy transmission and distribution for a given area. Most are simply surrounded by a chain-link fence and perhaps some barbed-wire/razor-wire. Once in a substation, many attack surfaces are available. An attacker may compromise the ICS/SCADA

[30] [P02] *Campbell, Richard J., Cybersecurity Issues for the Bulk Power System, Congressional Research Service, (10 June 2015). Retrieved 01 May 2018 from* https://fas.org/sgp/crs/misc/R43989.pdf

[31] [H42] Davies, Mike, *SmartGrid Device Security: Adventures in a new medium*, Blackhat 2009, (August 2009). *Retrieved 04 May 2018 from* https://www.blackhat.com/presentations/bh-usa-09/MDAVIS/BHUSA09-Davis-AMI-SLIDES.pdf

[32] [H43] Aurora Attack Video, CNN, (n.d.). *Retrieved 04 May 2018 from* https://www.youtube.com/watch?v=fJyWngDco3g

systems to change how they function, insert a backdoor or add a relay to allow easy access to the SCADA networks remotely. Often a substation will have a variety of interesting things to attack, but perhaps the most interesting is the network uplink. Substations are typically connected using a RF device of some sort, such as S&C SpeedNet radios,[33] or SilverSpring Networks eBridge.[34] If Ethernet connectivity options are used (as opposed to point-to-point serial links), TCP/IP networking is also frequently used, a fact which attackers can potentially leverage to attack other systems within the SCADA network. Some radio technologies are so bad by design, they can be coopted without entering the substation. Some radios currently deployed provide encryption but limit the choice of keys so that the key-space is 8-bits or less.

Once access to the SCADA network is obtained, through whatever means, ICS systems used to control the power grid are frequently the easiest targets to influence or compromise. In addition to an attacker directly causing harm, they can also provide false data from the field to the control center, which may cause a utility to make destructive decisions to compensate.

Energy Markets

To augment their existing generation capabilities, utilities rely on the energy market. Prices for energy on the market are determined by supply and demand. If the market is flooded by fake data for either one, the price of energy can be manipulated. Such fake data can be caused by abuse of Internet APIs, compromised utility networks, and other forms of misinformation.

Corporate Compromise

As with all other components in this ecosystem, standard business network/system compromise can lead to disastrous consequences. Whether the initial stages happen through Spear-phishing, business email compromise (BEC), or web browser exploitation, an attacker can pivot from that initial compromise throughout the utility network. Some utilities have taken great pains to lock down access from the corporate network to the control systems network. Some even have them separated completely, with a remote access VPN or other mechanism between them for maintenance purposes. However, since the corporate employees have to make changes that impact the control network, these networks often have the corporate enterprise resource planning (ERP) system bridging the networks. Logically this makes sense, since ERP systems can be programmed to handle any number of business-logic use-cases. However, ERP systems have a tendency to provide the least resilience to attack: They're easy.[35]

Meanwhile, ICS systems continue to be slow to adapt to the hostile environment of increasing connectivity. Whether pivoting through an email-compromise or guessing VPN/remote access passwords, once on the same network with ICS, most SCADA systems are not difficult to compromise and/or influence.

---

[33] [H49] *SpeedNet™ Radios*, S&E Electric Company, (n.d.). Retrieved 07 May 2018 from http://www.sandc.com/en/products--services/products/speednet-radios/

[34] [H48] *Network Management Systems: A Suite of Intelligent Devices*, Silver Spring Networks, (n.d.). Retrieved 07 May 2018 from https://www.silverspringnet.com/solutions/network-devices/#fndtn-content-7

[35] [H44] Bort, Julie, *Oracle's software was hacked by interns in an hour, researcher says*, businessinsider.com, *(*27 October 2015*). Retrieved 04 May 2018 from* http://www.businessinsider.com/oracle-erp-hacked-by-interns-in-an-hour-2015-10

Building / Local Energy Management Systems

Because most EVSEs are directly controlled by the vendor's cloud interface, successful attacks on the vendor network would be fruitful. However, compromising the local Energy Management System is significant. The vendor has direct control over EVSEs, but much of that control is pushed out to their customers (the people managing the BEMS/LEMS). This control includes charging rates, energy usage while charging, pricing models, and other access. If an attacker compromises the BEMS corporate network, credentials or session information for the EVSE Vendor's Portal may be leaked/hijacked allowing the attacker the control of the EVSEs and pricing information (as well as where the money goes). While each vendor's capabilities differ, it may also be possible to configure EVSE firmware updates and access passwords for a given EVSE.

5 Potential Threat Actors

5.1 Attacker Profile

This section of the document contains a brief holistic review of attacker motivations, including psychological, technical, financial, and political factors. In addition, this section will explore what makes a heavy vehicle an attractive target for a range of cyber attackers, from the lone attacker, to an insider threat, to an organized group with malicious intent, and why certain unique EV vulnerabilities may be targeted for exploit.

The profiles below denote certain classes of attackers; however, consideration needs to also be given to the intent and capability of the attacker to carry out an attack. A danger inherent with cyber-based attacks is the use of "canned" or cookbook attack instructions, combined with a potential reluctance to patch known vulnerabilities. This greatly enhances the capability aspect of an attacker who may be a "script kiddie," and thus is unaware of ramifications associated with the attack.

It is important to note the difference between a hacker and an attacker. Too often the term hacker is misused to denote a person with malicious intent. A true hacker is a person who utilizes cyber tools to overcome technical problems and/or create new methods of addressing a problem. An attacker also uses cyber tools but in an intentionally malicious fashion.

Individual

Individual attackers can have a wide range of expertise, from a simple "script kiddie", to expert knowledge of embedded systems and beyond. Individual attackers can also have varying levels of access to data on the system(s) they wish to attack, from internet provided, to proprietary information. A rogue mechanic is an example of an individual attacker.

Insider

Insider attackers benefit from having specialized knowledge about the target of the attack. One such insider is the disgruntled employee who may have detailed knowledge of the overall system and broad access to the system. Depending on the employee's position, they may also have access to proprietary data. A disgruntled employee may also know where potential vulnerabilities lie and what mitigations need to be overcome. This employee may be unhappy with their job/management or may be susceptible to promises of financial gain for imparting insider knowledge of the system. A disgruntled employee can occur anywhere in the system from the supply chain side, to the manufacturer, to the operator/aggregator.

Collectives

While the individual attacker presents a threat, collectives pool the efforts of multiple hackers and attackers and concentrate them. Collectives can also be associated with other groups, such as hacktivists, organized crime, nation state attackers, etc. Anonymous, which operates using a decentralized group model and has a global following, is known for hacking the Pentagon, Visa, MasterCard and PayPal, among others.

Not all collectives fall into the adversarial category. The Chaos Computer Club, one of Europe's largest groups, attacked a bank and stole 134,000 Deutsch Marks to highlight a security flaw. The money was returned establishing the group as an educator of cyber security. See [H34] for a listing of the top ten most powerful (known) hacking groups as of March 7th, 2018.

Criminal Enterprise/Organization

Monetization is the driving factor for this type of attacker. The heavy vehicle community is especially vulnerable to traditional types of criminal activities, such as cargo theft, which can be technologically enhanced through the use of stolen GPS location data by itself, or supplemented with vehicle disabling malware. In addition, the business aspect of heavy trucking can be vulnerable to techniques such as the deployment of ransomware (see section 7).

Nation State

This type of attacker typically employs the most sophisticated tools and techniques, and enjoys the technological and monetary benefits of a nation state. These types of attackers may go after IP and other private data for competitive advantage and propaganda value. They may also look for ways to strategically cripple industries through large scale cyber-attacks. Typically, these types of attackers employ complex attack methods (see section 7).

5.2 Attacker Motivation

What drives an attacker or group of attackers and why? The sections below address some of the common motivations for attackers:

Monetary Gain

For some types of attackers such as individuals and criminal enterprise/organizations, monetary gain, whether through ransomware payments, direct hire, and/or sale of IP and Personal Identification Information (PII), is the ultimate goal. These types of attackers will look to where the most financial gains for their efforts can be achieved. If there is little or no money to be gained, they will most likely not expend resources on a target.

Hacktivism

The Hacktivist seeks targets based on a multitude of beliefs, including political, social, environmental, and economic, selecting targets that they feel will exemplify their view point in a high-profile manner.

Strategic Intelligence/Disruption

Nation state attackers choose their targets based on the strategic value of the IP/PII that can obtained from the target and/or look for ways to disrupt and cripple critical systems on a national level (see section 7).

Ideological

Terrorists choose their targets for ideological reasons. These types of attacks are often catastrophic in nature and can be used to generate publicity. Generally, these types of attacks involve deliberate attempts to cause loss of life. From a vehicular perspective, these attacks can occur through the use of vehicle born explosives or using the vehicle itself as a weapon.

5.3 Targeted/Desirable Assets in the EV Environment

The Electrical Grid

In the heavy electric vehicle (MD/HDEV) environment, the attacker has some unique opportunities to cause wide spread harm. The interconnection between the MD/HDEV, EVSE, and the grid, gives an attacker the ability to disrupt the grid by gaining control over the EVSE, either through malware on the MD/HDEV, or by directly attacking the EVSE. In late 2017, a German researcher, Mathias Dalheimer presented at the Chaos Communication Congress on hacking electric vehicle charging stations. He determined that once he had physical access to the USB port inside the enclosure, upgrading the firmware on the charging station could be completed in a matter of minutes.[36] Once attacked the EVSE can be used to cause extreme power fluctuations through load cycling. This "whipsawing" effect, which can be multiplied across networked EVSEs, can put incredible strain on the grid's ability to maintain balance causing it to fail. Disruption of the grid could cause a cascading effect across many other sectors, such as healthcare, manufacturing, and commercial. Today, these sectors depend on HVs. In the future, they will depend on MD/HDEVs for delivery and transportation of goods, impacting the financial sector. As usage of MD/HDEVs increases, our dependence on a reliable grid structure becomes an important factor.

Operations

Unlike traditional ICE driven transportation models where a restriction in the fuel supply would have a gradual and delayed impact on operations, failure of an EVSE network would have direct and immediate impact on operations. It would require mobile generators of sufficient capacity to be located and transported to the site. An attacker wishing to disrupt operations could do so by disabling all the EVSEs on a company network. An attacker could also interfere with the EVSE/MDEV/HDEV to spoof the level of charge received by the MD/HDEV, resulting in partially charged vehicles being stranded on their routes, creating a high visibility incident that damages the public's perception of the company and MD/HDEVs in general.

[36] [H32] Dalheimer, M. [media.ccc.de], "*34C3 – Ladeinfrastrukur fur Elektroautos: Ausbau statt Sicherheit – English translation*", YouTube video, 52:54, (published 27 December 2017). Retrieved from https://www.youtube.com/watch?v=szYeqOIQ9Bw

Physical Plant and Vandalism

While MD/HDEV EVSEs will not be located remotely in the same manner as public light passenger EVSEs, the possibility of vandalism of EVSE installations for salvageable metals (especially copper) may occur. Examples of light passenger EVSE vandalism can be found in [H35] through [H38].

While the HV industry is aware of general vandalism issues, the vandalizing of an EVSE presents some unique issues due to the presence of potentially lethal current. The vandals themselves may be severely injured or killed while attempting to dismantle an EVSE, in addition, a partially dismantled EVSE may cause normally safe areas of the EVSE to be energized, creating a hazardous situation.

6 Potential Exploits

The intersection of communication and control between vehicle, charging stations, and power grid infrastructure creates an extremely complex system. This is true of communication paths, as well as, system control commands. Complex systems are difficult to understand as they usually do not allow all aspects to be documented and studied simultaneously. Another major issue is the domains being connected in this complex system have limited understanding of the other major domains, e.g. power grid vs. heavy trucks, and vice versa. Information gaps are usually a source of unknown and undocumented vulnerabilities.

Additionally, there are inherent design weaknesses in both vehicles and power grids that are difficult to mitigate. For example, in the CAN network, with basic prioritization all messages are unsigned and broadcast across the network. This means that any device on the CAN bus can listen and obtain the CAN messages; and it is not possible to authenticate the send of the message, i.e. a reprogrammed ECU anywhere on the network could imitate a critical system component sending out, breaking, and steering commands.

In response to load demand, grid systems have to make real-time decisions and adjustments to the supply of power. As a result, encryption and authentication are not often used on control systems because the performance requirements will not allow for the delay. Additionally, the grid systems themselves are complex systems. They can be thrown off balance by rapid and unexpected usage and availability changes, such as rapid load cycling and putting power back onto the grid unexpectantly. As discussed earlier, CAN (although not J1939) is also used in industrial control systems used by the power grids. They have the same issue as vehicles when used in a trusted network that cannot really be trusted.

There is a vast amount of documentation available on the types of attacks or potential exploits that can be deployed against information-based computer systems such as vehicles, charging infrastructure, industrial control systems, and power generation. A thorough inventory of potential exploits is outside the scope of this paper. Rather, the following list is provided to give the reader an idea of the possible.

6.1 Denial of Service Attack

Due to the inherent real-time communication requirements of vehicles, charging infrastructure, and power grids, they are vulnerable to “denial of service” attacks. A “denial of service” attack is when a network is flooded with excessive messages that restrict or block the transmission of legitimate traffic. This type of attack could be effective on a vehicle CAN bus to disrupt normal communication of the vehicle or throw a grid off balance by flooding the OpenADR systems with malicious messages.

6.2 War Dialing

A popular pass time, before the Internet, was to randomly, or with some pattern, dial telephone numbers in the hopes of getting connected to a computer modem and ultimately interacting with the computer. Security was rather lax since most people assumed that you had to "know" the number and that made it secure. It was always interesting to see what systems you could find and how far you could get into them. Unfortunately, this is still an effective exploit even today. Cell phone modems connected to telematics units and/or SCADA systems, such as those on power grids, often answer inbound phone calls, text messages, or network access requests via the cell phones network IP address. Some of these systems are open connections to the systems with little or no authentication. Research has found telematics devices allowed CAN bus messages to be sent and translated onto the vehicle CAN bus via text message.[37] Many microcontroller-based substation monitoring and control systems come with a handy GSM modem, and other equipment is also connected via dedicated phone lines for remote connectivity. If telephone numbers are assigned in groups or patterns and there is little or no security in place, war dialing a target area could yield advanced access to critical systems which could be used to cause havoc or further pivot to more valuable targets.

6.3 Man in the Middle (MiTM) Attack

When little or no authentication exists for communication between systems or system components, it becomes possible to insert a malicious service, actor or system in between systems to intercept and read the original traffic and at times, retransmit altered traffic. One of the more famous and highly effective MiTM attacks is a relay attack on a corporate environment running SMB with Windows NTLM authentication for inter-computer communication. The "bad guy" listens in on the authentication traffic and is able to capture and then replay the message to obtain access to the target computer. Once on the computer as an authenticated user, it is possible to grab password hash files which can be run through a hash cracker that most likely will result in plain text passwords. Before you know it, the bad guy has domain admin credentials to the network.

6.4 Diagnostic Packets

In systems with mechanical actuators and components, diagnostic functions are usually required to aid in the repair and maintenance of the systems. These are generally a special set of messages and instructions that are only available in some type of restrictive maintenance mode. A good example in vehicles would be brake systems and powertrains. As power control systems have grown in sophistication, there are now commercially available automated tools to calibrate phasor measurement units (PMUs) used for power system and control. This implies that there are diagnostic messages that affect the accuracy and function of the PMU.

[37] [H45] 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/

While most diagnostic functions have built-in protections to prohibit function during normal operations, it has been demonstrated that these protections can often be bypassed. For example, malicious diagnostic requests can be sent to release air from a truck break system or alter the readings that a PMU sends to the grid control causing unsafe and unexpected conditions to occur.[38]

6.5 Remote Code Execution (RCE) Attacks

Whether using memory corruption vulnerabilities, such as Buffer Overflows or Format String bugs, or injection attacks like command injection or SQL injection, any way an attacker can gain code execution on a microcontroller or computer system represents another step closer to malicious actions. RCE attacks are fruitful when attacker-provided data is processed without first validating correctness.

RCE is the epitome of control for an attacker, allowing the attacker any capability the computer system is physically allowed to do. RCE is a problem throughout the entire computer ecosystem, from EV ECUs to EVSEs to power grid components to BEMS.

6.6 Reprogramming ECUs

The complex systems under consideration (consisting of vehicles, EVSEs, and the grid) are actually a very large number of computers and embedded systems. Each embedded system has one or more processors (brain) that controls its function. These chips are initially programmed during the creation of the embedded system but most of the chips are also capable of being reflashed or reprogrammed once they have been deployed. If proper security protections, like secure boot loaders, are not used, it is possible to reprogram the chip with a custom arbitrary set of instructions that can contain malicious code and capabilities. This is a specialized form of RCE, giving the malicious actor complete control over the system. In the case of vehicles, a reprogrammed engine control module would give complete control of a vehicle. A reprogrammed EVSE could spread malware to connecting vehicles or scrape payment information from transactions.[39]

6.7 Hardware Attacks

Gaining access to millions of systems begins with gaining access to one. Whether EVSEs, ICS/SCADA, or ECUs, hardware attacks can gain access to that first target system. This access allows an attacker to obtain the firmware, discover any secrets that the system attempts to hide in non-volatile storage, and provides access to a live system for learning, testing, and tinkering.

Hardware attacks can include JTAG and Serial Console manipulation, data bus sniffing and injection, flash/EEPROM reading/writing, as well as side-channel attacks and fault-injection attacks.

Much can be done to secure JTAG and Serial Consoles: Lock them down.

---

[38] [H09] *Calibrating the Smart Grid*, Fluke.com, (n.d.). Retrieved 02 May 2018 from http://en-us.fluke.com/community/fluke-news-plus/electronic-news/calibrating-the-smart-grid.html

[39] [H02] 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)

Data bus sniffing/injection can be somewhat secured using epoxy, but there is little that will fully keep a dedicated attacker from information that traverses outside a microchip.

Side-channel attacks are attacks that use information gained from the design and operation of a system rather than an implementation weakness, such as power consumption, sound, timing information, etc. For example, there are attacks that use power consumption of a processor to break the encryption algorithms employed by the processor. Sometimes, side-channel attacks can be mitigated through implementation of software, and other times, the actual hardware and board layout can be helpful. There are more difficult to secure against, and this document is not the correct place to learn about the methods.

Fault-injection attacks are nearly impossible to overcome at scale for every architecture. This continues to be an active area of research, with continued success for creative attackers.

6.8 Supply Chain Attacks

In today's manufacturing environment, no company produces all the components that go into an information system. Processors, wiring harnesses, pumps, and whole subsystem components are outsourced to third parties. Then, the third parties often outsource parts and components as well. In this complex web of connections and parts, from inside the production line, it becomes possible to surreptitiously insert malicious components or functionality directly into the end product. It could be as simple as hard coded back doors for remote system access or rogue instructions. The industry is rife with examples of backdoors on firewalls, android phones preloaded with malware, and on trojanized firmware updates. For examples of supply-chain attacks, please see [H27] through [H29].

Supply chain attacks can be mounted against MD/HDEVs, EVSEs, and grid infrastructure. With high demand and an emerging industry, there are usually opportunities to inject malicious code or components into the supply chain, especially when it can be deployed into one area, such as a vehicle, with the intent to pivot into a different area, such as the EVSE.

6.9 Multi-Component Attacks

To compromise a well defended system, attackers will usually combine different exploits and attack methods to achieve their results. They may use spear phishing (targeted malware email campaign) with malware attachments or links to malicious websites to compromise a vendor in an attempt to plant trojanized firmware updates or compromise a vehicle through the OEM's telematics system. A war dialing connection to a telematics unit could be used to reflash an ECU or telematics device to give the attacker persistent access to a target network. Kevin Mitnick conducted a man in the middle social engineering attack against a researcher to find vulnerabilities in the VMS operating system to allow him to compromise other companies who ran that operating system[40].

A sophisticated attacker may leverage the connectivity between EV's and chargers to compromise fleets of both. Initially compromising an EVSE through physical means, an attacker could then exploit a vulnerability in the EV's charging module (or others) through the CAN- or PLC-connection. Because

[40] [H08] Mitnick, K (Author). Wozniak, S. (Foreword), Simon, W. (Contributor), *Ghost in the Wires: My Adventures as the World's Most Wanted Hacker*, Back Bay Books, (24 April 2012). ISBN-10: 0316037702.

many cars will use the EVSE, any car with targeted vulnerabilities would be compromised/infected. If a similar vulnerability is discovered in EVSEs which could be exploited from the charging vehicle, a multi-architecture worm could propagate, to potentially disastrous ends.

Automotive worms are already a concern as multiple Internet and Proximity network (DSRC/V2X) technologies are planned and deployed. Because these devices are often directly connected to the CAN bus, compromising the DSRC radio or Internet uplink, and make large portions of the car's CAN networks available over the air.

With Extreme Fast Charge (xFC) allowing charging at up to 1MW, remotely controlling 300 autonomous trucks could prove very dangerous. Consider an attacker draining these trucks to near-empty, then coordinating charging of all of them at the same time, strategically placed to break locality controls (eg. building management systems with aggregate control and limitations). Perhaps EVSEs will have safety checks to check with the grid control systems to ask permission first. However, if that request/control combination relies on the EVSE, it is possible an attacker can circumvent them. What if all of these vehicles started drawing maximum charge at the regional Peak Load? What if they are all charging and then simultaneously stopped? Controlling 300MW is no small matter. Systems architects will need to consider where and how to place compensating controls such that they are not easily circumvented.

It is important not to underestimate the effort an attacker will undertake to achieve their goals.

7 Ongoing Hacking Activities

The cyber security threat landscape is constantly evolving as the search for new vulnerabilities and attack vectors never stops. The examples of attacks below, while not directly tied to the MD/HDEV community, all contain common elements within the MD/HDEV environment. The attack on the Ukrainian power grid was done with malware that was specifically designed to have "plug and play" modules based on what power grid was being attacked. The insurance dongle attacks are examples of telematics devices being compromised, and the ransomware attacks describe an up and coming form of attack, which is very applicable to the MD/HDEV environment.

7.1 Power Grid Systems

Ukraine Power Grid

The Ukraine power grid attack is actually the tale of two attacks occurring in 2015, and again in 2016.

On December 23, 2015, several Ukrainian regional electrical distribution companies experienced outages caused by an attack on their computer systems, as well as, on their SCADA control systems. In all, seven substations were knocked off line causing power loss to approximately 225,000 customers for several hours. Even though the numbers were relatively small and power was quickly restored, this attack was important in that it was the first time a cyber-attack had resulted in a loss of power. Analysis of the attack showed that the attackers utilized a multi-prong approach, including spear-phishing emails and malware. The attackers harvested credentials from the breached networks and eventually gained access to the industrial control system (ICS) network. Once in the ICS, the attackers were able to operate elements of the SCADA network through the use of human machine interfaces (HMIs). The attackers also used custom designed malware to target field devices at substations. In addition, the attackers generated thousands of calls and flooded the company's phone systems in a DoS attack. This prevented customers from reporting the outages. A detailed report on this attack is available in [N11].

The second attack on the Ukrainian power grid occurred in December of 2016 when attackers disabled an electrical transmission station. This attack differed from the 2015 attack in several important ways. This attack utilized an extremely advanced version of malware specifically designed to attack power grids. Called "Crash Override," this malware can automate mass power outages (unlike the 2015 attacks where attackers had to utilize HMIs to perform the attack), and is designed with swappable modules, which allow attackers to target specific power grids. This feature allows attackers to attack power grids anywhere in the world. It is unknown how Crash Override was initially introduced into the system, and it is also unknown exactly who the authors of Crash Override are. For further reading and an in-depth analysis of Crash Override see [H16] and [H17].

BlackEnergy

BlackEnergy is a Trojan horse malware program that has targeted critical energy infrastructure since 2014, and has been upgraded several times since its initial release. This malware program was of specific concern as it was attributed to an advanced persistent threat actor for the purposes of information gathering for future attacks. This is based on the plug-in architecture of the malware supporting offloading data to USB drives, screen captures, keylogging, and even audio recording. For additional resources regarding BlackEnergy, please see [H21] and [H22].

7.2 Insurance Company Dongles

As vehicles become more feature rich and connected, a number of vendors have developed aftermarket devices that plug into the On-Board Diagnostic (OBD-II) port. When connected to the vehicle, these devices or "dongles" can create a wireless link directly into the CAN bus to support many types of applications, including fleet management, maintenance, insurance, engine diagnostics, driver habits feedback, and other types of expanded functionality. Many of the devices are mass produced and do not conform to secure coding practices, which allows attackers an easy way to wirelessly manipulate ECUs on the CAN bus. In recent years, several security researchers have demonstrated vulnerabilities in OBD-II dongle software. The vulnerabilities in the dongles allow attackers to influence the behavior of the vehicle, potentially disrupting a mission or injuring the operator. While the examples below pertain to the automotive environment, the principles of the attacks are valid for the heavy vehicle environment as well.

2014 - Zubie Aftermarket Service

Zubie is an aftermarket OBD-II device that, using a mobile application, allows drivers to track their driving habits, detect possible malfunctions in the vehicle, and share their location with friends or coworkers. The device communicates with the vehicle's internal CAN bus and it also has a mobile modem that connects it to the Zubie cloud. In early 2014, Argus Automotive Cybersecurity released a joint press release with Zubie disclosing a critical cyber security vulnerability that allowed an attacker to remotely control all vehicle functionality. The vulnerability was caused by poor coding practices within the device. The device could be easily compromised using a MITM attack to trick it into communicating with a hacker instead of the Zubie cloud. Furthermore, since the device accepted unsigned software updates, the attacker could send a malicious software update that caused it to malfunction. Some of the malfunctions Argus disclosed included a "Trojan horse on the Zubie device that effectively allows us to take control over the vehicle" and "tracking the vehicle's location… and transmitting the data to a third party." [41]

2015 - Progressive Insurance "Snapshot" Dongle

The Progressive Insurance "Snapshot" program is a Usage-Based Insurance (UBI) program that allows customers to save on their insurance costs by installing a OBD-II dongle that sends information on their driving behavior to Progressive. The device is one of many UBI solutions being used throughout the insurance industry. In late 2014, security researchers at Digital Bond Labs disclosed that the device was completely lacking secure coding principles. Digital Bond exploited the device by reverse engineering the dongle's firmware and mounting a MITM cellular attack. They noted, "What we found with this device was that it was designed with no security features …It wasn't even based on basic security coding practices. ... It's a house that has no doors, no windows and no fences, with valuables inside." It was not a case of researchers exploiting a weakness in the dongle's security; it was simply that no security existed. For more information, see [H25].

[41] [T01] *A remote attack on an aftermarket telematics service*, Argus Cyber Security (blog), Argus Security, (n.d.), Retrieved on 26 April 2018 from https://argus-sec.com/remote-attack-aftermarket-telematics-service/

2015 – Metromile Aftermarket Telematics Control Unit Dongle

In August of 2015, researchers from the University of California San Diego (UCSD) presented their findings on an Uber/Metromile/Mobile Devices Inc. dongle at the 2015 USENIX Workshop on Offensive Technologies (WOOT). Metromile's dongle, which plugs in under the dashboard, uses Uber's API to differentiate between when a driver is "on the job" and when they are using their car for personal or ride-seeking use. The device toggles the vehicle's insurance between Uber and the vehicle's personal insurance. The team found that the dongle was devoid of even the most basic security practices. The device could easily be hijacked with physical access via USB or remotely reconfigured via the Short Message Service (SMS) available in most modern mobile phones. Since the device communicates directly with the internal networks of the vehicle, it effectively exposes the safety critical systems of the automobile to the outside world. The company that produces the dongle claims that new products on the market do not suffer from the same vulnerabilities, although it is believed that there are still thousands of unpatched and unprotected dongles on the market (this claim was not verified by the UCSD researchers). This illustrates that even when vulnerabilities are patched in new releases, legacy dongles are still exploitable for the foreseeable future. US-CERT has issued a bulletin on the vulnerability.[42]

7.3 Ordinary Car Theft

In recent years, the occurrence of technologically assisted theft has been on the rise. In February of 2015, Metropolitan police in London reported a rise in keyless car thefts. In 2014, 6,283 cars were stolen without a key. Some of the thefts occur when thieves break a window and use the OBD-II port to flash a duplicate smart key for the car.[43]

A more sophisticated approach is the relay attack. Passive Keyless Entry and Start (PKES) systems employ a low frequency "is anyone out there?" signal. This signal is broadcast by the vehicle using a 120-135 KHz frequency band with a range of about 3 to 6 feet. If a PKES key fob is in range, it broadcasts a proximity acknowledgement using a 315-433 MHz frequency. The vehicle then broadcasts a challenge to the key fob. The key then sends its response.

Rather than attempting to cryptographically attack the vehicle to key fob link, attackers have taken advantage of the wireless aspect of the keyless entry system. Using a relatively simple radio repeater, the attacker is able to greatly extend the range of the vehicle and key fob signals and unlock the vehicle. Some vehicles can also be started and driven by this method. For a more detailed look at this type of attack, see "Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars," written by the Department of Computer Science ETH Zurich located in [H31].

A still more sophisticated approach is the deployment of a device similar to a device named "RollJam" created by well-known security researcher, Samy Kamkar. RollJam allows a hacker to unlock a car that has been locked by using a remote key fob. To defend against a simple replay of an unlock code,

---

[42] [H50] King, Chris, *Vulnerability Note VU#209512: Mobile Devices C4 ODB2 dongle contains multiple vulnerabilities*, CERT Software Engineering Institute, Carnegie Mellon University, (11 August 2015, last revised 28 August 2015). Retrieved 14 May 2018 from https://www.kb.cert.org/vuls/id/209512

[43] [H30] Brian, Matt, *London has a real problem with thieves targeting keyless cars*, Engadget.com, (03 February 2015). Retrieved 27 April 2018 from https://www.engadget.com/2015/02/03/london-keyless-car-theft/

manufacturers have long been employing a rolling code scheme whereby after a code is used to unlock the door, both the vehicle and key fob "roll" to the next code in the sequence. RollJam (see Figure 10) takes advantage of the fact that to get around the problem of the key fob being inadvertently pressed, the vehicle allows a generous block of codes to be accepted. When RollJam senses a key fob signal, it sends out a jamming signal on the most used frequencies for key fobs, jamming last few bits of the unlock signal from reaching the door lock receiver. Simultaneously, the RollJam device reads and captures the key fob signal. The unsuspecting user, after being unable to unlock their door, presses the key fob again. RollJam again jams the signal, but this time it replays the stored signal and captures the second one. The attacker now has the "next" unlock signal in the rolling code. RollJam will only work if the attacker uses it before the user presses one of the key fob buttons again. In 2016, South African hacker Andrew MacPherson demonstrated RollJam attacks using two RfCat dongles[44]. As opposed to the custom hardware Samy used, RfCats are reasonably inexpensive and easily available for purchase.

Figure 11 - RollJam Car Unlocking Device

Photo Credit: Engadget

[44] [H52] Dunson, Brandon, *RF Hacking: How-To Bypass Rolling Codes*, Hackaday.com, (6 March 2016). Retrieved on 15 May 2018 from https://hackaday.com/2016/03/06/rf-hacking-how-to-bypass-rolling-codes/

7.4 Ransomware Attacks

Ransomware is malicious software that employs cryptography to lock a system and/or its files and prevent access by legitimate system users. The software then offers the users (for a fee), access back into their system/files. Some ransomware attackers threaten to destroy the systems/files if the ransom is not paid within a set time period. Below are three recent stories of ransomware attacks:

City of Atlanta

Early this year the city of Atlanta was crippled by a ransomware attack. The attackers demanded the sum of $51,000 to unlock the city's computer systems. The restoration of the city's computer system has been a long and costly process. In 2016, the FBI reported that they had received 2,673 complaints of computer extortion with losses of over $2.4 million. In 2017, the number of reports increased to 3,000.[45]

Presbyterian Medical Center-Los Angeles CA

In February of 2016, Hollywood Presbyterian Medical Center in Los Angeles suffered a ransomware attack. Due to the life or death nature of the data stored on the hospital's computers, the hospital chose to pay the attackers $9,000. The attackers then demanded an additional $7,000. The hospital paid the ransom and received the encryption code to unlock their computers. However, it is unknown if the attackers now have the ability to strike again.[46]

Erie County Medical Center-Buffalo NY

Conversely in May of 2017, Erie County Medical Center in Buffalo, NY was hit with ransomware demanding a $30,000 payment. The hospital refused to pay and 6,000 of the hospital's computers were wiped by the attackers. It took the hospital six weeks to recover. Hospital officials estimate it cost $10 million to recover from the attack, including purchases of new software and hardware and rebuilding the hospital's computer system.[47]

Ransomware and the Connected Vehicle

The examples above illustrate that ransomware is a growing concern. With the advent of the connected vehicle, experts feel that it will not be long before vehicles become targets of specialized ransomware, which would disable a vehicle until the ransom has been paid. For additional reading on this topic, please see [H18] through [H20].

---

[45] [H13] FBI, *Internet Crime Report 2016*, Internet Crime Complaint Center, Tech. Rep., (2016). Retrieved on 26 April 2018 from https://pdf.ic3.gov/2016_IC3Report.pdf

[46] [H46] Infosec Institute, *Ransomware Case Studies: Hollywood Presbyterian & The Ottawa Hospital.*, infosecinstitute.com. (n.d.). Retrieved on 4 May 2018 from: http://resources.infosecinstitute.com/category/healthcare-information-security/healthcare-attack-statistics-and-case-studies/ransomware-case-studies-hollywood-presbyterian-and-the-ottawa-hospital/#gref

[47] [H14] Romo, Vanessa, *As Atlanta Seeks To Restore Services, Ransomware Attacks Are on the Rise*, NPR the two-way, (30 Mar 2018). Retrieved on 26 April 2018 from https://www.npr.org/sections/thetwo-way/2018/03/30/597987182/as-atlanta-seeks-to-restore-services-ransomware-attacks-are-on-the-rise

Ransomware and the MD/HDEV

To illustrate the impact of ransomware for MD/HDEVs, imagine you are the owner of Electron Trucking, a trucking company that specializes in LTL deliveries. You have recently converted your fleet over to MD/HDEVs and have a network of 15 DC Fast Chargers (DCFC) to service them. Unbeknownst to you, a disgruntled employee has loaded ransomware onto your EVSE network. The first sign of trouble appears when you receive a call that an EVSE is not charging, shortly afterwards all of your EVSEs are down. Upon further investigation, the display on the EVSE, which normally contains information on the charging status, now reads "Pwnd by 2E4TT6y" and an IP address. You go to the IP address and find instructions on how to make a payment to unlock your EVSEs.

Defending against ransomware is one of the challenges that the MD/HDEV cyber security environment faces. See Section 13 for steps that can be taken to protect against ransomware.

Ransomware and Transportation

Petya and NotPetya ransomware caused a number of problems for the transportation industry. For example, when TNT was hit with the Petya, ransomware that affected their tracking and routing services, the end cost was in excess of $300 million. Maersk, whose system was also impacted by Petya, was unable to dock or unload cargo ships in dozens of ports, resulting in excess of $300 million in losses. The attacks were not actually intended to hit the transportation industry, but rather was an accidental consequence of a suspected nation state level cyber-attack.[48] [49] [50]

7.5 Supply Chain Attacks

HAVEX

HAVEX remote access tool/malware has been targeting the energy sector since at least 2012.[51] It was designed to infect legitimate SCADA control software from ICS and SCADA suppliers. It has been delivered via email attachment, a link to a malicious website, or through vendor compromised software downloads. The malware was pieced together from other available malware source code libraries and examples, and did not contain any advanced hiding or exploit techniques. While not particularly sophisticated it did manage to infect installation files for several SCADA related products such as libMesaSR, eCatcher from eWON, and mbCHECK by MB Connect Line.

[48] [IM06] Coyne, Allie, *TNT Express still struggling to remediate after Petya attack*, iTnews.com, (03 Jul 2017). Retrieved on 26 April 2018 from https://www.itnews.com.au/news/tnt-express-still-struggling-to-remediate-after-petya-attack-467352

[49] [IM07] Kovacs, Eduard, *FedEx Profit Takes $300 Million Hit After Malware Attack*, SecurityWeek.com, (09 20 2017). Retrieved on 26 April 2018 from https://www.securityweek.com/fedex-profit-takes-300-million-hit-after-malware-attack

[50] [IM08] Schwartz, Mathew J., *Maersk Previews NotPetya Impact: Up to $300 Million*, BankInfoSecurity.com, (17 Aug 2017). Retrieved on 26 April 2018 from https://www.bankinfosecurity.com/maersk-previews-notpetya-impact-up-to-300-million-a-10203

[51] [H47] Walker, Danielle. *'Havex' malware strikes industrial sector via watering hole attacks*, Scmagazine.com, (Published June 25, 2014). Retrieved on 04 August 2018 from: https://www.scmagazine.com/havex-malware-strikes-industrial-sector-via-watering-hole-attacks/article/538721/

Preloaded Firmware

Malicious software can also be shipped from the factory. Anyone who has experience performing "Physical Penetration Tests" can attest to the power of a uniform, a badge, and the right attitude. Gaining access to the areas necessary to provide malicious "pre-flashed" firmware to chips is conceivable if not trivial. Do you trust your vendors to protect their systems and your investment? Do you trust them not to purposefully install malicious firmware? How much?

Hardware Backdoors

In addition to malicious software, microchips (microcontrollers, EEPROMs, etc…) have been the target of numerous attacks over the past decade. Microcontrollers/Microprocessors (like the ARM chip in your cell phone or the Intel/AMD chipset in your laptop) can be designed with malicious functionality built-in. So-called hardware backdoors can be built into chips after the design phase by the chip manufacturer, and allow an attacker reliable remote control.[52] Perhaps there are reasons why some chip manufacturers are cheaper than others?[53]

7.6 Attacks via Edge Devices

Go Fish

In April of 2018, the website "Security Affairs" posted an article about a casino having their data stolen via a fish tank situated in the casino lobby. The fish tank was a smart tank, interfacing with the casino's smart building system. Traditionally, casinos, along with banks are known for having robust cyber security, however, the smart fish tank's temperature sensor, an edge device in their smart building system, was not secure.

Attackers were able to compromise the fish tank's temperature sensor and through it gain access to the casino's data files. The attackers then downloaded the casino's "high-roller" client database via the compromised temperature sensor and transmitted the data out. Due to the sensitive nature of the attack, the names of the casino, smart thermostat, and fish have not been released.[54]

The story above, while making interesting reading, also points out that BEMS cyber security, like all cyber security, is not static and must be re-addressed as devices are added, software is updated, etc. For example, if an attacker were able to compromise a building thermostat on a BEMS network, they may be able to launch a cyber-attack using the compromised thermostat against any EVSEs that are interfaced with the BEMS.

---

[52] [H53] Greenberg, Andy, This 'Demonically Clever' Backdoor Hides In a Tiny Slice of a Computer Chip, Wired.com, (6 January 2016). Retrieved on 15 May 2018 from https://www.wired.com/2016/06/demonically-clever-backdoor-hides-inside-computer-chip/

[53] [H54] Simonite, Tom, NSA's Own Hardware Backdoors May Still Be a "Problem from Hell", MIT Technology Review, (8 October 2013). Retrieved on 15 May 2018 from https://www.technologyreview.com/s/519661/nsas-own-hardware-backdoors-may-still-be-a-problem-from-hell/

[54] [H39] *Attackers exfiltrated a casino's high-roller list through a connected fish tank*, securityaffairs.co, (16 April 2018). *Retrieved 04 May 2018 from* https://securityaffairs.co/wordpress/71433/hacking/fish-tank-hack.html

7.7 EVSE Hacking Briefings at Hackers Conferences

There have recently been two hacker conferences discussions on EVSE hacking and vulnerabilities. In December 2017, the Chaos Communication Congress (CCC) Conference in Germany featured a talk titled "Charging Infrastructure for Electric Cars: Expansion Instead Of Security."[55] The security researcher probed different components of the EVSE system and found security problems, such as:

- Insecure third-party ID tokens that allow copying personal card data and successfully charging with the copy
- Outdated versions of the OCPP protocol based on HTTP that allow setting up a man-in-the-middle attack by relaying the transaction
- Insecure EVSE USB ports that allow logs and configuration data to be copied to the drive via an empty flash drive which provide access to the login/password for the OCPP server via spoofed token numbers

In 2013, the Hack-in-the-Box (HITB) conference in Malaysia, featured a talk titled "Who Can Hack a Plug: Infosec risk of Charging Electric Cars." The security researcher identified potential EVSE vulnerabilities based on public information (e.g. vendor web sites):[56]

- Firmware can be extracted to identify eavesdropping points and access encryption keys
- RFID and protocol analysis to determine vulnerabilities
- Short range communications (RS-485) bandwidth and latency limits encryption and makes eavesdropping and man-in-the-middle attacks easier
- RFID short range communication is easy to eavesdrop and costly to patch
- If the same symmetric key is used for all EVSEs and payment cards does not scale and is open to relay and card attacks
- Internet of Things (IoT) protocols and web/mobile control are typically insecure
- Charge station Owners charging configuration and Driver payment methods need to be secured

[55] [H33] Dalheimer, M. [media.ccc.de], "*34C3 – Ladeinfrastrukur fur Elektroautos: Ausbau statt Sicherheit – English translation*", YouTube video, 52:54, (published 27 December 2017). Retrieved on 04 May 2018 from https://www.youtube.com/watch?v=szYeqOIQ9Bw

[56] [C12] Shezaf, Ofer, *Who can hack a plug? : The InfoSec risks of charging electric cars*, slides for presentation at Hack in the Box Security Conference 2013, (2013). Retrieved on 01 February 2018 from https://xiom.com/

8 Threat Impact

Generally, it is best to try to avoid "fear mongering" and consider cyber security as a process of risk identification, mitigation, and reduction. It is, however, important to have a basic understanding of the potential impact of cyber security issues to industry and national infrastructure. As can be inferred from the previous sections, the threat impact to industry and national security could be severe, running from thousands to hundreds of millions of dollars in losses and could have significant national security impacts. The following examples are not meant be exhaustive, but rather indicative of the types of impact that can be expected to allow the reader to get a sense of the stakes involved.

8.1 Cargo Theft

Cargo theft from large vehicles is already a concern, but with an MD/HDEV, it could add more complications. The old trend of cargo theft at trucks stops has given way to more sophisticated groups that are well financed and display a fair amount of patience. In some cases, cargo thieves focus on shipper facilities and set up surveillance to find valuable cargo. They follow trucks for long distances, using multiple driving teams to determine route patterns. Some operate fake trucking or warehouse business to help provide cover for their illegal operations and steal entire trailers. Thieves can target any cargo that is valuable, ranging from TVs to pharmaceuticals to nuts.

Slower charging stations for MD/HDEVs, potentially forcing cargo to sit for 8 hours, would make it an easier target for cargo theft. Tricking the vehicle into thinking its power is full and determining where the vehicle will die on its route is a possibility, too. A depleted EV that requires custom "hands off" equipment to charge will be difficult to get moving again.[57]

The best way to safeguard cargo is to keep it moving and safeguard shipment manifests and route patterns. As discussed previously, the new communication paths introduced with EVs and building/grid integration exposes another attack surface that could be exploited to gather information to further cargo theft.[58]

8.2 Transportation Service Level

A successful freight operation has good service levels, i.e. freight is transported from one location to another within short and predictable (and stable) timeframes. The freight industry spends a great deal of time and resources to optimize their logistics operations. A large event inside a carrier causes disruption to its operations with extensive economic loss.

A larger event affecting multiple freight carriers, even just partially, would quickly disrupt timely delivery of goods and impact business operations in a cascading manner. The "just in time" manufacturing processes now being employed in most factories, require daily on-time deliveries of raw materials and components. An American Trucking Association (ATA) study [IM02] showed that the slow down at the Canadian border during 9/11 caused an estimated loss of approximately $60,000 per hour

[57] [IM04] SensiGuard, *Supply Chain Security*, Sensitech.com, (n.d.). Retrieved on 26 April 2018 from http://www.sensitech.com/en/supply-chain-security/

[58] [IM05] Kilcarr, Sean, *Cargo theft now a tougher nut to crack*, FleetOwner.com, (01 Jun 2016). Retrieved on 26 April 2018 from http://www.fleetowner.com/fleet-management/cargo-theft-now-tougher-nut-crack

at automotive manufacturing plants who relied on parts and materials from across the border. In 1994, a 24-day trucking industry teamsters strike cost the industry an estimated $23 million a day, while factory and retail stores experienced an inventory shortage and prices increase on goods.[59] [60]

8.3 Economic Impact

If retail charging stations are compromised, it becomes possible to intercept and collect personally identifiable information (PII), such as account numbers, credit card numbers, etc. This information could be used for small-scale energy theft and credit card fraud. For commercial fleet accounts, it would be possible to stage larger scale energy thefts.

Given the current design of smart grid infrastructure, it is possible to manipulate grid loads to impact electricity prices. This could be achieved either through the network load balancing algorithms, which provide input into the pricing models, or an attack on the price signal and optimization algorithms used by the EVSE provider, all of which are updated in real-time. The current vision for commercial electric vehicles includes two-way exchange of power, i.e. a vehicle could potentially feed power back into the grid. Even if there were only a one-way exchange of power, a coordinated increase in load could increase electricity prices as well. Any type of artificial impact on the pricing signals and algorithms could have a huge economic impact on fleets who rely on electric vehicles, as well as, other unrelated industries.[61] [62]

8.4 Power Grid Stability

When intelligently connecting large numbers of heavy vehicle high-capacity batteries to the grid, it is possible that maliciously coordinated charging could overload and/or destabilize the grid. While in most cases it would cause local equipment, such as transformers, to short out, it is possible it might reach further. The power required for the rapid charging of heavy vehicles would require upgrades to local infrastructure that would allow more power to flow through the endpoints. This added capacity could be used against the grid in a manner than otherwise intended.

The charging stations reviewed during our research were a one-way draw of power to charge the vehicle, with bi-directional power control systems. There has been some discussion in the reviewed literature that would allow for bi-directional power flow but nothing substantive due to concerns of load balancing. It is feasible that some charging synchronization systems could try to utilize existing fully charged vehicle batteries as an additional source of power during peak charging events.

---

[59] [IM09] Sanchez, Jesus, *Teamsters Strike Shuts Down 22 Trucking Firms*, LA Times, (07 April 1994). Retrieved 10 May 2018 from http://articles.latimes.com/1994-04-07/news/mn-43292_1_trucking-firms

[60] [IM10] Watson, Rip, *Teamsters, TMI Reach Tentative Settlement Union Officials to Vote Today on Package*, Joc.com, (28 April 1994). Retrieved 10 May 2018 from https://www.joc.com/teamsters-tmi-reach-tentative-settlement-union-officials-vote-today-package_19940428.html

[61] [G06] ChargePoint, Inc., "*Next-Generation Grid Communication for Residential PEVs (EPC-14-078)*," Presentation slides for the Fourth Annual California Multi-Agency Update on Vehicle-Grid Integration Research, Sacramento, CA (05 December 2017). Retrieved on 25 April 2018.

[62] [P07] *December 2017 Edition: Real-Time vs. Day-Ahead Pricing*, AEP Energy, (05 January 2018). Retrieved 01 May 2018 from https://www.aepenergy.com/2018/01/05/december-2017-edition/

Pushing power back onto the grid or local charging station networks becomes more problematic with fleets of heavy vehicles as they have bigger batteries and larger power connections to the grid. If not properly balanced, or if the charging infrastructure were to be subverted, this could destabilize the grid and cause serious power issues over extended geographical areas.

Connecting vehicles and their owners, with all their varied attack surfaces, to charging stations will provide additional attack vectors into the grid system itself. Users with mobile phone applications communicate over the internet with accessible addresses connected to cloud-based EV charging billing services of 3rd party integrators that control the EVSEs. The EVSEs themselves connect with everything from Bluetooth, Wi-Fi, ZigBee, to RFID, as well as a number of hardwired connections that all eventually tie into the local or remote load management systems. All of these new connection points to the grid have far-reaching implications and a significant increase in complexity in comparison to even newer AMI smart grid technology.

It is possible that general ransomware could spread into other systems due to common architecture such as processors, embedded system operating systems, etc. It is important to note that the spread could go in various directions, e.g. from vehicle to power grid, energy management systems to vehicles, etc., spreading malware in previously untested directions. For example, in 2003 an outbreak of the Blaster/Slammer worm affected many utility power grid systems, including an Ohio nuclear plant operated by FirstEnergy Corp. [63] [64] As a result of an increasingly connected architecture, with many touch points to open systems, it is possible that self-propagating malware could unintentionally affect the stability of grid operations. Malware from a USB drive plugged into a car could exploit the ARM processor in the infotainment unit, which could then spread to the EVSE and up the line due to similar embedded system architectures and operating systems which are ubiquitous but not easily patched.

If the goal is to disrupt transportation, it might be possible to attack grids and, once inside, simulate malicious events at charging stations (or other false positives) to force the provider to terminate services to 3rd party aggregators and/or charging stations. This would be a difficult issue to resolve given the number of charging stations, and the response team would essentially be trying to confirm a negative. This would force a utility provider to do the dirty work of turning off the supply to the EV without requiring the malicious actor to compromise all the systems.

Unfortunately, once a malicious actor or self-propagating malware is on the power grid / utility network, the reach could be all the way back to the power plants. Since the grid network is generally considered to be “isolated,” there are not many defensive layers present due to the need of high speed communication requirements for intelligent power distribution. This means that once the actor or malware is established on the network, they could take out the entire grid along with power producing equipment, and it would be difficult to pinpoint the source of the attack.

[63][H23] Poulsen, Kevin, *Slammer worm crashing Ohio nuke plant network*, SecurityFocus.com, (19 August 2003). Retrieved 01 May 2018 from https://www.securityfocus.com/news/6767/

[64] [H24] Verton, Dan, *Blaster worm linked to severity of blackout*, ComputerWorld.com, (29 August 2003). Retrieved 02 May 2018 from https://www.computerworld.com/article/2571068/disaster-recovery/blaster-worm-linked-to-severity-of-blackout.html

8.5 National Security

The smart grid is already considered critical infrastructure by DHS. While the motor freight transportation industry is considered an important part of the national security picture, it has yet to be formally classified as critical infrastructure. The combination of power grids and transportation industry creates a nexus of mission critical systems and services whose disruption can have significant impacts on national security. Weaknesses in the design and implementation in the electrification of our commercial transportation infrastructure could have a far-reaching impact on national security. This includes:

- Loss of power in far reaching regions
- Ability to destabilize grid and damage power producing assets
- Lack of transportation that would quickly affect fuel, food, potable water, emergency services, etc.

While there are many benefits to the smart grid and vehicle connectivity, it does open up significant risks. The ability to disrupt the country's power and transportation capabilities would be an extremely valuable ability in a conflict with nation states. As such, we should assume that adversaries are already working towards this goal. The recent cyber-attacks against Ukraine utilities has already confirmed that this is the case.

9 Incident Response Coordination

An area of great concern for MD/HDEV and charging infrastructure is incident response and coordination for an attack or malware outbreak inside these newly connected industries. It would be beneficial for stakeholders to be identified according the Responsible, Accountable, Consulted, and Informed (RACI) model for MD/HDEV, EVSE station attacks, or grid attacks. Our research indicates that this has not been done. One reason is that there is an extremely large number of diverse stakeholders who are not normally connected to each other by any other activity or process.

For communication and coordination to be effective during an actual incident there must be predefined and well-publicized communication paths for all stakeholders to be able to consult. The very last thing to be doing during an actual incident is looking up phone numbers and trying to connect with new people.

9.1 Who are the Players Involved?

When evaluating the secure design, implementation, installation, and operation of MD/HDEVs and associated charging infrastructure, a cursory review yields a large number of stakeholders involved throughout the process. The list below is not exhaustive but should provide a good overview:

- DHS
- ICS-CERT / US-CERT
- DOT (NHTSA, FMCSA)
- Automotive ISAC
- Electricity ISAC (E-ISAC)
- NIST
- DOE
- FERC / NERC / NARUC
- NCCIC
- States Public Utility Commission (PUC) and Public Services Commission (PSC)
- Vehicle OEMs, Tier 1s
- Telecommunication Companies
- Telematics providers
- EVSE Manufacturers
- EVSE Operators
- Utility Companies
- 3rd Party Utility Aggregators and Distributors
- Building Energy Management Systems (BEMS) Manufacturers
- Customers (operators of heavy trucks for private and for-hire freight)
- Insurance companies (systemic risk)
- Credit card processors (retail charging)
- Law Enforcement – State Police and Federal (FBI)
- SAE (Vehicle and EVSE standards)
- IEEE (Power standards)
- ISO (Standards)
- UL (Product and component testing)
- National Fire Protection Association (EVSE installations)
- International Code Council (Building standards)
- Local and state governments (Building codes)

9.2 What are their Responsibilities?

Given the sheer depth and diversity of the stakeholders, it is extremely unlikely that all the specific stakeholders could be identified and contacts established for each instance. Just as an example for each entity, e.g. OEM, Utility, etc., we would have to determine what their role is for a list of events such as:

- Vehicle compromise
- EVSE compromise
- Grid takedown
- Cargo Theft
- Standards
- Audit/Compliance
- Supplying power to MD/HDEV
- Paying for utilization

Even if it was possible, there is such a diversity in scenarios that if you tried to develop a RACI matrix it would soon be unworkable. It therefore seems more logical to develop best practices, top down communication paths, and standards that can tailored for each stakeholder.

9.3 Communication Path

To successfully communicate amongst a large heterogeneous group of stakeholders in times of crisis, there must be only a few central coordination points that everyone can feed into and get information from. Based on our industry analysis, there are three obvious candidates that can already communicate with each other and can incorporate all the major stakeholders at a high level. The three organizations would be the Automotive ISAC, Electricity ISAC, and the National Cybersecurity and Communications Integration Center (NCCIC). Improving the communication and collaboration between these organizations, as well as, improving their MD/HDEV and EVSE industry understanding will be critical. Industry and government leaders will need to work with these organizations to create a well-defined reporting flow and awareness campaign.

10 Current Security Measures

There are a number of security measures that are currently utilized to protect the networks, systems, and components included in this domain. Even more are under development. “Security measures” does not only include physical design, implementation, and use of security technology but also processes such as penetration testing. The following section highlights some of the security measures that are presently in widespread use or in the leading edge of development and deployment. The list is not meant to be exhaustive, but rather illustrative.

The categorization below is for illustration purposes only as many of the security measures are used across vehicles, EVSEs, BEMS, and power grid networks. Not all vendors and companies implement the same security measures and in the same way, therefore the cyber security posture will vary between companies and industries.

10.1 Vehicles

A great deal of research and commercial progress has been made in securing the automotive architecture. There have been significant improvements in design, including network segregation and security gateways. In addition, there have been improvements in leading edge technologies such as CAN traffic analysis and encryption. While there are no specific rules and regulations for vehicle cyber security, there are best practices available from both NHTSA and the Auto-ISAC.

Segregation

Rather than relying on a single CAN bus network, vehicles have started to break out and separate communication functions into separate segments. This not only allows groups of ECUs to be separated out, but also provides the ability to use different implementation techniques. For example, FlexRay can be used in one segment while CAN FD or high-speed CAN be used in another. The segments are joined together via a gateway which controls what messages may pass between the different segments. For example, this allows the braking system to be separated from the infotainment system. This makes it much harder for an attacker to pivot inside a particular network segment to a possibly more sensitive network. This helps introduce a measure of risk mitigation and reduction.

One of the reasons segregation and isolation is important is that OEMs source their components and subsystems from multiple vendors. This means that if there is a vulnerability in a component or subsystem from one supplier, it can be somewhat contained inside its own CAN segment, helping isolate it from other components.

Security Gateways

Security gateways are devices that inspect and restrict communication between two different interfaces. They can be used to bridge different CAN networks together or to isolate a particularly vulnerable component, such as an infotainment system. They can either contain a list of approved messages (white listing) or a list of denied messages (black listing). Security gateways are actively being deployed in vehicles today to improve segregation and isolate vulnerable systems.

NMFTA is working with a number of industry participants to develop a data diode which can act as a one-way physical firewall between CAN segments and/or components. Its primary purpose is to provide one-way communication for electronic logging devices from the diagnostic port that may have security problems. This technology can also be applied in other areas where a “listen only” mode would be desirable.

CAN Traffic Analysis (IDS/IPS)

While not commonly deployed into production vehicles yet, there is significant interest in research and product development around intrusion detection and prevention systems for connected vehicles as well as means to secure the communication between ECUs.

Implementation strategies vary according to vendor and researcher. Some look to apply machine learning to CAN message traffic to figure out if there is malicious activity on the CAN bus. Others use pre-defined signatures, which would indicate a compromised system. Other solution providers have products that ensure that the ECUs are only running approved configurations. Other solutions provide the ability to encrypt communication between sensitive ECUs in order to safeguard the communication and only allow communication between authorized components. Some providers, such as CypherFrame, use a combination of technologies, including ECU fingerprinting and machine learning, to monitor and automatically disable potentially compromised components by sending error frames. This causes the CAN stack to disable or use alternative means depending on implementation.

Research into CAN traffic analysis is ongoing for heavy vehicles running J1939. NMFTA has built a CAN bus data repository that holds over 4,000 hours of raw CAN bus data from commercial vehicles in normal operation. NMFTA and the University of Tulsa developed a low cost and unobtrusive CAN bus data recorder that can be connected to the J1939 diagnostic port. We then recruited member carriers to participate in the program by attaching the recorders to their trucks during normal operation. We collected the data in a central repository where it is available for academic and commercial research. At the time of this paper, we have four different teams working on individual research projects inside the research environment that contains over 10 billion CAN messages.

Advanced telematics systems are also using data analytics and vehicle behavioral monitoring to provide an IDS capability across entire fleets. This function is a natural extension of existing logistics optimizations that these systems are capable of doing. Most, if not all, major telematics providers for heavy trucks incorporate data sampling from the vehicle and machine learning technology on back end systems.

While most of these technologies are not widely deployed in vehicles at this time, the rate of innovation and progress is impressive and worth monitoring. There could soon be commercially viable solutions deployed inside vehicles.

Hardware Security Modules

Hardware Security Modules (HSMs) are pieces of hardware with associated software that attaches to the inside of a system (either as a plug-in or as a component on the circuit board). The HSM is purpose-built for security and suitable (meeting FIPS 140-2 standards) for storing sensitive data and provide cryptographic primitives for the core system. Splitting this functionality out from the core processing system can improve the processing for encryption, provide segregation and isolation for security processes, and help protect private keys.

Network Security Architecture Review (NSAR)

As numerous complex systems are deployed and networked together (think corporate network, in-vehicle network, etc.), periodic review of the designed architecture provides insight to how the systems may interact in ways that allow easy compromise of individual systems and the overall network. Examples of this include multi-connected non-security devices, which allow an attacker to traverse from one trust domain to another easily (e.g. from a corporate DMZ or the Internet directly into the internal network), or the ability to flash the ABS module firmware from the Infotainment unit.

Product Security Architecture Review (PSAR)

Like the Network Security Architecture Review, a Product Security Architecture Review provides a periodic assessment of the way a product (ECU, EVSE, and Smart Meter) is intended to operate. Design specifications are used to identify weaknesses in design, due to insecure functionality or lack of sufficient security measures in a product. While a PSAR may use real products for validation, it is focused at the design level.

Security Testing

Penetration Testing (pen-testing) is assessing the attack surface of a system or network of systems to identify potential weaknesses and then iteratively working to exploit them. Pen-testing is a hands-on exercise with real or virtualized systems. Scope can vary significantly, depending on the system(s) being tested and the assessment of risk for given scenarios. For example, pen-testing an ECU may involve network access, as well as, analyzing/testing the components of the circuit-board. Pen-testing a vehicle may focus on the vehicle-network, and it may focus on all aspects of the vehicle. Since discovering all vulnerabilities in complex systems is neither feasible nor affordable, pen-testing strategy is frequently employed, allowing periodic assessments of the same systems, and different systems over time.

Procurement Requirements

As cyber security awareness has started to permeate the industry, cyber security requirements are making their way into the supply chain. OEMs now have specific cyber security requirements that are incorporated into their supplier agreements. As this trend continues, the entire industry will benefit as more subsystems and components become more secure over time.

10.2 Charging Stations

As the design and development of EVSEs is relatively new, manufacturers are able to take advantage of lessons learned from other industries, as well as, incorporate new methods and technologies to secure their devices. These techniques range from network monitoring, gateways, and reach all the way down to the component levels.

Firewalls/Network Intrusion and Detection

EVSEs must often communicate with the internet over cellular connections using traditional network protocols, such as HTTP and HTTPS. This means that they can utilize existing traditional firewalls with network intrusion and detection to protect the device from external remote attacks. The IDS/IPS can block traffic based on known signatures for malicious activity. The firewalls can also restrict traffic to only whitelisted IP addresses, as well as, control and secure DNS lookups. There are a number of light weight solutions that can be incorporated into embedded systems. It is important to note that IDS/IPS usually requires signature updates, unless they are based on static AI models (i.e. Cylance).

Potting

Potting is a technique used for components, especially those in embedded systems, where an electronic component is placed in a form (pot) and then filled with a curable liquid. Not only does this help protect the device from normal environmental factors, it also makes it more resistant to tampering and reverse engineering. However, for a dedicated attacker, potting can provide support and guidance to hold probes in place after drilling through to the traces/chips on the PCB.

Segregation

EVSEs represent a central connection point for vehicles, EVSE vendor's systems, and the power grid. EVSEs can segregate the network and communication paths either logically or physically. This is particularly important for local access ports (serial, USB, etc.), near field protocols (RFID, Wi-Fi, etc.), and remote cellular modems. Separating communication and access by function can help separate various aspects of the systems from others. As discussed previously, this separation provides some measure of isolation, which can help protect one part of a compromised system from another.

Updateable Cryptography

Given the various secure communication methods required by EVSEs, it is important to include the ability to update encryption as the effectiveness of various cipher suites (TLS 1.0, SSL 1.0, etc.) degrade and become obsolete. TLS 1.3 is on the verge of becoming the new production standard, as both TLS 1.0 and TLS 1.1 have been deprecated. Based on hard lessons from the obsolescence of TLS 1.0 in the computer industry, updateable cryptography is new a best practice.

10.3 BEMS/EVSE Vendors

Our research indicates that BEMS and EVSE vendors are deploying cloud-based solutions for their aggregated operations and controls. This means that they are able to deploy traditional network security tools and systems for their back-end systems. This includes things such as firewalls, IDS/IPS, web application firewalls, SEIM aggregation and analysis, data analytics, and many other tools, technologies, and techniques. It is critically important that the back-end systems of these vendors are secure since they tie together large numbers of embedded control systems. A review of all available network security tools, systems, and processes is outside the scope of this document.

10.4 Power Grids

As discussed previously, the Bulk Electric Systems (BES), aka the power grid, is essentially a very large set of purpose built connected industrial control systems. BES systems operate a number of ICS, network, and communication protocols. Operators deploy BES specific firewalls which can block other traffic based on industry specific equipment and configurations. The utilities also deploy traditional network security tools, such as network and host-based IDS/IPS, SEIM collection and analysis, encryption, two-factor authentication, and monitoring solutions. BES operators also employ security assessments and penetration testing to help identify, mitigate, and reduce risk.

The NERC Critical Infrastructure Protection (CIP) plan is a set of requirements designed to secure the assets required for BES operation. They mandate a number of cyber security and physical security requirements. These requirements are fairly specific and low level. For those who are familiar with the credit card processing industry, these requirements are not dissimilar from PCI DSS requirements. A complete review of these requirements is outside the scope of this document, but more detailed information can be obtained from NERC.[65] NIST has also published guides and reports on securing the smart grid that can provide some perspective on how power grids are currently protected.[66]

[65] [P10] NERC, *CIP Standards*, North American Electric Reliability Corporation, (n.d.). Retrieved 03 May 2018 from https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

[66] [G11] NIST. *NISTIR 7628, Guidelines for Smart Grid Cyber Security*, (September 2010). Retrieved 27 April 2018 from https://www.nist.gov/sites/default/files/documents/smartgrid/nistir-7628_total.pdf

11 Research and Standards Activity

There is a great deal of ongoing research and standards activity by many individuals, groups, and organizations. The following is not an exhaustive list but provides some reference of where interesting work is presently ongoing.

11.1 Idaho National Labs

Kenneth Rhode of Idaho National Labs (INL) has been conducting significant research into the cyber security of EVs, EVSEs, and the power grid as part of a multiyear research program within the Grid Modernization Laboratory Consortium. This has included full EV and EVSE security assessments as well as the development of potential cyber security technology including the Diagnostic Security Module (DSM) Framework. The research work has not been completed and further research and results are expected.

There has been a body of EVSE security testing research conducted by DOE's Idaho National Laboratory (INL):

- **2014-2015**[67]: INL conducted unbiased and independent EVSE testing for efficiency, reliability research, and cybersecurity posture (i.e. remote compromise, unauthorized access, firmware modifications, potential grid impact) on four (4) pre-production systems delivered by Siemens, Eaton, GE, and Delta. Listed below are some potential cybersecurity issues which pertain to EVs:
    - Software Development mistakes (i.e. implementation of "complex" code on a small embedded device leads to poor decision making)
    - Sanity checking of remote input lacking
    - Processes are executed with extensive privileges (i.e. root)
    - Memory corruption vulnerabilities (i.e. ARM, X86)
    - Poor web application implementation SQL injection, cross-site scripting (XSS), input validation, and insecure credentials
    - Billing and price information were manipulated
    - Remote updating was very poorly implemented
    - Malicious firmware lead to full compromise of all units from one vendor

[67] [C23] Francfort, Jim, INL Efficiency and Security Testing of EVSE, DC Fast Chargers, and Wireless Charging Systems, US DOE (14 May 2013). Retrieved on 15 May 2018 from https://www.energy.gov/sites/prod/files/2014/03/f13/vss096_francfort_2013_o.pdf

- **2016-2018**[68]: INL conducted cybersecurity testing on two production Level 2 EVSEs and the testing results were only shared with the vendors. INL also conducted cybersecurity testing on a DC Level-2 Fast Charger (DCFC) with both a CHAdeMO and a SAE J1772-Combo cordset. Cybersecurity testing revealed the following findings:
    - A compromised Plug-In Electric Vehicle (PEV) charge module can infect the DCFC vehicle controllers and local servers and vice versa
    - A compromised PEV is not only a potential safety concern, but it is also a grid network access concern. The biggest potential problem is for a coordinated charging event that causes widespread disruption of the grid
    - The cybersecurity testing identified some unknown issues that need to be resolved (e.g. who owns the EVSEs and network connections, are EVSEs considered part of the Utilities network perimeter, and can Utilities handle increased electrical loads)

11.2 Pacific Northwest National Lab

In 2013 and 2014, the Pacific Northwest National Laboratory (PNNL), in conjunction with DOE, SAE, and University of Vermont, conducted research into vehicle communications and charging controls. The focus of the research was the development of intelligent charging coordination to improve efficiencies and optimize performance. They were able to obtain a significant increase in efficiency. This information was distributed and incorporated by SAE into J2847/1, J2847/3, and J2836/5. PNNL also provided input to J2831/1, J2836/2, and J2847/2 for inclusion into the Self-Generation Incentive Program (SGIP) catalog of standards for smart grid interoperability. This research indicated that significant optimization can be achieved through intelligent coordination that supports the premise of future BEMS and LEMS coordination for EV charging.

Recently, PNNL researchers have developed a new electrolyte solution that does not corrode the electrodes in lithium-metal batteries. A lithium-metal has double to triple the storage capacity of a lithium-ion battery.[69]

11.3 Lawrence Berkeley National Laboratory

Recently, the energy analysis and environmental impacts division of Lawrence Berkeley National Laboratory, developed software tools to enable simulation of transportation-electric systems.

The collection of tools known as the BEAM Framework (Behavior, Energy, Autonomy, and Mobility), was used to simulate PEV mobility, energy consumption, and spatiotemporal charging demand. BEAM was applied to the San Francisco Bay Area and used to conduct a preliminary calibration and validation of its prediction of charging load based on observed charging infrastructure utilization for the region in 2016. In order to view the report, see [R08].

---

[68] [C24] Chugg, Jonathan and Rohde, Kenneth, CAN Bus Security Across Multi-Sector Platforms, VSATT (October 2015). Retrieved on 15 May 2018 from https://avt.inl.gov/sites/default/files/pdf/presentations/VSATTOctober2015CANBusOverview.pdf

[69] [R08] Sheppard, Andrew, et al., *Modeling plug-in electric vehicle charging demand with BEAM: The framework for behavior energy autonomy mobility*, Energy Analysis and Environmental Impacts Division Lawrence Berkeley National Laboratory, (May 2017). Retrieved 03 May 2018 from https://eta.lbl.gov/sites/default/files/publications/lbnl-2001018.pdf

Lawrence Berkeley National Laboratory is partnering with Idaho National Laboratory in a project to provide historical PEV charging load profiles from real-world PEV charging that was observed in two major charging infrastructure demonstrations: The EV Project and ChargePoint America.

It will also provide defensible future projections of PEV load profiles resolved temporally (by time of day) for a certain number years (TBD) into the future and spatially by region in California, for:

- any scenario for the number of PEVs deployed by year
- any assumptions on the type and fleet mix of PEVs that are deployed (e.g. EVs and PHEVs)
- any assumptions on how/when people charge their vehicles, e.g. home vs. work vs. public charging, L1 vs. L2 or faster charging

11.4 SAE International (SAE)

SAE International is working on a number of standards that can have an impact on EV and EVSE design and development. Current publications such as J3061 and its successor, the SAE/ISO Joint Standard on Automotive Cybersecurity, have a direct impact on secure design processes. Additionally, there are a number of new standards currently under development, such as J3101 (Hardware Protected Security). There is also a standards effort underway to harden and secure the diagnostic port (J3138) and a standard for securing devices that connect to the diagnostic port (J3005/1 and J3005/2).

Other Standards of Interest

A number of interesting SAE standards on the subject include:

- **J1772** - Electric Vehicle and Plug-in Hybrid Electric Vehicle Conductive Charge Coupler
- **J2847/1** - Communication between Plug-in Vehicles and the Utility Grid
- **J2847/2** - Communication between Plug-In Vehicles and Off-Board DC Chargers
- **J2931/1** - Digital Communications for Plug-in Electric Vehicles
- **J2931/4** - Broadband PLC Communication for Plug-in Electric Vehicles
- **J2954** - Wireless Power Transfer for Light-Duty Plug-In/Electric Vehicles and Alignment Methodology
- **J3105** – Electric Vehicle Power Transfer System Using a Mechanized Coupler

11.5 IEEE

The Institute of Electrical and Electronic Engineers (IEEE) organization is working on a number of different standards and initiatives for the EV industry. There are a number of current standards, including 2690, the Standard for Charging Network Management Protocol for Electric Vehicle Charging Systems. IEEE also has a number of ongoing initiatives including certification programs for the rapid charging and dynamic DC charging standards.[70]

Other Standards of Interest

- **2030.1.1-2015** - IEEE Standard Technical Specifications of a DC Quick Charger for Use with Electric Vehicles
- **2030.5 (formally SEP 2.0)** - Adoption of Smart Energy Profile 2.0 - Defines the mechanisms for exchanging application messages, the exact messages exchanged, including error messages, and the security features used to protect the application messages

11.6 IEC

The International Electrotechnical Commission (IEC) publishes standards for a wide array of electrotechnologies. Together with the ISO and ITU, the IEC has been successful in developing international standards for electric technology across over 82 nation members. In relation to EV and MD/HDEV's, the IEC has established the TC 69 to prepare international standards for road vehicles and electric industrial trucks.[71] Currently under development are the IEC 63110 and IEC 63119, which pertain to charging stations.

- **IEC 63110** – International standard protocol for the management of electric vehicles charging and discharging infrastructures. Places a strong emphasis on energy management and enabling multi-vendor networks.
- **IEC 63119** – Information exchange for electric vehicle charging roaming service. Developed to support internetwork roaming and peer-peer or clearinghouse communication.
- **IEC 61851** – An international standard under development for electric vehicle conductive charging systems
- **IEC 62196** – An international standard for plugs, socket outlets, and vehicle couplers for conductive charging of electric vehicles
- **ISO/IEC 15118** - Road vehicle-to-grid communication interface standard

For more information on IEC TC 69 efforts, please see [C21].

[70] [R06] IEEE, *IEEE Forms Committee to Develop a Certification Plan for Rapid Charging of Electric Vehicles and Approves Standard Revision on Dynamic Dc Charging up to 400kw*, BusinessWire.com, (28 November 2017). Retrieved 02 May 2018 from https://www.businesswire.com/news/home/20171128005135/en/

[71] [C22] *TC 69 Electric Vehicles and Electric Industrial Trucks*, International Electrotechnical Commission, (n.d.). Retrieved 09 May 2018 from http://www.iec.ch/dyn/www/f?p=103:7:15337487968483:::FSP_ORG_ID,FSP_LANG_ID:1255,25

11.7 OCPP

The Open Charge Point Protocol (OCPP) and the Open Smart Charging Protocol (OSCP) standards from the Open Charge Alliance are widely adopted standards for communication between vehicles and EVSEs. The current version is 1.5 and will be updated to version 1.6 in 2018 to include more guidance on cyber security. Additionally, version 2.0 is presently under development, and it will include more specific cyber security recommendations. The cyber security related portions can be found in the functional block A and functional block L01 of the standard. Additional resources can be found in [C17] and [C18].

11.8 ElaadNL

The E-laad Foundation established a network of more than 3,000 public charging stations for electric cars across the Netherlands. In 2014, the foundation split up its activities into two separate platforms: ElaadNL and EVnetNL. EVnetNL is responsible for managing the existing charging points together with municipal partners. ElaadNL continued the foundations efforts to expand research and stimulate innovation regarding smart charging and the use of sustainable energy for electric vehicles. ElaadNL has a number of ongoing research activities in this area including cyber security. In 2016, the European Network for Cyber Security (ENCS) developed a set of EV charging system security requirements on behalf of ElaadNL. Version 1.0 of these specifications can be referenced from their website https://www.elaad.nl/projects/cybersecurity/ [R09].

11.9 US Department of Energy

The U.S. Department of Energy (DOE) Vehicle Technologies Office (VTO) combines research and development, outreach and education, and partnership-building. Activities by the DOE/VTO are to:

- Improve the competitive position of U.S. industry and create jobs through American innovation
- Enhance energy security by reducing our dependence on foreign oil
- Save money by cutting fuel costs for American families and businesses
- Protect our health and safety by mitigating the impact of energy production and use on climate change.

The DOE/VTO accomplishes these outcomes by having partnerships among the private sector, the Federal government, states and communities, national laboratories, universities, nongovernmental organizations, and individual consumers. Some of these partnerships are:

- the U.S. DRIVE light-duty research and development partnership
- the Memorandum of Understanding with Edison Electric Institute
- the Clean Cities network of local coalitions

In addition to collaborating with outside stakeholders, DOE/VTO works closely with other DOE agencies, such as the Office of Science, Office of Electricity, and ARPA-e on research that focuses on development of advanced batteries, electric drive systems, and lightweight materials. For further reading on DOE/VTO's role in the EV environment see: https://www.energy.gov/eere/electricvehicles/electric-vehicles and https://www.energy.gov/eere/electricvehicles/about-electric-vehicles.

11.10 US CERT

Stemming from the 1963 presidential memorandum that established the National Communications System, US-CERT has some existing guidelines for effectively defending industrial control systems. It also contains a collection of best practices for industrial control systems that could all be applicable to the general infrastructure for EV, EVSEs and associated infrastructure. Additional resources for US-CERT guidelines and practices can be found in [G21] and [G22].

In addition, US-CERT publishes cyber security alerts. These technical alerts describe the systems affected, provide an overview of the issue, a description of the attack/vulnerabilities, what the possible impacts could be, and, whenever possible, solutions for the vulnerability/attack. For example, alert TA18-074A, first published on March 15, 2018 is a technical alert that describes Russian Government cyber activity targeting energy and other critical sectors.[72] For further reading on US-CERT and their catalogs of alerts, bulletins, and tips see: https://www.us-cert.gov/about-us

11.11 National Institute of Standards and Technology (NIST)

NIST is a non-regulatory government agency and standards laboratory that promotes innovation and the development and use of standards.

Some of the work NIST has done related to EVs:

- **7628 Guidelines for Smart Grid Cybersecurity** - An analytical framework that organizations can use to develop effective cyber security strategies tailored to their particular combinations of Smart Grid-related characteristics, risks, and vulnerabilities
- **Handbook 44-Section 3.40-Electric Vehicle Fueling Systems** (tentative code) - Code applies to devices, accessories, and systems used for the measurement of electricity dispensed in vehicle fuel applications wherein a quantity determination or statement of measure is used wholly or partially as a basis for sale or upon which a charge for service is based
- **Handbook 44-Section 5.55-Timing Devices** - Code applies to devices used to measure time during which services are being dispensed. This code also applies to Electric Vehicle Supply Equipment (EVSE) when used to assess charges for time-based services in addition to those charged for electrical energy

[72] [H51] United States Computer Emergency Readiness Team, *Alert (TA18-074A) Russian government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors*, Department of Homeland Security, (last revised 16 March 2018). Retrieved 04 May 2018 from https://www.us-cert.gov/ncas/alerts/TA18-074A

11.12 Underwriters Laboratories (UL)

A name long familiar with electrical devices, UL is a global safety and consulting agency that works with a wide array of commercial stakeholders to support responsible design and production of goods, solutions, and innovations.

Some of the UL standards work done related to the EV environment:

- **UL2202-Standard for Electric Vehicle (EV) Charging System Equipment -** Conductive charging system equipment intended to be supplied by a branch circuit of 600 volts or less for recharging the storage batteries in over-the-road electric vehicles (EV). The equipment includes off board and on-board chargers
- **UL2231-Standard for Personnel Protection Systems for Electric Vehicle (EV) Supply Circuits -** Requirements cover conductive charging system equipment intended to be supplied by a branch circuit of 600 volts or less for recharging the storage batteries in over-the-road electric vehicles (EV). The equipment includes off-board and on-board chargers
- **UL2251-Standard for Plugs, Receptacles and Couplers for Electric Vehicles -** Requirements cover EV plugs, EV receptacles, vehicle inlets, vehicle connectors, and EV breakaway couplings, rated up to 800 amperes and up to 600 volts AC or DC. These devices are intended for use with conductive electric vehicle supply equipment (EVSE) and are intended to facilitate the conductive connection from the EVSE to the vehicle.
- **UL2271-Batteries for use in Light Electric Vehicle (LEV) Applications -** Requirements cover electrical energy storage assemblies (EESAs), such as battery packs and combination battery pack-electrochemical capacitor assemblies, and the subassembly/modules that make up these assemblies for use in light electric-powered vehicles (LEVs), as defined in this standard.
- **UL2594-Electric Vehicle Supply Equipment -** Conductive electric vehicle (EV) supply equipment with a primary source voltage of 600 V AC or less, with a frequency of 50 or 60 Hz, and intended to provide AC power to an electric vehicle with an on-board charging unit.

11.13 CyberTruck Challenge

The CyberTruck Challenge is a non-profit event with a twin focus – to educate and excite the next generation workforce about the career potentials in heavy truck transportation cyber security; and also, to help foster and support a community of interest among technical workers from both OEMs and the supplier community, government officials, carriers, academics, college students, and the researcher/hacker community. The goal is for enhanced engagement, improved solutions, and a more secure transportation system.

The Challenge is strictly industry friendly. The event's purpose is to provide helpful contacts and an intense, challenging, and unique real-world training environment.

The organizers are planning on adding electric vehicles in 2019 and 2020. This will include cyber security components of inductive charging and charging stations. The organizers are engaged with different government groups to support this future training with engineers, trainers, and equipment. For information and to get involved, please see their website www.cybertruckchallenge.org.

12 Recommendations

The following are recommended actions, activities, and projects to support MD/HDEV cyber security gaps and support risk mitigation activities.

12.1 Immediate Stakeholder Actions

The following sections provide some guidance on what actions various stakeholders can take immediately to reduce their risk profile, increase their cyber security posture, and better prepare for potential cyber threats. The sections on protecting vehicles, networks, and incident response are adapted from the NMFTA white paper "A Survey of Heavy Vehicle Cyber Security," included as Appendix D to this document. In general, there are a number of NIST standards that can be helpful, including the NIST SP 800 series as well as the NIST Framework and NIST 800-60. We also recommend the *Critical Security Controls for Effective Cyber Defense* by the Center for Internet Security. 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.[73]

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 actions that stakeholders can take responsibility for 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. Ask if your vendor has a vulnerability disclosure program. A vulnerability disclosure program allows for vulnerabilities discovered by researchers, and other external entities to be reported, tracked, and mitigated.
- **Established Maintenance Plans** – Establish documented maintenance plans for the vehicles and EVSE equipment, 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. 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.

[73] [G23] Center for Internet Security, *Powerful Best Practices*, CISsecurity.org, (n.d.). Retrieved 03 May 2018 from https://learn.cisecurity.org/20-controls-download

- **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 will see features such as convoy platooning and autonomous heavy vehicles on highways soon. 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.

Protect Your Networks

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. 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, EVSEs, and grid components 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, EVSEs, and grid components 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.

Protect Your Products

If you are developing products for the EV and EVSE space it is incumbent on you to follow best practices and include cyber security as part of the design. There are a number of good references, including J3061[74] (soon to be replaced by joint SAE/ISO standard) as well as NIST Framework for Improving Critical Infrastructure Cybersecurity,[75] that can be consulted when designing, testing, and deploying EVSEs and associated infrastructure.

The most important first step would be to get a professional cyber security risk assessment. This will allow you to determine a baseline for your cyber security posture. From there, it is possible to mitigate and reduce risk and improve the cyber security posture over time. As demonstrated from previous sections it is also critically important to build a supply chain with cyber security integrated into the process. Do you have a supply chain worth believing in?

Incident Response Plan

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.

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 should also include communication, coordination, and contact information so there is no ambiguity on who needs to be contacted and how they can be reached. Incident response plans should also be tested and updated regularly. It is highly recommended that all industry stakeholders immediately start working with each other to develop an incident response plan.

[74] [G19] *Cybersecurity Guidebook for Cyber Physical Vehicle Systems*, SAE International, (14 January 2016). Retrieved 02 May 2018 from https://www.sae.org/standards/content/j3061_201601/

[75] [G20] *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*, National Institute of Standards and Technology, (16 April 2018) Retrieved 02 May 2018 from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

NMFTA has previously provided a basic outline of an incident response plan in other published documents. The figure below was the result of a working group from an NMFTA Heavy Vehicle Cyber Security workshop.

Preparation	Create team Establish communication plan and crisis management structure Conduct exercises
Identification	Identify if attack has occurred or is ongoing Identify the impacted assets
Assessment	Assess the scope, impact and risk of the incident Investigate the cause and establish first course of action Collect forensics and critical data for next steps Create profile of affected units
Containment	Minimize and isolate the damage or risk Use profile to strategically contain affected units Implement contingency plans to maintain continuity of business
Eradication	Determine the root cause Conduct analysis on forensics data collected and assets Restore / rebuild systems affected
Recovery	Implement irrevocable corrective actions Restore normal operations
Follow-up	Lessons learned collected and incident response plan is updated Identify other units with similar vulnerability and create remediation plans

Figure 12 - Overview of an Incident Response Plan

Incident response plans will vary by industry and there are a number of public resources available on the subject including NIST publication 800-61r2 and ICS/SCAC Systems – DHS Recommended Practice: Developing an Industrial Control Systems Cybersecurity Incident Response Capability.[76] [77]

[76] [G24] Cichonski, P., Millar, T., Grance, T., & Scarfone, K., *Computer Security Incident Handling Guide Special Publication 800-61 Revision 2*, National Institute of Stands and Technology, (August 2012). Retrieved 03 May 2018 from http://dx.doi.org/10.6028/NIST.SP.800-61r2

[77] [G25] Control systems Security Program, *Recommended Practice: Developing an Industrial Control Systems Cybersecurity Incident Response Capability*, Department of Homeland Security National Cyber Security Division, (October 2009). Retrieved 03 May 2018 from https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/final-RP_ics_cybersecurity_incident_response_100609.pdf

12.2 EVSE Cyber Security Best Practices

In August 2017, the European Network for Cyber Security (ENCS), commissioned by ElaadNL, developed a public document titled, “EV Charging Systems Security Requirements”. The ENCS/ElaadNL EV Charging Systems Security Architecture provides an EVSE system reference architecture describing the devices, functionalities, communication interfaces between the systems. For more information, see [C19] and [R27].

12.3 Inter-Industry and Government Stakeholders Working Group

To establish clear communication and encourage collaboration in the field of MD/HDEV and EVSE cyber security, an inter-industry and government agency working group needs to be established. This working group should include representatives from power producers, power distributors, 3rd part aggregators, EVSE manufacturers, heavy vehicle OEMs, Tier 1s, as well as commercial fleet operators. The Information Sharing and Analysis Centers (ISACs) for the automotive (Auto ISAC) and electricity sectors (E-ISAC) should also be included. Collaboration will also require the involvement of responsible government agencies such as US DOE, DOT, and other various agencies that have regulatory jurisdiction so they can provide guidance and keep up to date on ongoing industry efforts.

12.4 Identify and Expand Research Facilities

While there are some existing research facilities, such as the DOE national labs that are currently capable of conducting research and testing on MD/HDEV and EVSEs, more locations and facilities are needed. To have transparent research, testing, and evaluations of the heavy electric vehicles we will need to map out and invest in our research infrastructure. The first step would be to catalog all existing facilities, evaluate their potential, and determine what upgrades and/or additions would be required to meet the needs of our industries.

The most logical approach to increase research and testing capabilities would be to make investments into existing facilities and centers of excellence. This effort can be funded through government grant programs, joint public private partnerships, or through entirely private means. For example, the University of Tulsa, which is a close partner of the NMFTA Heavy Vehicle Cyber Security Program, has an existing substation research facility that can be upgraded and improved to conduct research and testing. The University of Tulsa also has dedicated labs, facilities, and a garage. They are presently looking at test range space that could accommodate cyber testing of large vehicles in motion.

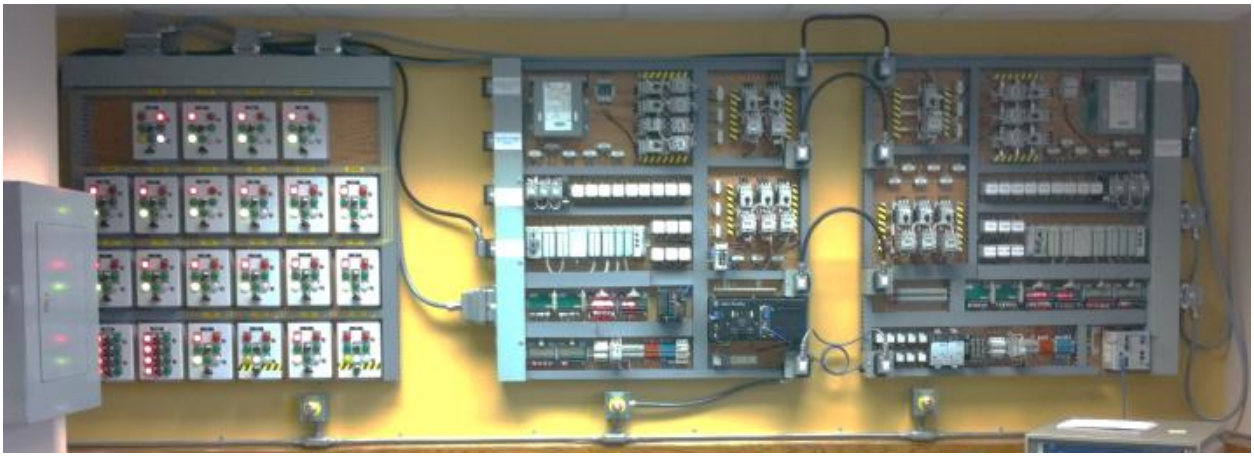


Figure 13 - Ring-type electric power substation testbed located in the Henneke building at the University of Tulsa

Figure 14 - The TU Automotive Research Center in the forefront and the Henneke Building across the street to the left of the photograph

This facility is an example of an excellent potential research facility that can be upgraded with minimal effort and expense. Given the expected dramatic growth in these technologies, we need to identify additional candidates as well to ensure that there is enough research and lab capacity to meet our needs so that we may properly understand all the issues and cyber security concerns for this complex issue.

13 Recommended Research Assessment and Pilot Projects

13.1 xFC/DC Chargers Cyber Security Threat and Risk Assessment

Medium and heavy-duty EVs, especially over-the-road tractor-trailers, will likely require a charging infrastructure with charge rates of 1MW or higher. These vehicles will have significantly larger batteries than light-duty passenger EVs and require much longer ranges than 400 kW charging provided by xFC chargers can support. With power transfer rates of 1MW and higher, it is anticipated that automated charging, whether conductive or inductive, will be required to eliminate safety concerns with vehicle operators handling the recharging equipment. Since the vehicles themselves are still in the development stage, charging equipment manufacturers may be reluctant to invest in the research needed to develop the hardware and control systems that will be required for these 1MW+ chargers.

High power charging events could have an impact on the electric grid stability and reliability, and there are major cyber security concerns.

Project Summary:

Research should be conducted to develop and validate techniques and technologies that provide cyber resilience to xFC units with power transfer rates of 300kW and above, as well as other to vehicle chargers. It is imperative that an "*xFC/DCFC Cybersecurity Threat and Risk Assessment*" on MD/HDEV charging be conducted by the US Trucking industry. The NIST 800 Series provides cost-effective methods for optimizing the security of information technology (IT) systems and networks in a proactive manner. The publications cover all NIST-recommended procedures and criteria for assessing and documenting threats, vulnerabilities, and the implementation of security measures to minimize the risk of adverse events. The publications can be useful as guidelines for enforcement of security rules and as legal references in case of litigation. In general, the NIST 800 series considers MD/HDEV and the electric charging ecosystem an "information system" and recommends identifying the assets of the information system to protect and minimize the impacts of compromises to those assets. In addition, attack vectors and the assets that would be most desired by an attacker need to be defined by conducting threat modeling. The team should have experience with vehicle charging cyber security, high power charging equipment operations and controls, and grid cyber security.

Project Complexity: Medium-High

Leveraging Opportunities: FY19 INL and other National Labs FOE Projects

Deliverable:

- *xFC/DCFC Cyber security Threat and Risk Assessment*

ROM Cost Estimate: TBD

13.2 Secure EVSE Over-the-Air (OTA) Firmware Update Pilot

EVSEs have or will have Over-the-Air (OTA) firmware update and remote flash capabilities, for example, ChargePoint's EVSE[78] and Siemen's EVSE[79]. OTA update capability is typically insecure, for example, software repositories run by major organizations such as Adobe, Apache, Debian, FreeBSD, GitHub, Linux, Microsoft, Opera PHP, RedHat, RubyGems, SourceForge, and WordPress repositories have all been compromised via their OTA functionality that was lacking cyber security protections.

One candidate for use in secure OTA is the Open Charge Point Protocol (OCPP). OCPP is the product of a global consortium of public and private EV infrastructure leaders who are promoting an open standard approach to cyber security as it applies to the EVSE. It has become the de facto standard in over 10,000 charging stations worldwide. For further information on OCPP see: http://openchargealliance.org/

Project Summary:

For this project, there will be three phases:

- Phase 1: Investigate EVSE Firmware Update Mechanisms
- Phase 2: OTA Firmware Update Framework Selection
- Phase 3: Secure EVSE OTA Pilot Demonstration and EVSE OTA Cyber Security Guidance Development

Phase 1: Investigate EVSE Firmware Update Mechanisms

Investigate and understand the current and future EVSE market which includes xFC and DCFC chargers for Commercial HDs (class 7 and 8) and "last mile" MD E-Trucks and plans to implement OTA firmware updates and if cyber security protections to address potential vulnerabilities (e.g. lack of digitally signed software and encryption) have been or will be implemented. Document the findings in a White Paper.

Phase 2: OTA Firmware Update Framework Selection

An analysis and investigation to determine the most suitable OTA Firmware update framework and architecture will be conducted and the recommendations will be documented in a White Paper.

There are at least two Secure OTA frameworks that could be implemented for EVSE Firmware Updates:

- **Uptane:** Uptane is the first compromise-resilient software update security system for the automotive industry that was funded by DHS Science and Technology (S&T) Cybersecurity Division (CSD), developed by New York University Tandon School of Engineering (NYU), the University of Michigan Transportation Research Institute (UMTRI), and the Southwest Research Institute (SWRI). It was designed in collaboration with major vehicle manufacturers and suppliers responsible for 78% of vehicles on U.S. roads, as well as government regulators. Unlike other software update security systems (e.g., SSL / TLS, or signing updates with a single offline GPG / RSA key), Uptane addresses a comprehensive threat model. It is designed to make it

[78] [C23] ChargePoint, Inc., *CT4000 Family*, ChargePoint.com (n.d.). Retrieved 27 April 2018 from https://www.chargepoint.com/products/commercial/ct4000/

[79] [C07] Siemens, *New Wi-Fi enabled VersiCharge™ SG electric vehicle charging stations*, paper is version RPFL-VCSGD-0915, (2015). Retrieved 27 April 2018 from https://www.downloads.siemens.com/download-center/Download.aspx?pos=download&fct=getasset&id1=BTLV_44824

extremely difficult for attackers to be able to install malware on all vehicles maintained by a manufacturer, even if attackers have compromised some keys used to sign updates. At the same time, Uptane has been designed to be extremely flexible, so as to accommodate a wide variety of deployment scenarios and other domains. It allows for on-demand customization of updates installed on vehicles. In 2017, Uptane is already being adopted by several suppliers. Among the public adopters are Lear Corporation and Advanced Telematic Systems / HERE Technologies.[80]

Uptane's primary goal is to create a software update mechanism for vehicles capable of retaining the strongest level of security possible, even if said vehicle is attacked by an intelligent and determined adversary. To the extent that is practical, defense in depth should be employed to force an attacker to need to compromise many different systems (which are protected in diverse ways) to achieve a goal.

- **Internet Engineering Task Force (IETF) IoT Firmware Update Architecture:** The IETF develops and promotes voluntary Internet standards, in particular the standards that comprise the Internet protocol suite (TCP/IP). On November 17, 2017, IETF published their "IoT Firmware Update Architecture",[81] their proposal — if approved — puts forward a series of ground rules that IoT device makers could implement when designing the firmware update mechanism for their future devices. The proposed rules are nothing out of the ordinary, and security experts have recommended and advocated for most of these measures for years. Some hardware vendors are most likely already compliant with the requirements included in this IETF draft. The update mechanism must work the same even if the firmware binary is delivered via Bluetooth, Wi-Fi, UART, USB, or other mediums.

NEMA and NIST documents provide a good framework to develop "secure" EVSE OTA requirements and process:

- **NEMA Smart Grid Standards Publication SG-AMI 1-2009 - *Requirements for Smart Meter Upgradeability*, December 2016** defines functional and security requirements for the secure upgrade of Smart Meter/AMI for both local and remote for industry stakeholders such as regulators, utilities, and vendors.[82]
- **NISTIR 7823: Advanced Metering Infrastructure Smart Meter Upgradeability Test Framework, March 2015** describes conformance test requirements that may be used voluntarily by testers and/or test laboratories to determine whether Smart Meters and Upgrade Management Systems conform to the requirements of NEMA SG-AMI 1-2009**.** For the publication, see reference [G10].

[80] [G08] Advanced Telematic Systems, *ATS is integrating the Uptane security framework for over-the-air software updates to connected websites*, AdvancedTelematic.com, (June 2017). Retrieved 27 April 2018 from https://advancedtelematic.com/en/press-releases/ats-is-integrating-the-uptane-security-framework-for-over-the-air-software-updates-to-connected-vehicles.html

[81] [G09] Moran, B., Meriac, M., Tshofenig, H., *A Firmware Update Architecture for Internet of Things Devices draft-moran-suit-architecture-03*, this paper is a 3rd internet draft published by Arm Limited, (05 March 2018). Retrieved 27 April 2018 from https://tools.ietf.org/html/draft-moran-suit-architecture-03

[82] [C28] *Caskey, J., et al., NEMA Smart Grid Standards Publication SG-AMI (R2015): Requirements for Smart Meter Upgradability, National Electrical Manufacturers Association, (2015). Retrieved 04 May 2018 from* https://www.nema.org/Standards/Pages/Requirements-for-Smart-Meter-Upgradeability.aspx#download

Phase 3: Secure EVSE OTA Pilot Demonstration and EVSE OTA Cyber Security Guidance Development

The requirements for a pilot will be documented and a Proof-Of-Concept (POC) Pilot implementing a secure EVSE OTA firmware update will be demonstrated from end-to-end. Based on the pilot findings, an EVSE OTA Cyber Security Guidance Development document will be developed for the HD and MD markets.

Project Complexity: Medium-High

Leveraging Opportunity:

- DHS/UMTRI/NYU/SwRI – Uptane Framework
- IETF's - A Firmware Update Architecture for Internet of Things (IoT) Device
- NEMA Smart Grid Standards Publication SG-AMI 1-2009 - *Requirements for Smart Meter Upgradeability*, December 2016
- NISTIR 7823: Advanced Metering Infrastructure Smart Meter Upgradeability Test Framework

Deliverable(s)

- EVSE OTA Firmware Update Investigation White Paper
- EVSE OTA Firmware Update Framework Selection White Paper
- Secure EVSE OTA Pilot Demonstration
- EVSE OTA Cyber Security Guidance Development

ROM Cost Estimate: TBD

13.3 Develop MD/HDEV Charging Station Intrusion Detection System

In the event of a cyber-incident involving a MDHDVE charging station, IDS monitoring of the station for anomalies would provide the first indication of an attack. The components of the MD/HDEV-Charging Systems-Grid interfaces need to operate seamlessly without any interruptions. MD/HDEV charging stations will require remote Intrusion Detection System (IDS) monitoring and tracking. There is a major need to develop IDS/IPS systems specifically designed for MD/HDEV charging stations to detect and prevent hacking attempts in real-time. In the event of a cyber incident involving a MD/HDEV charging stations, IDS monitoring of the station for anomalies would provide the first indication of an attack.

This project will need to conduct a study to determine whether MD and HD Chargers are currently being designed and implemented with IDS/IPS functionality.

Any MD/HD IDS system will need to identify security issues that might occur on the Charging Device or Interface. The chargers IDS system will need to store for each security event at least the interface, the event type, a time stamp, and the user, role, or process causing the event, e.g. log-in attempts, replay attacks, configuration changes, firmware updates/patches, attempted replay attacks, alarms on physical manipulations, etc. The charging stations should allow remote monitoring of information about the device status such as processor and memory usage. Time synchronization is required to allow logs events from different devices to be correlated. Different technologies are available for time synchronization, such as Network Time Protocol (NTP) and Global Positioning Systems (GPS).

DOE's Idaho National Laboratory (INL) has a major 3-year project that has been underway since 2016 to develop a set of Diagnostic Security Modules (DSMs) that will detect intrusions to Electric Vehicle Charging Stations (i.e. EVSEs) integrated with the EVs and BEMS. INL coordinated with DOT/Volpe

Center and NMFTA and concluded that the DSM technology currently being designed and implemented for light-passenger EVs could be ported to MD/HDEV charging stations which will require high-power charging capabilities. The project identified in this section of the paper will describe the steps required to develop a "Pilot" to test the DSM/IDS concepts for MD/HD Chargers.

DSM Project Status:

- **October 2016 (Year 1):** Completed the initial equipment setup in INL laboratory space and the initial development of the DSM framework and communications channels.
- **April 2018 (Year 2):** Complete BEMS-to-EVSE-to-EV DSM framework implemented in the prototype environment at INL. A demonstration of the functionality of the system provided to all partners.
- **October 2018 (Planned)**: Deployment of the DSM framework in another DOE National Lab vehicle laboratory environment and develop a working demonstration of the DSM framework in the integrated lab environment.
- **April 2019 (Planned):** A publication of the developed methods for monitoring DSM connected EV and EVSE will be completed. This includes the algorithms used for generating the system fingerprints and detecting anomalous behavior. A detailed specification of the protocols developed and used for exchanging the security information from EV and EVSE to the BEMS. Cyber security testing of the DSM framework will take place at the 2019 SAE CyberAuto Challenge, see https://www.sae.org/attend/cyberauto/ . A final report detailing the effectiveness of DSM and the security framework during the cyber assessment will be made. Publication of the DSM framework methods, algorithms, and protocol will take place. Publication of an integration document for DSM to BEMS communications will also take place.

Project Summary:

Phase 1: MD/HDEV Charger Cyber Security Study

In Phase 1, a study will be needed to determine whether MD and HD chargers are currently being designed and implemented with IDS/IPS functionality. Interviews will be conducted with MD/HDEV OEMs and charging station vendors (e.g. ChargePoint, ABB, etc.) to discuss current and future plans to implement a real-time remote cyber security monitoring and detection capability.

Phase 2: MD/HDEV DSM/IDS Pilot

As described earlier, INL has a major and current 3-year project to develop set of Diagnostic Security Modules (DSMs) that will detect intrusions to EVSEs integrated with the EVs and BEMS for light-passenger vehicles.

For Phase 2, an EVSE vendor will be selected and INL will define any "unique" MD/HDEV charging station requirements, port, integrate, and test a "Pilot" MD/HDEV DSM/IDS capability that can be tested with a MD/HDEV.

In addition, a functional security test and penetration test will need to be performed by an "independent" third party cyber security testing team on the HD DSMIDS systems to provide assurance that attackers cannot bypass detection mechanisms and/or modify the security logs.

> ***NOTE:*** *A future CyberTruck Challenge would be a great opportunity to conduct this type of cyber security testing.*

Phase 3: MD/HDEV DSM/IDS Specification

The publication of the developed specification, including the algorithms used for generating the system fingerprints and detecting anomalous behavior for a MD/HDEV DSM/IDS capability, will be developed. Also, all the protocols developed and used for exchanging the security information from the MD/HDEV and MD/HDEV Charger will be documented in the specification. **The specification will be shared with the MD/HDEV Charging Station vendor and the Automotive OEMs.**

Project Complexity: Medium-High

Deliverables:

- MD/HDEV Charger Cyber Security Study
- MD/HDEV DSM/IDS Pilot
- MD/HDEV DSM/IDS Specification

Leveraging Opportunities:

- INL's Diagnostic Security Modules (DSM) for Electric Vehicle to Building Integration Project (2016-2019), for more information, see [G15] and [R05].
- ENCS's EVSE Charging Systems Security Requirements Report, (see the Section 3.2, Logging), will be used as a framework to develop the requirements for a MD/HDEV DSM/IDS Pilot.[83]

ROM Cost Estimate: TBD

13.4 Current and Near Term EVSE Cyber Security Mitigation Study

It is currently unknown what, if any, cyber security protections are being designed and implemented for MD/HDEV Chargers. MD/HDEV Charging Systems present several "unique" cyber security vulnerabilities. When an MD/HDEV is connected to the Charging Station there will be a two-way communication between itself and the vehicle. MD and HD Chargers can be used as a potential entry point for malware to spread to BEMS), Grid, telecommunications networks, and billing systems.

Project Summary:

This project would be a study of MD/HDEV Chargers vendors to determine the current status of cyber security mitigations currently in use and future plans for cyber security. Based on the findings, a Cyber Security Best Practices for MD/ HDEV Chargers document will be developed.

> ***Note:*** *The ENCS/Elaad "EV Charging Systems Security Requirements" Document, August 2017 will provide the trucking industry a good starting point for the Cyber Security Best Practices.*[84]

Project Complexity: Low

[83] [C19] European Network for Cyber Security, *EV Charging Systems: Security Requirements version 1.0*, Elaadnl, (April 2016). Retrieved 17 January 2018 from https://www.oasis-open.org/committees/download.php/59272/EV%20Charging%20Systems%20Security%20Requirements.pdf

[84] [C20] European Network for Cyber Security, *EV Charging Systems: Security Requirements version 1.01*, Elaadnl, (August 2017). Retrieved 21 March 2018 from https://www.elaad.nl/uploads/downloads/downloads_download/Security_Requirements_Charge_Points_v1.01_august2017.pdf

Deliverables:

- Cyber Security Best Practices for MD/HDEV Chargers document

Leveraging Opportunity:

- ENCS/Elaad "EV Charging Systems Security Requirements" document (Sections 2-6)

ROM Cost Estimate: TBD

13.5 Incident Response

Most organizations have an incident response plan; however, they are unlikely to have one that covers the unique and possibly far ranging aspects of an incident involving EVSEs, MD/HDEVs, and other facets unique to the EV environment.

Project Summary:

The purpose of the project is to develop an incident response plan which is specific to the M/HDEV environment that can be tailored by an organization to their unique requirements. The plan would cover MD/HDEV incident policies and procedures that address purpose, scope, roles, responsibilities, management commitment, coordination among the organizations entities and external entities along with compliance and procedures to facilitate implementation of the incident response policy and associated incident controls.

Project Complexity: Medium-High

Deliverable(s)

- Generic Electric Heavy Vehicle Incident Response Plan

ROM Cost Estimate: TBD

13.6 Cyber Security Best-Practices for MD/HDEV Wireless Charging Systems

There will be many stakeholders involved in the production of MD/HDEVs, and the competitive and proprietary nature of the automotive industry has led to differences in how MD/HDEVs are designed, tested, and deployed. Further, the drive for low-cost solutions can lead to a diminishment of security features. While there are standards being developed to enable basic functions and interoperability, no such guidance document currently exists stipulating the cyber security requirements for MD/HDEVs and wireless chargers.

The novel cyber security challenges surrounding MD/HDEVs highlight the increased attack surface and potential risk of a cyber-attack. Compromised MD/HDEVs and wireless chargers are not only potential public safety concerns, but are also potential malware vectors to other systems because of the shared connectivity and mobility of MD/HDEV. The growing significance of MD/HDEV in the global transportation market combined with the many unique cyber security challenges and diverse stakeholders necessitates a standard set of cyber security guidelines and best practices to ensure the industry can move forward safely and securely.

Project Summary:

For this project, a *Cyber Security Design Best-Practices for Wireless Charging Systems* document will be developed that will define security controls specific to on-board/vehicle system charging equipment for both wired and wireless solutions. The document will also focus on a security by design development practice and cover topics, such as: developing a secure reference architecture that is generic yet representative of a real-world implementation, creating cyber security best-practices and guidance based on such an architecture, and designing guidelines that enable secure integration with off-board chargers. The document will communicate cyber security expectations in a clear and repeatable manner and it will provide a baseline set of cyber security guidance in developing on-board charging systems for use for OEMs, suppliers, asset owners, operators, and integrators during the development process. The goal is to develop the cyber security best-practices internally, then to release for the community to review, contribute, and benefit together. The output of the project is not a standard, but by establishing guidelines and proven best practices it could serve as input to a future, formal standardization effort or procurement language document.

Fortunately, there is prior work on a guideline for off-board, EVSE security requirements. In 2016, European Network for Cyber Security (ENCS) developed a document titled "EV Charging Systems Security Requirements". This project will leverage the ENCS document and attempt use it as a guideline for the onboard parts of the charging system similar to what the document is for the EVSE/CPO/DSO parts of the charging system.

This Guidance document would be applicable to Wired/Wireless Charging Cyber Security Requirements for Electric Buses and MD/HDEVs because the communications paths are similar to light passenger EVs. Some resources and effort may be required to ensure any differences are handled appropriately.

Project Complexity: Medium

Deliverable(s):

- *Cyber Security Design Best-Practices for Wireless Charging Systems* document that contains a reference architecture for on-board charging systems and cyber security guidelines for on-board chargers enabling secure interoperability with off-board chargers

Leveraging Opportunities:

- Wireless Charging Cyber Security SMEs from Idaho National Laboratory (INL)
- ENCS's EVSE Charging Systems Security Requirements Report will be used as a framework and for insight into charging station cyber security requirements

ROM Cost Estimate: TBD

14 Conclusions

Hopefully this baseline reference document will assist all the different stakeholders within this very diverse set of industries to establish a common understanding of the complex and diverse issues surrounding Heavy Electric Vehicle and Charging Infrastructure Cyber Security. The following sections outline our short-term recommendations for closing key gaps and next steps in identifying, mitigating, and reducing the cyber security risks associated with this exciting trend of innovation and vehicle development.

14.1 Immediate Gaps

At the time of this paper, the following are some of the immediate gaps that need to be filled:

- The most pressing and immediate gap is the lack of a controlling body or standing industry working group to coordinate and communicate.
- Communication paths for incident response need to be flushed out at a high level among ISACs and government agencies. This top-level communication plan can then be disseminated to all the various stakeholders through existing means.
- An inventory of existing capable and near capable research facilities are needed that can be upgraded to allow for further research and development.
- Cyber security best practices need to be developed for MD/HDEV and EVSE Vendors.
- Additional research into maintenance and operations of heavy vehicles needs to be conducted to allow carriers to get more operational data on MD/HDEV.

14.2 Next Steps

It is important to emphasize that there is a great deal of activity and work being performed in this domain space by a very large and diverse set of stakeholders. There are on-going research projects, new research projects are being funded, and new vehicles are being developed by non-traditional and traditional OEMs. A number of different standards bodies are working on new and updated standards ranging from fast charging, batteries, utilities, operations, etc. The sheer amount of activity in this space can be overwhelming. This makes it very difficult to find a good starting point for a next step.

Based on our research, the best and next step needs to be the establishment of a single working group supported by both industry and government to help coordinate and facilitate information exchange.

15 Acknowledgments

NMFTA would like to thank Kate Vajda, Matt Carpenter, Kevin Harnett, and Graham Watson for their assistance in researching and assisting in the development of this paper. We would also like to thank all the domain experts from across the entire range of stakeholders of this area who contributed to this paper through a generous donation in their time in providing us with information and reviewing early drafts of the paper. We would also like to thank the internal NMFTA team of diligent editors who helped pull all this together and make it almost readable. Additionally, we would like to thank all the other academics, security professionals, white hat hackers, and hobbyists who have published the information that forms the core of our survey on the state of affairs in this area. Our reference section and appendices contain 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.

16 Annotated Reference Section

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 [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
- The [C##] set are those documents exploring charging station design and cyber vulnerabilities
- The [P##] set are those documents pertaining to power grid design and its cyber vulnerabilities
- The [BE##] set those documents referenced in the white paper exploring building/local energy management systems
- The [H##] set are those documents which are additional references discussing hacking electric vehicles
- The [R##] set are resources pertaining to proposed or active research programs regarding electric vehicles
- The [IMXX] set is composed of those documents discussing potential impacts from heavy vehicle hacking
- The [GXX] set are those documents provided as related recommendations or references in the white paper for further reading
- The [T##] set are those documents referenced in the white paper and/or those that are useful resources pertaining to the trucking industry
- The [VN##] set is composed of those documents that are specific to vehicle networking which are comparatively technical in nature;

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.

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 on 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 on 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.[85]

[A03] "Adventures in Automotive Networks and Control Units" was authored by Dr. Charlie Miller and Chris Valasek[86] 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.
>
> 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 on 22 July 2015 from: http://illmatics.com/car_hacking.pdf.

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

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

[86] 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.[87] 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.

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 on 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.

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.

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

[A06] Biner-Leube, Thomas, *48 Volt Technology*, Mercedes-Benz, PowerPoint presentation slides, (25 January 2018). Retrieved on 12 April 2018. SAE presentation not publically downloadable.

[87] 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)

[A07] Horvat, Gary, *Outlook for Longer Range Battery Electric Heavy Duty Vehicles*, Proterra, PowerPoint presentation slides, (n.d.). Retrieved on 5 February 2018. SAE presentation not publically downloadable.

16.2 The Core Papers Exploring Charging Station Design and Cyber Vulnerabilities

There are many resources available discussing the intricate design structure of charging stations and how they work. Much of this reading can be helpful in building a knowledge foundation of how charging stations work and their potential vulnerabilities within cyber security. This section will provide the sources referenced throughout the white paper and some additional resources concerning charging station design infrastructure and more specific technical documents such as operation manuals and current/future protocol.

[C01] Wikipedia contributors, *IEC 62196*, In Wikipedia, The Free Encyclopedia, (Last revised 23 April 2018). Retrieved on 26 April 2018 from https://en.wikipedia.org/wiki/IEC_62196

[C02] evcStation, *EV Chargers*, (n.d.). Retrieved on 26 April 2018 from http://www.evcstation.com/index.php/extras/ev-chargers

[C03] Herron, David, *Range Confidence: Charge Fast, Drive Far, with your Electric Car*, GreenTransportation.com, (2016-2017). Retrieved on 26 April 2018 from https://greentransportation.info/ev-charging/range-confidence/chap8-tech/ev-dc-fast-charging-standards-chademo-ccs-sae-combo-tesla-supercharger-etc.html

[C04] Hanley, Steve, *New Wireless EV Charging Standard From SAE Supports Up To 11 kW Charging Power*, CleanTechnica.com, (30 November 2017). Retrieved on 26 April 2018 from https://cleantechnica.com/2017/11/30/new-wireless-ev-charging-standard-sae-supports-11-kw-charging-power/

[C05] Charlton, Alistair, *Wireless electric vehicle charging explained*, Techradar.com, (16 April 2018). Retrieved on 26 April 2018 from https://www.techradar.com/news/wireless-electric-vehicle-charging

[C06] *Wireless Power Transfer for Light-Duty Plug-In/Electric Vehicles and Alignment Methodology*, SAE International, SAE J2954, (17 January 2012). Retrieved on 02 May 2018 from https://www.sae.org/standards/content/j2954/

[C07] Siemens, *New Wi-Fi enabled VersiCharge™ SG electric vehicle charging stations*, paper is version RPFL-VCSGD-0915, (2015). Retrieved on 27 April 2018 from https://www.downloads.siemens.com/download-center/Download.aspx?pos=download&fct=getasset&id1=BTLV_44824

[C08] Southern California Edison Company, *Charge Ready Program: Electric Vehicle Charging Stations and Related Services*, (n.d.). Retrieved on 07 March 2018 from https://www.sce.com/wps/portal/home/business/electric-cars/Charge-Ready/Charge-Ready-Support/!ut/p/b1/hdBNT4NAEAbgX8OVfVk-pN62FZddqPSDVroXQw1SDGUbiuXvi6Yealqd20yed5IZokhGVJOfqjLvKt3k9VevvBcpHpjFHSowCV2wcCL5dGVBRO4ANgPAjWL4L_9M1CVJ0oiCrRaz2H904HHrDCyfs1AsIfyUBxDjCKP1jEp_6v0GfHFHIeQ6iJOxReHQMxhxBKFMBpDObQh7jqclYzbws-GPKyRRZa233x_ZsGZr-yVRbfFWtEVrfrTDeNd1h-O9AQN935ul1mVdmK96b-BaZKePHckuJTnsM1Ti3a1PMfsEejNBKA!!/dl4/d5/L2dBISEvZ0FBIS9nQSEh/#sce_HashableContentPane_1-hash/sce_HashableContentPane_43-hash

[C09] Strategic Infrastructure Analysis Division, *Infrastructure System Overview: Electric Vehicle Charging Stations*, National Protection and Programs Directorate and Office of Cyber and Infrastructure Analysis (OCIA), (21 September 2017). Retrieved on 11 November 2017 from https://info.publicintelligence.net/OCIA-ElectricVehicleChargingStations.pdf

[C10] Marino, Frank, *Raytheon Provides ChargePoint Smart EV Charging for Employees*, ChargePoint, (2017). Retrieved on 11 November 2017 from https://www.chargepoint.com/files/customerstories/cs-raytheon.pdf

[C11] Smith, Scott, *Smart charging stations for electronic cars are extremely vulnerable to hacking*, Quartz.com, (22 May 2013). Retrieved on 15 April 2018 from https://qz.com/87385/smart-charging-stations-for-electronic-cars-are-extremely-vulnerable-to-hacking/

[C12] Shezaf, Ofer, *Who can hack a plug? : The InfoSec risks of charging electric cars*, slides for presentation at Hack in the Box Security Conference 2013, (2013). Retrieved on 01 February 2018 from https://xiom.com/

[C13] "Spinning reserve, non-spinning reserve", In *Energy Dictionary*, (n.d.). Retrieved on 25 April 2018 from: https://www.energyvortex.com/energydictionary/spinning_reserve__non_spinning_reserve.html

[C14] Wood, E., et al., *National Plug-In Electric Vehicle Infrastructure Analysis*, Office of Energy Efficiency & Renewable Energy, (September 2017). Retrieved on 02 May 2018 from https://www.nrel.gov/docs/fy17osti/69031.pdf

[C15] Howell, D, et al., *Enabling Fast Charging: A Technology Gap Assessment*, U.S. Department of Energy and Office of Energy Efficiency & Renewable Energy, (October 2017). Retrieved on 26 April 2018 from https://www.energy.gov/sites/prod/files/2017/10/f38/XFC%20Technology%20Gap%20Assessment%20Report_FINAL_10202017.pdf

[C16] Gies, Erica, *Electric Trucks Begin Reporting for Duty, Quietly and Without All the Fumes*, InsideClimateNews, (18 December 2017). Retrieved on 03 May 2018 from https://insideclimatenews.org/news/18122017/electric-truck-urban-package-delivery-ups-tesla-semi-daimler-byd-china-battery

Charging Station Protocols

These documents contain information regarding various charging station protocols.

[C17] Timbergren, Jonel, "*OCPP Compliancy Testing Tool – Scenario #2*", YouTube video, 04:03, (published 21 September 2016). Retrieved on April 25 2018 from https://www.youtube.com/watch?v=9wjUD-sxPAc&feature=youtu.be

[C18] Timbergren, Jonel, "*OCPP Compliancy Testing Tool – Scenario #1*", YouTube video, 03:38, (published 27 July 2016). Retrieved on 25 April 2018 from https://www.youtube.com/watch?v=FchMx3QzuhY&feature=youtu.be

[C19] European Network for Cyber Security, *EV Charging Systems: Security Requirements version 1.0*, Elaadnl, (April 2016). Retrieved on 17 January 2018 from https://www.oasis-open.org/committees/download.php/59272/EV%20Charging%20Systems%20Security%20Requirements.pdf

[C20] European Network for Cyber Security, *EV Charging Systems: Security Requirements version 1.01*, Elaadnl, (August 2017). Retrieved on 21 March 2018 from https://www.elaad.nl/uploads/downloads/downloads_download/Security_Requirements_Charge_Points_v1.01_august2017.pdf

[C21] Rodine, Craig *Electric Vehicle Charging System Standards and Security*, Slide deck from the 2018 SANS Automotive Cybersecurity Summit in Chicago (2018). Retrieved on 10 May 2018 from https://www.sans.org/summit-archives/cyber-defense

[C22] *TC 69 Electric Vehicles and Electric Industrial Trucks*, International Electrotechnical Commission, (n.d.). Retrieved on 10 May 2018 from http://www.iec.ch/dyn/www/f?p=103:7:15337487968483::::FSP_ORG_ID,FSP_LANG_ID:1255,25

[C23] Francfort, Jim, INL Efficiency and Security Testing of EVSE, DC Fast Chargers, and Wireless Charging Systems, US DOE (14 May 2013). Retrieved on 15 May 2018 from https://www.energy.gov/sites/prod/files/2014/03/f13/vss096_francfort_2013_o.pdf

[C24] Chugg, Jonathan and Rohde, Kenneth, CAN Bus Security Across Multi-Sector Platforms, VSATT (October 2015). Retrieved on 15 May 2018 from https://avt.inl.gov/sites/default/files/pdf/presentations/VSATTOctober2015CANBusOverview.pdf

Charging Station Specifications and Manuals

These documents and references contain information regarding various charging stations including specification sheets, installation manuals, etc. which we studied as part of our research.

[C25] ChargePoint, Inc., *CT4000 Family*, ChargePoint.com (n.d.). Retrieved on 27 April 2018 from https://www.chargepoint.com/products/commercial/ct4000/

[C26] ChargePoint, *ChargePoint Express 100 (CPE100) Charging Station*, ChargePoint Express 100 installation guide, (n.d.). Retrieved on 11 November 2017 from https://www.chargepoint.com/files/install/install_guide_cpe100.pdf

[C27] Arcom, *Section 262653 – Electric Vehicle Charging Equipment – Level 2*, product masterspec licensed by Arcom to ChargePoint, Inc., (June 2015). Retrieved on 23 April 2018 from https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwil_Of92eTaAhVBheAKHdeZBYoQFjAAegQIABBj&url=https%3A%2F%2Fwww.chargepoint.com%2Ffiles%2Fms%2F262653_FL_ELECTRIC_VEHICLE_CHARGING_EQUIPMENT.doc&usg=AOvVaw0RcxwhIF1CsUrZX26HI4vC

[C28] Caskey, J., et al., *NEMA Smart Grid Standards Publication SG-AMI (R2015): Requirements for Smart Meter Upgradability*, National Electrical Manufacturers Association, (2015). Retrieved on 04 May 2018 from https://www.nema.org/Standards/Pages/Requirements-for-Smart-Meter-Upgradeability.aspx#download

[C29] Schneider Electric, *EVlink™ Electric Car Charging Stations*, Catalog 2800CT1001 R009/15, (2015). Retrieved on 11 November 2017 from https://www.solaris-shop.com/content/EVlink%20Catalog.pdf

[C30] *Express 200 DC Commercial Charging Stations: Specifications and Ordering Information Guide*, ChargePoint, (2017). Retrieved on 11 November 2017 from https://www.chargepoint.com/files/datasheets/ds-cpe200.pdf

[C31] *Installation and service manual AC Level 2 electric vehicle supply equipment (EVSE)*, Eaton Instruction Manual IM0EV00002E, (March 2015). Retrieved on 11 November 2017 from https://www.ideadigitalcontent.com/files/10964/IM0EV00002E.pdf

[C32] *NEMA EVSE Charging Station User Manual & Installation Instructions*¸ GE EV Charging Station, (n.d.). Retrieved on 11 November 2017. http://apps.geindustrial.com/publibrary/checkout/DEH-44160?TNR=Installation%20and%20Instruction%7CDEH-44160%7Cgeneric

[C33] *AeroVironment™ EV Solutions™ Charging Dock Model EVSE-RS User Guide with Installation Instructions for Your Electrician*, EV Solutions™, (n.d.). Retrieved on 11 November 2017 from https://www.evsolutions.com/Upload/Nissan/NNA_EVSE-RS_UserGuide_Rev2_v3_lowres_040811.pdf

[C34] Clean Cities Technical Response Service, *Plug-In Electric Vehicle Handbook for Public Charging Station Hosts*, National renewable Energy Laboratory (NREL), a national laboratory of the U.S. Department of Energy, Office of Energy Efficiency and Renewable Energy, (April 2012). Retrieved on 11 November 2017 from https://www.afdc.energy.gov/pdfs/51227.pdf

[C35] Sitraffic Epos charging system, *The smart electric vehicle charging solution*, Siemens, (2010). Retrieved on 25 November 2017 from https://www.siemens.com/press/pool/de/events/corporate/...ecartec/epos_ws_en.pdf

[C36] *Wireless Power Transfer for Light-Duty Plug-In/Electric Vehicles and Alignment Methodology (J2954)*, SAE International, WIP. Available at https://www.sae.org/standards/content/j2954/

[C37] *Communication for Smart Charging of Plug-in Electric Vehicles using Smart Energy Profile 2.0 (J2847)*, SAE International, (05 November 2013). Available at https://www.sae.org/standards/content/j2847/1_201311/

16.3 The Core Papers Exploring Power Grid Design and Cyber Vulnerabilities

Many resources for this white paper referenced power grids and their numerous cyber security vulnerabilities. This section provides those resources referenced above, as well as additional papers that would offer the reader more in-depth knowledge of how a power grid works and its relationship to vehicle cyber security.

[P01] Graham, R., Francis, J., and Bogacz, R.J., *Challenges and Opportunities of Grid Modernization and Electric Transportation*, (March 2017). Retrieved on 13 November 2017 from https://www.energy.gov/sites/prod/files/2017/06/f34/Challenges_and_Opportunities_of_Grid_Modernization_and_Electric_Transportation.pdf

[P02] Campbell, Richard J., *Cybersecurity Issues for the Bulk Power System*, Congressional Research Service, (10 June 2015). Retrieved on 01 May 2018 from https://fas.org/sgp/crs/misc/R43989.pdf

[P03] Hong, D.T., et al., *Charging and Discharging of Plug-In Electric Vehicles (PEVs) in Vehicle-to-Grid (V2G) Systems: A Cyber Insurance-Based Model*, (05 January 2017), published in *IEEE Access vol. 5*, pp: 732-754, doi: 10.1109/ACCESS.2017.2649042. Retrieved on 15 April 2018 from https://ieeexplore.ieee.org/document/7807218/

[P04] Wagman, David C., *Cyber Defense tool Is an Early Warning System for Grid Attacks*, spectrum.ieee.org, (27 March 2018). Retrieved on 16 April 2018 from https://spectrum.ieee.org/energywise/energy/the-smarter-grid/cyber-defense-tool-targets-grid-vulnerability

[P05] Dunietz, Jesse, *Is the Power Grid Getting More Vulnerable to Cyber Attacks?*, ScientificAmerican.com, (23 August 2017). Retrieved on 16 April 2018 from https://www.scientificamerican.com/article/is-the-power-grid-getting-more-vulnerable-to-cyber-attacks/

[P06] Parfomak, Paul W., *NERC Standards for Bulk Power Physical Security: Is the Grid More Secure?*, Congressional Research Service, (19 March 2018). Retrieved on 16 April 2018 from https://fas.org/sgp/crs/homesec/R45135.pdf

[P07] *December 2017 Edition: Real-Time vs. Day-Ahead Pricing*, AEP Energy, (05 January 2018). Retrieved on 01 May 2018 from https://www.aepenergy.com/2018/01/05/december-2017-edition/

[P08] Hybrid Committee, *Use Cases for Communication Between Plug-in Vehicles and the Utility Grid*, SAE International, Standard J2836/1, (08 April 2010). Retrieved on 02 May 2018 from https://www.sae.org/standards/content/j2836/1_201004/

[P09] Hybrid Committee, *Security for Plug-In Electric Vehicle Communications*, SAE International, Standard J2931/7, (15 February 2018). Retrieved on 02 May 2018 from https://www.sae.org/standards/content/j2931/7_201802/

[P10] NERC, *CIP Standards*, North American Electric Reliability Corporation, (n.d.). Retrieved on 03 May 2018 from https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

[P11] NERC, *Bulk Electric System Definition Reference Document*, North American Electric Reliability Corporation, (n.d.). Retrieved on 04 May 2018 from https://www.nerc.com/pa/RAPA/BES%20DL/bes_phase2_reference_document_20140325_final_clean.pdf

[P12] Minkel, JR, *The 2003 Northeast Blackout – Five Years Later*, ScientificAmerican.com, (13 August 2008). Retrieved on 14 May 2018 from https://www.scientificamerican.com/article/2003-blackout-five-years-later/

[P13] NESCOR, *Electric Sector Failure Scenarios and Impact Analyses*, prepared by Technical Working Group 1, (June 2014). Retrieved on 11 November 2017. No source available. Document provided in Supplement File Directory.

16.4 Papers Exploring Building/Local Energy Management Systems

This section provides the references made in the white paper involving BEMS and their associated involvement with heavy electric vehicle security. [BE01] provides an outlook for the cyber security risks of BEMS hacking, while [BE02] provides a more technical outlook on how a BEMS may integrate algorithms to reduce electricity requirements and control energy output.

[BE01] *"Smart Buildings Pose Big Risks" is a short article by Jaikumar Vijayan posted on ComputerWorld.com. This article references several risks that BEMS can face due to their interconnected networks with the outside world. With the adaptation of charging stations and power supply routing into the BEMS, this article would be a good reference for the reader to discover several different attack vectors and their associated risks.*

Vijayan, Jaikumar, *Smart Buildings Pose Big Risks*, ComputerWorld.com, (12 May 2014). Retrieved on 11 November 2017 from https://www.computerworld.com/article/2489343/security0/with-the-internet-of-things--smart-buildings-pose-big-risk.html

[BE02] Marmaras, C., Javed, A., Rana, O., and Cipcigan, L., *A Cloud-Based Energy Management System for Building Managers*, ICE '17 Companion Proceedings of the 8th ACM/SPEC on International Conference on Performance Engineering Companion 22-26 April 2017, pp 61-66, doi: 10.1145/3053600.3053613. Retrieved on 27 April 2018 from https://research.spec.org/icpe_proceedings/2017/companion/p61.pdf

16.5 Additional Resources Further Discussing Vehicle Hacking Techniques

Vehicle Hacking Techniques can take varying strategies and attack vectors. Due to these various methods, this section has been divided up for the reader's convenience into multiple sections regarding cyber incidents, ongoing hacking activities, and potential threat actors.

References [H01] through [H09] relate to the varying techniques a malicious attacker may employ concerning heavy electric vehicles and contains some of the foundational papers and publications in the subject.

[H01] "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 [H01] 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.

[H02] "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 [H02] 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)

[H03] "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. Instead, each method of theft should be considered as an exploit that might later be scaled and weaponized.[88] This paper [H03] 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

[H04] "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 [H04] 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

[H05] Vaas, Lisa, *How to hack an electric car-charging station*, NakedSecurity.com, (17 May 2013). Retrieved on 25 April 2018 from https://nakedsecurity.sophos.com/2013/05/17/how-to-hack-an-electric-car-charging-station/

[H06] Ahmed, S., Dow, F.M., *Electric Vehicle and Charging Station Technology as Vulnerabilities Threaten and Hackers Crash the Smart Grid*, published in the International Journal of Innovative Science, Engineering & Technology, Vol. 3 Issue 10, (October 2016). Retrieved on 15 April 2018 from https://pdfs.semanticscholar.org/aac1/5d7ded4ee419672439b3cadf3302f851223a.pdf

[H07] Sripad, Shashank, et al., *Vulnerabilities of Electric Vehicle Battery Packs to Cyberattacks on Auxiliary Components*, arXiv.org, (15 November 2017). Retrieved on 15 April 2018 from https://arxiv.org/pdf/1711.04822.pdf

[H08] Mitnick, K (Author). Wozniak, S. (Foreword), Simon, W. (Contributor), *Ghost in the Wires: My Adventures as the World's Most Wanted Hacker*, Back Bay Books, (24 April 2012). ISBN-10: 0316037702.

[H09] *Calibrating the Smart Grid*, Fluke.com, (n.d.). Retrieved on 02 May 2018 from http://en-us.fluke.com/community/fluke-news-plus/electronic-news/calibrating-the-smart-grid.html

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

16.6 Resources on Cyber Incidents and Trend Analysis

[H10] through [H14] are additional resources provided for the reader concerning a cyber security overview and trend analysis. These reports provide statistical research involving current trends and incidents in the field of cyber security.

[H10] through [H12] 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 [H10] through [H12] be at least quickly skimmed.

[H10] Mandiant, *M-Trends 2018, (2018).* Retrieved on 16 April 2018 from https://www.fireeye.com/content/dam/collateral/en/mtrends-2018.pdf

[H11] Mandiant, *M-Trends 2014: Beyond the Breach.* Retrieved on 31 August 2015 from: https://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf

[H12] 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.

[H13] FBI, *Internet Crime Report 2016*, Internet Crime Complaint Center, Tech. Rep., (2016). Retrieved on 26 April 2018 from https://pdf.ic3.gov/2016_IC3Report.pdf

16.7 References for Ongoing Hacking Activities

The following resources are mostly news articles and journal publications by selected authors concerning cyber security incidents and related attack to electric vehicles. These resources have been divided up based on their target and attack type. These articles are recommended to be skimmed through for a better knowledge of how electric vehicles are targeted and specific incidents relating to the subject.

[H14] Romo, Vanessa, *As Atlanta Seeks To Restore Services, Ransomware Attacks Are On the Rise*, NPR the two-way, (30 Mar 2018). Retrieved on 26 April 2018 from https://www.npr.org/sections/thetwo-way/2018/03/30/597987182/as-atlanta-seeks-to-restore-services-ransomware-attacks-are-on-the-rise

[H15] Lee, R.M., Assante, M.J., Conway, T, *Analysis of the Cyber Attack on the Ukrainian Power Grid*, SANS ICS Report, (18 March 2016). Retrieved on 25 April 2018 from https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf

[H16] Greenburg, Andy, *'Crash Override': The Malware That Took Down a Power Grid*, Wired Magazine, (12 June 2017). Retrieved on 25 April 2018 from https://www.wired.com/story/crash-override-malware/

[H17] Lee, Robert, *CRASHOVERRIDE: Analysis of the threat to electric grid operations*, Dragos.com, (12 June 2017). Retrieved on 26 April 2018 from https://dragos.com/blog/crashoverride/CrashOverride-01.pdf

[H18] Wolf, M., & Lambert, R., Schmidt, AD., Enderle, T., *WannaDrive? Feasible Attack Paths and Effective Protection against Ransomware in Modern Vehicles*, (n.d.), Retrieved on 25 April 2018 from https://www.escrypt.com/sites/default/files/documents/Ransomware-against-cars.pdf

[H19] Plungis, Jeff, *Your Car Could Be the Next Ransomware Target*, ConsumerReports.com, (01 June 2017). Retrieved on 25 April 2018 from https://www.consumerreports.org/hacking/your-car-could-be-the-next-ransomware-target

[H20] Goud, Naveen, *Connected Cars are vulnerable to Ransomware Attacks*, Cybersecurity Insiders, (n.d.). Retrieved on 25 April 2018 from https://www.cybersecurity-insiders.com/connected-cars-are-vulnerable-to-ransomware-attacks/

[H21] Kaspersky lab, *BlackEnergy APT Attacks in Ukraine*, usa.kaspersky.com, (n.d.). Retrieved on 01 May 2018 from https://usa.kaspersky.com/resource-center/threats/blackenergy

[H22] F-Secure Labs Security Response, *BlackEnergy & Quedagh: The convergence of crimeware and APT attacks*, F-Secure, (n.d.). Retrieved on 01 May 2018 from https://www.f-secure.com/documents/996508/1030745/blackenergy_whitepaper.pdf

[H23] Poulsen, Kevin, *Slammer worm crashing Ohio nuke plant network*, SecurityFocus.com, (19 August 2003). Retrieved on 01 May 2018 from https://www.securityfocus.com/news/6767/

[H24] Verton, Dan, *Blaster worm linked to severity of blackout*, ComputerWorld.com, (29 August 2003). Retrieved on 02 May 2018 from https://www.computerworld.com/article/2571068/disaster-recovery/blaster-worm-linked-to-severity-of-blackout.html

[H25] Bigelow, Pete, *2 million Progressive Snapshot customers may be at risk for car hacking: Cyber-Security Firm Says Popular Device contains No Security*, AutoBlog.com, (21 January 2015). Retrieved on 04 May 2018 from https://www.autoblog.com/2015/01/21/2-million-progressive-snapshot-customers-may-be-at-risk-for-car/

[H26] *A remote attack on an aftermarket telematics service*, Argus Cyber Security (blog), Argus Security, (n.d.), Retrieved on 26 April 2018 from https://argus-sec.com/remote-attack-aftermarket-telematics-service/

[H27] Khandelwal, Swati, *Pre-Installed Malware Found on 5 Million Popular Android Phones*, thehackernews.com, (15 March 2018). Retrieved on 30 April 2018 from https://thehackernews.com/2018/03/android-botnet-malware.html

[H28] Zetter, Kim, *New Discovery around darkreading Backdoor Raises More Questions About the Company*, Wired.com, (08 January 2016). Retrieved on 30 April 2018 from https://www.wired.com/2016/01/new-discovery-around-juniper-backdoor-raises-more-questions-about-the-company/

[H29] Peters, Sara, *Pharmaceuticals, Not Energy, May Have Been True Target of Dragonfly, Energetic Bear*, DarkReading.com, (22 October 2014). Retrieved on 30 April 2018 from https://www.darkreading.com/pharmaceuticalsnot-energy-may-have-been-true-target-of-dragonfly-energetic-bear/d/d-id/1316869

[H30] Brian, Matt, *London has a real problem with thieves targeting keyless cars*, Engadget.com, (03 February 2015). Retrieved on 27 April 2018 from https://www.engadget.com/2015/02/03/london-keyless-car-theft/

[H31] Francillon, A., Danev, B., and Capkun, S., *Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars*, In Proceedings of the Network and Distributed System Security symposium (NDSS), (February 2011). Retrieved on 26 April 2018 from https://eprint.iacr.org/2010/332.pdf

[H32] Uttmark, Michael, *LTE IMSI Catcher*, Hackaday.com, (30 May 2017). Retrieved on 10 May 2018 from https://hackaday.com/2017/05/30/lte-imsi-catcher/

[H33] Dalheimer, M. [media.ccc.de], "*34C3 – Ladeinfrastrukur fur Elektroautos: Ausbau statt Sicherheit – English translation*", YouTube video, 52:54, (published 27 December 2017). Retrieved on 04 May 2018 from https://www.youtube.com/watch?v=szYeqOIQ9Bw

[H34] Atkinson, Blake, *10 Most Powerful (Known) Active Hacking Groups*, TurboFuture.com, (last update Mar 7 2018). Retrieved on 25 April 2018 from https://turbofuture.com/internet/Most-Powerful-Active-Hacking-Groups

[H35] Williams, T., *Barstow, CA Tesla Supercharger Vandalized before Thanksgiving Weekend (Update)*, INSIDEEVs, (23 November 2016). Retrieved on 25 April 2018 from https://insideevs.com/barstow-tesla-supercharger-vandalized-thanksgiving-weekend/

[H36] *Charging Station Vandalism – Downtown Phoenix*, TeslaMotorClub.com, Blog Post, (01 August 2013). Retrieved on 02 May 2018 from https://teslamotorsclub.com/tmc/threads/charging-station-vandalism-downtown-phoenix.19678/

[H37] *Charging Cord Vandalism. (Warning to all EV car owners)*, MyNissanLeaf.com, Blog Post, (11 April 2011). Retrieved 02 May 2018 from http://www.mynissanleaf.com/viewtopic.php?t=3330

[H38] Gordon-Bloomfield, Nikki, *Why Baltimore's Vandalized Charging Stations Have Taken Too Long To Fix*, PlugInCars.com, (28 June 2013). Retrieved on 02 May 2018 from http://www.plugincars.com/why-baltimores-vandalized-charging-stations-have-taken-too-long-fix-127614.html

[H39] Paganini, Pierluigi, *Attackers exfiltrated a casino's high-roller list through a connected fish tank*, securityaffairs.co, (16 April 2018). Retrieved on 04 May 2018 from https://securityaffairs.co/wordpress/71433/hacking/fish-tank-hack.html

[H40] *Hacking Zigbee Devices with Attify Zigbee Framework*, blog.attify.com, (24 April 2014). Retrieved on 04 May 2018 from https://blog.attify.com/hack-iot-devices-zigbee-sniffing-exploitation/

[H41] Wright, Joshua, *How Attackers Exploit Modern, "Secure" Wireless Networks*, blogs.sans.org, (13 October 2010). Retrieved on 04 May 2018 from https://blogs.sans.org/pen-testing/files/2011/11/Wright-ExploitModernWlan-Webcast-20111013.pdf

[H42] Davies, Mike, *SmartGrid Device Security: Adventures in a new medium*, Blackhat 2009, (August 2009). Retrieved on 07 May 2018 from https://www.blackhat.com/presentations/bh-usa-09/MDAVIS/BHUSA09-Davis-AMI-SLIDES.pdf

[H43] *Staged cyber-attack reveals vulnerability in power grid*, CNN, (published 27 September 2007). Retrieved on 07 May 2018 from https://www.youtube.com/watch?v=fJyWngDco3g

[H44] Bort, Julie, *Oracle's software was hacked by interns in an hour*, researcher says, businessinsider.com, (27 October 2015). Retrieved on 04 May 2018 from http://www.businessinsider.com/oracle-erp-hacked-by-interns-in-an-hour-2015-10

[H45] 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/

[H46] Infosec Institute, *Ransomware Case Studies: Hollywood Presbyterian & The Ottawa Hospital.*, infosecinstitute.com. (n.d.). Retrieved on 4 May 2018 from http://resources.infosecinstitute.com/category/healthcare-information-security/healthcare-attack-statistics-and-case-studies/ransomware-case-studies-hollywood-presbyterian-and-the-ottawa-hospital/#gref

[H47] Walker, Danielle, *'Havex' malware strikes industrial sector via watering hole attacks*, Scmagazine.com, (Published June 25, 2014). Retrieved on 04 August 2018 from https://www.scmagazine.com/havex-malware-strikes-industrial-sector-via-watering-hole-attacks/article/538721/

[H48] *Network Management Systems: A Suite of Intelligent Devices*, Silver Spring Networks, (n.d.). Retrieved on 07 May 2018 from https://www.silverspringnet.com/solutions/network-devices/#fndtn-content-7

[H49] *SpeedNet™ Radios*, S&E Electric Company, (n.d.). Retrieved on 07 May 2018 from http://www.sandc.com/en/products--services/products/speednet-radios/

[H50] King, Chris, *Vulnerability Note VU#209512: Mobile Devices C4 ODB2 dongle contains multiple vulnerabilities*, CERT Software Engineering Institute, Carnegie Mellon University, (11 August 2015, last revised 28 August 2015). Retrieved on 14 May 2018 from https://www.kb.cert.org/vuls/id/209512

[H51] United States Computer Emergency Readiness Team, *Alert (TA18-074A) Russian government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors*, Department of Homeland Security, (last revised 16 March 2018). Retrieved on 04 May 2018 from https://www.us-cert.gov/ncas/alerts/TA18-074A

[H52] Dunson, Brandon, *RF Hacking: How-To Bypass Rolling Codes*, Hackaday.com, (6 March 2016). Retrieved on 15 May 2018 from https://hackaday.com/2016/03/06/rf-hacking-how-to-bypass-rolling-codes/

[H53] Greenberg, Andy, This 'Demonically Clever' Backdoor Hides In a Tiny Slice of a Computer Chip, Wired.com, (6 January 2016). Retrieved on 15 May 2018 from https://www.wired.com/2016/06/demonically-clever-backdoor-hides-inside-computer-chip/

[H54] Simonite, Tom, NSA's Own Hardware Backdoors May Still Be a "Problem from Hell", MIT Technology Review, (8 October 2013). Retrieved on 15 May 2018 from https://www.technologyreview.com/s/519661/nsas-own-hardware-backdoors-may-still-be-a-problem-from-hell/

16.8 Resources on Selected Research Programs (Proposed and Active)

This section contains several resources on the current or proposed research activities in the field of electric vehicle cyber security. These references are beneficial to a reader looking to familiarize themselves with the research programs on the subject and additional publications on cyber security research and development.

[R01] Carlson, Barney, *INL's Electric Vehicle Charging Infrastructure Laboratory,* Idaho National Laboratory Electric Vehicle Infrastructure Lab, (October 2015). Retrieved on 11 November 2017 from https://avt.inl.gov/sites/default/files/pdf/presentations/VSATTOctober2015EVIL.pdf

[R02] House and Senate Energy & Technology Committees, *Michigan Plug-in Vehicle Preparedness Taskforce*, presentation by Plug-In Michigan, (10 May 2011). Retrieved on 13 November 2017. Source not found.

[R03] Ghanish, Isaac, California Energy Commission, *Smart Grid Cyber Security Potential Threats, Vulnerabilities and Risks: Interim Project Report*, (May 2012). Retrieved on 11 November 2017 from www.energy.ca.gov/2012publications/CEC-500-2012-047/CEC-500-2012-047.pdf

[R04] Pratt, Rick, *Vehicle Communications and Charging Control*, Pacific Northwest National Laboratory, (2014). Retrieved on 13 February 2018 from https://www.energy.gov/sites/prod/files/2014/07/f18/vss142_pratt_2014_p.pdf

[R05] Rohde, Kenneth, *VTO Diagnostic Security Modules for Electric Vehicle to Building Integration*, Idaho National Laboratory Cyber Security R&D Department, presented by Barney Carlson, (07 July 2016). Retrieved on 11 November 2017.

[R06] IEEE, *IEEE Forms Committee to Develop a Certification Plan for Rapid Charging of Electric Vehicles and Approves Standard Revision on Dynamic Dc Charging up to 400kw*, BusinessWire.com, (28 November 2017). Retrieved 02 May 2018 from https://www.businesswire.com/news/home/20171128005135/en/

[R07] Bauer, Susan, *Research hints at double the driving range for electric vehicles*, (27 March 2018). Retrieved on 03 May 2018 from https://www.pnnl.gov/news/release.aspx?id=4497

[R08] Sheppard, Andrew, et al., *Modeling plug-in electric vehicle charging demand with BEAM: The framework for behavior energy autonomy mobility*, Energy Analysis and Environmental Impacts Division Lawrence Berkeley National Laboratory, (May 2017). Retrieved on 03 May 2018 from https://eta.lbl.gov/sites/default/files/publications/lbnl-2001018.pdf

[R09] ElaadNL, *Cybersecurity*, ElaadNL.com, (n.d.). Retrieved on 03 May 2018 from https://www.elaad.nl/projects/cybersecurity/

16.9 Potential Impacts from Heavy Vehicle and other Cyber Physical Hacking

This section provides various references and additional resources concerning the many impacts heavy electric vehicle hacking may pose. [IM01] through [IM03] provide the reader with additional education regarding the strategic importance of the industry, while [IM06] through [IM08] are those resources specific to the Petya attack referenced in Section 7.4 of the white paper.

[IM01] "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 [IM01] 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 on 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".[89]

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, [IM01] through [IM03] need not be reviewed.

[IM02] "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 .

[IM03] "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.

[IM04] SensiGuard, *Supply Chain Security*, Sensitech.com, (n.d.). Retrieved on 26 April 2018 from http://www.sensitech.com/en/supply-chain-security/

[IM05] Kilcarr, Sean, *Cargo theft now a tougher nut to crack*, FleetOwner.com, (01 Jun 2016). Retrieved on 26 April 2018 from http://www.fleetowner.com/fleet-management/cargo-theft-now-tougher-nut-crack

[IM06] Coyne, Allie, *TNT Express still struggling to remediate after Petya attack*, iTnews.com, (03 Jul 2017). Retrieved on 26 April 2018 from https://www.itnews.com.au/news/tnt-express-still-struggling-to-remediate-after-petya-attack-467352

[IM07] Kovacs, Eduard, *FedEx Profit Takes $300 Million Hit After Malware Attack*, SecurityWeek.com, (09 20 2017). Retrieved on 26 April 2018 from https://www.securityweek.com/fedex-profit-takes-300-million-hit-after-malware-attack

[IM08] Schwartz, Mathew J., *Maersk Previews NotPetya Impact: Up to $300 Million*, BankInfoSecurity.com, (17 Aug 2017). Retrieved on 26 April 2018 from https://www.bankinfosecurity.com/maersk-previews-notpetya-impact-up-to-300-million-a-10203

[IM09] Sanchez, Jesus, *Teamsters Strike Shuts Down 22 Trucking Firms*, LA Times, (07 April 1994). Retrieved 10 May 2018 from http://articles.latimes.com/1994-04-07/news/mn-43292_1_trucking-firms

[IM10] Watson, Rip, *Teamsters, TMI Reach Tentative Settlement Union Officials to Vote Today on Package*, Joc.com, (28 April 1994). Retrieved 10 May 2018 from https://www.joc.com/teamsters-tmi-reach-tentative-settlement-union-officials-vote-today-package_19940428.html

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

16.10 Cyber Security and Related Recommendations

The following papers outline selected cyber security practices provided throughout the industry for improving countermeasures to cyber threats. These practices are tailored toward electric vehicles or other forms of electric transportation. [G01] through [G03] are more technical in nature, while [G18] through [G25] provide helpful guidebooks and frameworks for Industrial Control Systems.

[G01] "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[90] 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 [G01] 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

[G02] "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. [G02] 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/.

[G03] "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. [G03] 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/.

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

[G04] "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 [G04] is recommended reading.

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

[G05] "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 [G05] 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

[G06] ChargePoint, Inc., "*Next-Generation Grid Communication for Residential PEVs (EPC-14-078),*" Presentation slides for the Fourth Annual California Multi-Agency Update on Vehicle-Grid Integration Research, Sacramento, CA (05 December 2017). Retrieved on 25 April 2018. http://www.energy.ca.gov/research/notices/2015-12-14_workshop/presentations/08__EPIC_ChargePoint__Quattrini.pptx

[G07] Chugg, J., Rohde, K., *CAN Bus Security Across Multi-Sector Platforms*, Idaho National Laboratory, (n.d.). Retrieved on 11 November 2017 from https://avt.inl.gov/sites/default/files/pdf/presentations/VSATTOctober2015CANBusOverview.pdf

[G08] Advanced Telematic Systems, *ATS is integrating the Uptane security framework for over-the-air software updates to connected websites*, AdvancedTelematic.com, (June 2017). Retrieved on 27 April 2018 from https://advancedtelematic.com/en/press-releases/ats-is-integrating-the-uptane-security-framework-for-over-the-air-software-updates-to-connected-vehicles.html

[G09] Moran, B., Meriac, M., Tshofenig, H., *A Firmware Update Architecture for Internet of Things Devices draft-moran-suit-architecture-03*, this paper is a 3rd internet draft published by Arm Limited, (05 March 2018). Retrieved on 27 April 2018 from https://tools.ietf.org/html/draft-moran-suit-architecture-03

[G10] Iorga, M., Shorter, S., *Advanced Metering Infrastructure smart Meter Upgradeability Test Framework*, National Institute of Standards and Technology Interagency Report 7823, (March 2015). Retrieved on 27 April 2018 from https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.7823.pdf

[G11] NIST. *NISTIR 7628, Guidelines for Smart Grid Cyber Security*, (September 2010). Retrieved on 27 April 2018 from https://www.nist.gov/sites/default/files/documents/smartgrid/nistir-7628_total.pdf

[G12] NHTSA, *Cybersecurity Best Practices for Modern Vehicles*, USDOT NHTSA, (October 2016). Retrieved on 11 November 2017 from https://www.nhtsa.gov/staticfiles/nvs/.../812333_CybersecurityForModernVehicles.pdf

[G13] United States Department of Transportation Volpe Center and United States Department of Energy Office of Policy, *DOE/DHS/DOT Volpe Technical Meeting on Electric Vehicle and Charging Station Cybersecurity Report*, US Department of Transportation Volpe Center, (March 2018). Retrieved on 13 March 2018 from https://rosap.ntl.bts.gov/view/dot/34991/dot_34991_DS1.pdf

[G14] Rohde, Kenneth, *Electric Vehicle Cyber Research*, presentation slides for SANS Automotive Cybersecurity Workshop, (May 2017). Retrieved on 11 November 2017 from https://www.sans.org/summit-archives/file/summit-archive-1493817272.pdf.

[G15] Rohde, Kenneth, *Electric Vehicle Cyber Research*, presentation slides for 2017 Energy Exchange, (16 August 2017) .Retrieved on 11 November 2017 from https://www.2018energyexchange.com/wp-content/uploads/T7S6_Rohde.pdf

[G16] Bourton, Mike, *IEEE 2030.5 Cyber Security v.1*, Kitu Systems, Inc., (11 December 2017). Retrieved 23 April 2018. Source not found.

[G17] Ross, R, McEvilley, M, Carrier Oren, J, *Systems Security Engineering: considerations for a Multidisciplinary approach in the Engineering of Trustworthy Secure Systems*, National Institute of Standards and Technology Special Publication 800-160 Vol.1, (November 2016). Retrieved on 22 March 2018 from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1.pdf

[G18] Karali, Nihan, *Vehicle-Grid Integration: Cyber-security of PEVs*, Energy Analysis and Environmental Impacts Division Lawrence Berkeley National Laboratory: International Energy Studies Group, (July 2017). Retrieved on 15 April 2018 from https://www.iea.org/media/topics/transport/VehicletoGridCybersecurityBrief.pdf

[G19] Hybrid Committee, *Cybersecurity Guidebook for Cyber Physical Vehicle Systems*, SAE International, (14 January 2016). Retrieved on 02 May 2018 from https://www.sae.org/standards/content/j3061_201601/

[G20] *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*, National Institute of Standards and Technology, (16 April 2018) Retrieved on 02 May 2018 from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[G21] *Seven Steps to Effectively Defend Industrial Control Systems*, National Cybersecurity and Communications Integration Center, (n.d.). Retrieved on 02 May 2018 from https://ics-cert.us-cert.gov/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%20Control%20Systems_S508C.pdf

[G22] *Recommended Practices*, Industrial Control Systems Cyber Emergency Response Team, (n.d.). Retrieved on 02 May 2018 from https://ics-cert.us-cert.gov/Recommended-Practices

[G23] Center for Internet Security, *Powerful Best Practices*, CISsecurity.org, (n.d.). Retrieved on 03 May 2018 from https://learn.cisecurity.org/20-controls-download

[G24] Cichonski, P., Millar, T., Grance, T., & Scarfone, K., *Computer Security Incident Handling Guide Special Publication 800-61 Revision 2*, National Institute of Standards and Technology, (August 2012). Retrieved on 03 May 2018 from http://dx.doi.org/10.6028/NIST.SP.800-61r2

[G25] Control systems Security Program, *Recommended Practice: Developing an Industrial Control Systems Cybersecurity Incident Response Capability*, Department of Homeland Security National Cyber Security Division, (October 2009). Retrieved on 03 May 2018 from https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/final-RP_ics_cybersecurity_incident_response_100609.pdf

[G26] Hazarika, Mrinmoyee, *ENCS and ElaadNL to protect EV smart charging infrastructure from cyber security threats*, Power-Technology.com, (25 July 2017). Retrieved on 04 May 2018 from https://www.power-technology.com/news/newsencs-and-elaadnl-to-protect-ev-smart-charging-infrastructure-from-cyber-security-threats-5882702/

16.11 References for Trucking

This section provides the papers referenced within the white paper, as well as additional resources explaining the current trucking industry and the recent adoption of heavy electric vehicles. Included below are resources exploring the heavy electric vehicle market, as well as technical information regarding battery packs and their range limit. [T05] through [T07], and [T11] through [T18] reference current or future plans for industry adoption of heavy electric vehicles and provide a closer look into individual company strides with heavy electric vehicles.

[T01] Owner-Operator Independent Drivers Association, *Trucking Facts*, OOIDA, (n.d.). Retrieved on 03 May 2018 from https://www.ooida.com/MediaCenter/trucking-facts.asp

[T02] Federal Motor Carrier Safety Administration, *Federal Register Vol. 76 No. 248*, Department of Transportation, (27 December 2011). Retrieved on 01 May 2018 from https://cms.fmcsa.dot.gov/regulations/rulemaking/2011-32696

[T03] Federal Motor Carrier Safety Administration, *HOS Regulations*, Department of Transportation, (n.d.). Retrieved on 01 May 2018 from http://www.werner.com/assets/pdf/drivers/HOSRegulations.pdf

[T04] *The Revised Hours-Of-Service (HOS) Regulations*, Werner.com, (n.d.). Retrieved on 01 May 2018 from http://www.werner.com/content/drivers/driver_resources/hours_of_service.cfm

[T05] Fleet Owner Staff, *Volvo to release electric truck next year in Europe*, Fleet Owner, (18 April 2018). Retrieved on 27 April 2018 from http://www.fleetowner.com/blue-fleets/volvo-release-electric-truck-next-year-europe?NL=FO-06&Issue=FO-06_20180427_FO-06_895&sfvc4enews=42&cl=article_6_1&utm_rid=CPENT000003440627&utm_campaign=18128&utm_medium=email&elq2=62b76e176e924f17b74a31b666800155

[T06] Baldwin, Robert, *Daimler's electric trucks start making deliveries in Japan and US: A quieter, cleaner delivery truck*, Engadget.com, (27 October 2018). Retrieved on 27 April 2018 from https://www.engadget.com/2017/10/27/daimler-efuso-mercedes-electric-truck/

[T07] ZumMallen, Ryan, *Thor Trucks Storming Into Heavy-Duty EV Market*, Trucks.com, (13 December 2017). Retrieved on 27 April 2018 from https://www.trucks.com/2017/12/13/startup-thor-trucks-electric-truck-market/

[T08] FMCSA, *What is a private motor carrier?* , Federal Motor Carrier Safety Administration, (02 December 2014). Retrieved on 27 April 2018 from https://ask.fmcsa.dot.gov/app/answers/detail/a_id/247

[T09] O'Dell, John, *California Readies $398-million Green Truck Incentive Package*, Trucks.com, (11 December 2017). Retrieved on 27 April 2018 from https://www.trucks.com/2017/12/11/california-green-truck-incentive-package/

[T10] Turpen, Aaron, *Tesla Semi truck's battery pack and overall weight explored*, Teslarati.com, (24 February 2018). Retrieved on 27 April 2018 from https://www.teslarati.com/how-much-tesla-semi-truck-battery-pack-weigh/

[T11] Hensley, B., Knupfer, S., Tschiesner, A., *What's sparking electric-vehicle adoption in the truck industry*, Mckinsey.com, (September 2017). Retrieved on 02 May 2018 from https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/whats-sparking-electric-vehicle-adoption-in-the-truck-industry

[T12] Carey, Nick, *UPS partners with Workhorse to build electric delivery vans*, Reuters.com, (22 February 2018). Retrieved on 02 May 2018 from https://www.reuters.com/article/us-ups-workhorse-group/ups-partners-with-workhorse-to-build-electric-delivery-vans-idUSKCN1G61S7#_blank

[T13] *Low Emission Zone*, Transport For London, (n.d.). Retrieved on 02 May 2018 from https://tfl.gov.uk/modes/driving/low-emission-zone

[T14] van Rooij, Rogier, *Driverless Electric Trucks To Enter Sweden's Roads Later This Year*, CleanTechnica.com, (05 February 2018). Retrieved on 02 May 2018 from https://cleantechnica.com/2018/02/05/driverless-electric-trucks-enter-swedens-roads-later-year/

[T15] Huddleston Jr., Tom, *Semi-Autonomous Trucks May Drive Across the Country in Platoons*, Fortune.com, (17 November 2017). Retrieved on 02 May 2018 from http://fortune.com/2017/11/17/electric-semi-autonomous-trucks-platoon-peloton/

[T16] Lockridge, Deborah, *Daimler Pumping R&D into Electric Trucks, Connectivity, Autonomous Trucks*, Truckinginfo.com, (March 2018). Retrieved on 02 May 2018 from http://www.truckinginfo.com/channel/fleet-management/article/story/2018/03/daimler-pumping-r-d-into-electric-trucks-connectivity-autonomous-trucks.aspx

[T17] RTT News, *Volvo's UD Trucks Plans to Unveil Electric & Autonomous Trucks Within Next 2-yrs*, Nasdaq.com, (23 April 2018). Retrieved on 02 May 2018 from https://www.nasdaq.com/article/volvos-ud-trucks-plans-to-unveil-electric--autonomous-trucks-within-next-2yrs-20180423-00764

[T18] *UD Trucks' innovation roadmap aims to offer fully-electric, autonomous trucks towards 2030*, Automotiveworld.com, (23 April 2018). Retrieved on 02 May 2018 from https://www.automotiveworld.com/news-releases/ud-trucks-innovation-roadmap-aims-offer-fully-electric-autonomous-trucks-towards-2030/

[T19] Howell, D., et al., *Enabling Fast Charging: A Technology Gap Assessment*, Office of Energy Efficiency & Renewable Energy, (October 2017). Retrieved on 02 May 2018 from https://www.energy.gov/sites/prod/files/2017/10/f38/XFC%20Technology%20Gap%20Assessment%20Report_FINAL_10202017.pdf

[T20] Gannon, Rob, *With some all-electric buses, Metro Transit rides into the future*, The Seattle Times, (02 October 2017). Retrieved on 03 May 2018 from https://www.seattletimes.com/opinion/with-some-all-electric-buses-metro-transit-rides-into-the-future/

[T21] Technavio, *Global Electric Bus Market 2016-2020*, published by Technavio, (April 2016). Retrieved on 03 May 2018 from https://www.technavio.com/report/global-automotive-manufacturing-electric-bus-market?utm_source=T5&utm_medium=BW&utm_campaign=Media

[T22] Kilcarr, Sean, *Navigating the many challenges facing trucking*, FleetOwner.com, (18 April 2017). Reetrieved 03 May 2018 from http://www.fleetowner.com/blog/navigating-many-challenges-facing-trucking

[T23] Shankleman, Jess, *The Electric Car Revolution Is Accelerating*, Bloomberg News, (06 July 2017). Retrieved on 04 May 2018 from https://www.bloomberg.com/news/articles/2017-07-06/the-electric-car-revolution-is-accelerating

[T24] Burks, S. V., Belzer, M., Kwan, Q., Pratt, S., Shackelford, S., *Trucking 101: An Industry Primer*, Transportation Research Board, Transportation Research Circular Number E-C146, (December 2010). Retrieved on 04 May 2018 from http://onlinepubs.trb.org/onlinepubs/circulars/ec146.pdf

[T25] Mathers, Jason, *How electric trucks could disrupt highway transport and save businesses billions*, Environmental Defense Fund, (04 January 2018). Retrieved on 03 May 2018 from https://www.edf.org/blog/2018/01/04/how-electric-trucks-could-disrupt-highway-transport-and-save-businesses-billions

16.12 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.

[PAGE INTENTIONALLY LEFT BLANK]

17 Glossary of Abbreviations

AC	Alternating Current
ACL	Access Control List
ADAS	Advanced Driver Assistance Systems
ADR	Automated Demand Response
AMI	Advanced Metering Infrastructure
APN	Access Point Name
APT	Advanced Persistent Threat
ATA	American Trucking Association
AVR	Automatic Voltage Regulator
BAS	Building Automation System
BEC	Business Email Compromise
BEMS	Building Energy Management System
BES	Bulk Electric System or “Power Grid”
BMS	Building Management System
CA	Certificate Authority
CAPEC	Common Attack Pattern Enumeration and Classification Schema
CAN	Controller Area Network
CCC	Chaos Computer Club
CCS	Combined Charging System
CCTV	Closed-Circuit Television
CD-ROM	Compact Disk – Read Only Memory
CDMA	Code Division Multiple Access
CEMs	Central Energy Management Systems
CF	Compact Flash
CI	Critical Infrastructure
CIP	Critical Infrastructure Protection
CIS	Customer Information System
CPP	Critical Peak Pricing
CSP	Commercial Service Provider
DC	Direct Current
DER	Distributed Energy Resources
DERMS	Distributed Energy Resources Management Systems
DGM	Distribution Grid Management

DHS S&T CSD	Department of Homeland Security Science and Technology Cyber Security Division
DIN	Deutches Institut fur Normung e.V. (The German Institute for Standardization
DMS	Distribution Management System
DMZ	Demilitarized Zone
DOE	Department of Energy
DoS	Denial-of-Service
DDoS	Distributed Denial-of-Service
DOT	Department of Transportation
DR	Demand Response
DRAS	Demand Response Automation Server
DSM	Diagnostic Security Module
DSO	Distribution Systems Operator
DSRC	Dedicated Short Range Communication
ECU	Electronic Control Unit
EESA	Electronic Energy Storage Assemblies
EHV	Extra High Voltage
ELD	Electric Data Loggers
ENCS	European Network for Cyber Security
ERP	Enterprise Resource Planning
ESCC	Electricity Subsector Coordination Council
ESCWG	Energy Sector Control Systems Working Group
ET	Electronic Transportation
EV	Electric Vehicle
EVSE	Electric Vehicle Supply Equipment
FDEMS	Field DER Energy Management System
FEP	Front End Processor
FERC	Federal Energy Regulatory Commission
FISMA	Federal Information Security Management Act
FMCSA	Federal Motor Carrier Safety Administration
GCWR	Gross Combined Weight Rating
GPS	Global Positioning System
GSM	Group Special Mobile
GSMC	Global Systems for Mobile Communication
GVW	Gross Vehicle Weight

GVWR	Gross Vehicle Weight Rating
HAN	Home Area Network
HDEV	Heavy Duty Electric Vehicle
HITB	Hack-In-The-Box
HMI	Human-Machine Interface
HVAC	Heating, Ventilation, and Cooling
HVDC	High-Voltage Direct Current
ICE	Internal Combustion Engine
ICS	Industrial Control System
ICMP	Internet Control Message Protocol
ICT	Information and Communications Technologies
IDS	Intrusion Detection System
IEA	International Energy Agency
IED	Intelligent Electronic Device
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
INL	Idaho National Laboratory
IT	Information Technology
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
ISO	International Organization of Standardization
ISO	Independent Systems Operator
IVI	In-Vehicle Infotainment
JTAG	Joint Test Action Group
kV	kiloVolts
LAN	Local Area Network
LCV	Longer Combination Vehicles
LEMS	Local Energy Management System
LEV	Light Electric Vehicle
LIN	Local Interconnect Network
LSS	Line Sharing Switch
LTC	Load Tap Charger
LTL	Less-than-Truckload

MDEV	Medium Duty Electric Vehicle
MDMS	Meter Data Management System
MITM	Man in the Middle
MWs	Megawatts
NCCIC	National Cybersecurity and Communications Integration Center
NEC	National Electrical Code
NERC	North American Electric Reliability Cooperation
NESCOR	National Electric Sector Cybersecurity Organization Resource
NFC	Near Field Communication
NHTSA	National Highway Traffic Safety Administration
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency Report
NSTC	National Science and Technology Council
NTP	Network Time Protocol
OBD	On-Board Diagnostic
OC	Optical Carrier
OCA	Open-Charge Alliance
OCPP	Open Charge Protocol
OEM	Original Equipment Manufacturer
OOIDA	Owner-Operator Independent Drivers Association
OpenADR	Open Automated Demand Response
OPSEC	Operational Security
OTA	Over the Air
OTAP	Over the Air Programming
PCB	Printed Circuit Board
PCC	Point of Common Coupling
PDC	Phasor Data Concentrator
PEV	Plug-In Electric Vehicle
PHEV	Plug-In Hybrid electric Vehicle
PII	Personal Identification Information
PIN	Personal Identification Number
PKES	Passive Keyless Entry and Start

PKI	Public Key Infrastructure
PLC	Power Line Carrier
PMU	Phasor Measurement Unit
PoC	Proof-of-Concept
PWM	Pulse-Width Modulation
QoS	Quality of Service
RACI	Responsible, Accountable, Consulted, and Informed
RBAC	Role-Based Access Control
RCE	Remote Code Execution
RDS	FM Radio Data Service
REP	Retail Energy Provider
RF	Radio Frequency
RFID	Radio-Frequency Identification
RP	Recommended Practice
RTO	Regional Transmission Organization
RTU	Remote Terminal Unit
SAE	Society of Automotive Engineers
SCADA	Supervisory Control and Data Acquisition
SD	Secure Digital
SEP	Smart Energy Profile
SGIP	Self-Generation Incentive Program
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SME	Subject Matter Expert
SMS	Short Message Service
SOTAU	Secure Over the Air Updates
SVC	Static VAR Compensators
TLS	Transportation Layer Security
TMC	The Maintenance Council
TOC	Total Cost of Ownership
TOU	Time-of-Use
TPM	Trusted Platform Module
TPMS	Tire Pressure Monitoring System

TWG	Technical Working Group
UBI	Usage-Based Insurance
UDS	Unified Diagnostic Services
UHV	Ultra-High Voltage
UMTS	Universal Mobile Telecommunications System
USB	Universal Serial Bus
V2G	Vehicle to Grid
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
VDA	Vehicle Diagnostic Adapter
VLAN	Virtual Local Area Network
VMT	Vehicle Miles Traveled
Volpe	John A. Volpe National Transportation Systems Center
VPN	Virtual Private Network
VTO	Vehicle Technology Office
W3C	World Wide Web Consortium
WAMPAC	Wide Area Monitoring, Protection, and Control
WAN	Wide Area Network
WPT	Wireless Power Transfer
xFC	Extreme Fast Charging
XSS	Cross-site Scripting

APPENDIX A: NMFTA Survey of Heavy Electric Vehicle Use Cases

1 Survey Overview

In January of 2018, NMFTA conducted an informal survey among our less-than-truckload (LTL) motor freight carrier members to determine practical usage scenarios for electric trucks. We received replies from many different LTL carriers of different sizes and geographic locations. While we did not receive a multitude of responses, we believe that the answers are representative of our membership. The survey consisted of six questions that are outlined below, along with anonymized and randomized answers, which we thought were indicative of the sample set and useful in our analysis.

1.1 About how many vehicles do you keep per terminal, e.g. min to max, that you would need to charge at the same time?

No electric trucks…but as many as 25 electric forklifts. That facility has 5 charging stations. IF we switched to electric trucks, we would probably ONLY consider a hydrogen fuel Cell vehicle rather than battery-only. With as many as 150 trucks at one of our facilities, we would need 50 to 75 charging stations and electrical input that would far exceed the available capacity from our utility company to effectively provide in a single location, absent a substation.
Dependent upon operating range. At this point, likely 1 to 10 potential
On average about 35 per terminal
Number of units at each service center varies by location from 12 power units at smaller locations to 70 power units at larger locations
With 8 small terminals, I range from 1 unit to 7 units. If I had elec units, I would need to charge all units at the end of the work day.

1.2 **Do you have vehicles that are operated without a significant period of rest, i.e. 6 to 8 hours?**

Yes. All our Linehaul vehicles are used, during the day, by P&D driver and in the eve/night by a Linehaul driver. So, about 1,200.
Multiple yes responses
About 5,000 trucks
Most of my units operate on a continuous basis from 0600-1800. Only my evening linehaul units (3 units) are operated outside these hours. They operate 1700 to about 0300

1.3 What would be the maximum vehicle charge time to accommodate efficient operations?

60 minutes would stretch it.
Dependent upon location but estimate 6-8 hours
I could accommodate up to 10 hours
Distance traveled based, quick charge vs. full charge, etc. You can fill a truck at 40 gal/min that is roughly 292 miles per minute of charge, just to break even.
The majority of our units are of the dual use variety and wouldn't allow for the down time necessary to charge an electric vehicle

1.4 Which type of usage would have a higher priority for electric trucks, i.e. last mile delivery, long haul, short haul, etc.?

Last mile and short haul trucks
Short Haul and Final Mile
The extremes, Brooklyn, NY where trucks get no MPG, and trucks that run extreme high miles as it has a high rate of fuel burn
Pickup and delivery, last mile delivery, intermodal shuttle
I would guess that our use for an electric vehicle would be in our city operation (Short Haul).

1.5 How important is it to be able to calculate electric fuel operating cost (cost per MwH/mile)?

Just as significant as Diesel MPG.
It is important to understand the operational efficiency compared to other fuels but more so to understand total cost of ownership.
Essential. How would you make operating decisions without it?
As far as calculating electric fuel cost we're not familiar enough with the available systems to enable an accurate answer but would guess that Yes MwH/Mile would be important
Knowing my operating cost is critical

1.6 Do you have any environmental performance concerns regarding electric trucks such as low operating temperatures, etc.?

Low operating temperatures, life of battery, durability of battery in trucking application, short operating cycles during the dispatch (city P&D work, for instance), range effects of accessory operation such as lift gates, etc. Other concerns: safety lockouts for technicians, safety lockouts for emergency responders in the event of accidents, battery containment in the event of accidents, ergonomics for battery replacement, weight displacement for range, etc.
Yes, environmental concerns related to cold weather locations. Resources necessary to equip our terminals with the charging stations
Sure, range vs temp? Power vs Temp? Battery degradation over time, replacement costs, maintenance projections, etc.
Yes – where will all the electrical power come from? Coal? That is why we believe a Hydrogen Fuel cell vehicle makes more sense than an all-electric-battery truck. We ordered one fuel cell truck.
With the winters being in a sub-zero condition at times, we need the ability to be fully functional in these extreme weather conditions.

1.7 Conclusion

At this point in time, we do not see wide adoption of electric trucks nor do we see serious consideration for this among our members. The ability to accurately gauge operating costs, range, load capacity, and maintenance/operational impact are key to adoption. From the survey participant's perspective, there is not enough readily available real world data on the emerging electric trucks. More research needs to be conducted on how the electric trucks perform in real world environment and in various operating capacities. Additionally, given the large batteries required to power Class 8 electric trucks charge time, load capacity, and range are also going to be key factors for adoption. While rapid charging technology is being developed that might be able to improve charge times, there are also operating safety and capacity concerns given those higher charging rates. Practical charging solutions need to be developed to allow multiple vehicles to charge quickly and safely without having to install power generation equipment at every facility.

APPENDIX B: NMFTA Survey on the Usage of Electric Forklifts

1 Survey Overview

In January of 2018, NMFTA conducted an informal survey among our less-than-truckload (LTL) motor freight carrier members to determine current usage of electric forklifts as an indicator of issues or concerns that might arise in the adoption of electric trucks. We received replies from many different LTL carriers of different sizes and geographic locations. While we did not receive a multitude of responses, we believe that the answers are representative of our membership. Only three (3) of the 13 respondents use electric forklifts. The most common fuel type was propane. The survey consisted of eight questions that are outlined below, along with anonymized and randomized answers, which we thought were indicative of the sample set and useful in our analysis.

1.1 How many electric forklifts to do you have in operation?

14 electric lift trucks
22 electric forklifts
6 electric forklifts
zero - all propane
Zero

1.2 What are the makes/models of units?

Crowns, Raymond, Toyota. Models include: sit down 2500# capacity, stand up reach lifts, and double reach lifts
Toyota 5000#
Crown 5200 series
N/A

1.3 How many charging stations do you operate?

10 charging stations
6 charging stations
30+
N/A

1.4 Are the charging stations from the forklift OEM or are they 3rd party?

Hawker Lifeplus
3rd party. 2 – Enforcer HF10 , 8 – Enersys Express TwinMax (2 lifts can plug into 1 charging station)
OEM primarily
N/A

1.5 Do the forklifts communicate with the charging stations or external systems?

Charging stations do communicate with the forklifts. They do not communicate to any external systems.
Yes, they monitor charge cycles
No
N/A

1.6 Do the charging stations connect to the internet or other communications networks?

They are capable, but not attached
No
No
N/A

1.7 What is the charge time for the forklifts?

7 hours
8 hours
2-4 hours
N/A

1.8 Are there any existing concerns or issues regarding their operation and maintenance?

Battery acid spills during refills
No concerns at this time.

General preventative maintenance is done in house. Any outside maintenance is always slow and expensive. The talent is questionable for OEMs, often they replace multiple items until they find the issue. Always over quoting the repairs needed.
N/A

1.9 Conclusion

The survey revealed that most motor freight carrier operations utilize propane-fueled forklifts and that there is no major ongoing shift towards electric forklifts. One of the more interesting aspects of the survey was the communication link between the forklift and the charging station and internet capability of some charging stations. Battery and vehicle maintenance seem to be an issue. Serious consideration must be given to how fleet operators can safely maintain the larger batteries on Class 8 electric vehicles. The lack of qualified technicians to work on Class 8 electric vehicles could be a major obstacle to successful adoption, as it could have a negative impact on operational costs.

DOE/DHS/DOT Volpe Technical Meeting on Electric Vehicle and Charging Station Cybersecurity Report

Prepared by:
United States Department of Transportation Volpe Center and
United States Department of Energy Office of Policy

Final Report—March 2018

DOT-VNTSC-DOE-18-01

Prepared for:
U.S. Department of Energy.
1000 Independence Ave., S.W.
Washington, DC 20585-1615

U.S. Department of Transportation
Volpe Center

Disclaimer

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE:	3. REPORT TYPE AND DATES COVERED
	March 2018	Technical Meeting Report

4. TITLE AND SUBTITLE	5a. FUNDING NUMBERS
DOE/DHS/DOT Volpe Technical Meeting on Electric Vehicle and Charging Station Cybersecurity Report	VXU6A1/RE572
6. AUTHOR(S) Kevin Harnett, Brendan Harris, Daniel Chin, Graham Watson	5b. CONTRACT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) U.S. Department of Transportation John A. Volpe National Transportation Systems Center 55 Broadway Cambridge, MA 02142-1093	8. PERFORMING ORGANIZATION REPORT NUMBER DOT-VNTSC-DOE-18-01
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) U.S. Department of Energy 1000 Independence Ave., S.W. Washington, DC 20585-1615	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
11. SUPPLEMENTARY NOTES	
12a. DISTRIBUTION/AVAILABILITY STATEMENT This document is available to the public on the National Transportation Library (NTL) Repository and Open Science Access Portal (ROSA P) website at:	12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)

On November 29-30, 2017, the U.S. Department of Energy's (DOE) Office of Policy (OP), in collaboration with DOE's Vehicle Technology Office (VTO), the U.S. Department of Homeland Security's (DHS) Science and Technology Directorate (S&T) Cyber Security Division (CSD), and the U.S. Department of Transportation's (DOT) John A. Volpe National Transportation Systems Center (Volpe), held a technical meeting on key aspects of electric vehicle (EV) and electric vehicle supply equipment (EVSE) cybersecurity. This report summarizes key takeaways and discussion points.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Electric Vehicle (EV), Electric Vehicle Supply Equipment (EVSE), Cybersecurity, Charging Station, Smart Grid, Utility, Building Energy Management Systems (BEMS), Vehicle Technology Office (VTO)	28
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASS	UNCLASS	UNCLASS	Unlimited

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18
298-102

Acknowledgments

The Department of Energy (DOE) and U.S. DOT Volpe Center would like to thank subject matter experts (SMEs) from the California Public Utilities Commission's (CPUC) Vehicle-Grid Integration Communications Protocol Working Group, Idaho National Laboratory (INL), Lear Corporation, Fiat Chrysler Automotive (FCA), and Daimler AG for their insight on topics in this report. In addition, we would like to acknowledge and give thanks to all the organizations who participated in the DOE/DHS/DOT Volpe Center Technical Meeting on Electric Vehicle and Charging Station Cybersecurity on November 29-30, 2017, in Arlington, VA, and for providing their insights and expertise.

Contents

List of Figures

List of Tables

List of Abbreviations

Abbreviation	Term
ADR	Automated Demand Response
AMI	Advanced Metering Infrastructure
BEMS	Building Energy Management System
CAN	Controller Area Network
CCC	Chaos Communications Conference
CCS	Combined Charging System
CD	Compact Disk
CDMA	Code Division Multiple Access
CEMS	Central Energy Management Systems
CharlN e.V.	The Charging Interface Initiative
DC	Direct Current
DCFC	DC Fast Charger
DHS S&T CSD	Department of Homeland Security Science and Technology Cybersecurity Division
DIN	Deutsches Institut für Normung e.V. (the German Institute for Standardization)
DOE	Department of Energy
DOS	Denial of Service
DOT	Department of Transportation
DSO	Distribution System Operator
ECU	Electronic Control Unit
EESA	Electrical Energy Storage Assemblies
ENCS	European Network for Cyber Security
ESCC	Electricity Subsector Coordinating Council
ESCSWG	Energy Sector Control Systems Working Group
EV	Electric Vehicle
EVSE	Electric Vehicle Supply Equipment
FISMA	Federal Information Security Management Act
GPS	Global Positioning System
GSM	Global System for Mobile Communications
HAN	Home Area Network
HITB	Hack-in-the-Box
ICT	Information and Communications Technologies
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
INL	Idaho National Laboratory
IoT	Internet of Things
ISO	International Organization of Standardization
ISO	Independent System Operator

Abbreviation	Term
LEV	Light Electric Vehicle
MITM	Man In The Middle
NEC	National Electrical Code
NERC	North American Electric Reliability Corporation
NESCOR	National Electric Sector Cybersecurity Organization Resource
NFC	Near Field Communications
NHTSA	National Highway Traffic Safety Administration
NIST	National Institute of Standards and Technology
NSTC	National Science and Technology Council
OBD	On-Board Diagnostic
OCA	Open Charge Alliance
OEM	Original Equipment Manufacturer
OP	Office of Policy
OTA	Over The Air
PEV	Plug-In Electric Vehicle
PHEV	Plug-In Hybrid Electric Vehicle
PIN	Personal Identification Number
RF	Radio Frequency
RTO	Regional Transmission Organization
SAE	Society of Automotive Engineers
SD	Secure Digital
SME	Subject Matter Expert
SMS	Short Message Service
TLS	Transportation Layer Security
TPMS	Tire Pressure Monitoring System
UMTS	Universal Mobile Telecommunications System
USB	Universal Serial Bus
V2G	Vehicle to Grid
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
VTO	Vehicle Technology Office
W3C	World Wide Web Consortium
WPT	Wireless Power Transfer
XSS	Cross-site scripting

Executive Summary

On November 29-30, 2017, the U.S. Department of Energy's (DOE) Office of Policy (OP), in collaboration with DOE's Vehicle Technology Office (VTO), the U.S. Department of Homeland Security's (DHS) Science and Technology Directorate (S&T) Cyber Security Division (CSD), and the U.S. Department of Transportation's (U.S. DOT) John A. Volpe National Transportation Systems Center (Volpe) held a technical meeting on key aspects of electric vehicle (EV) and electric vehicle supply equipment (EVSE) cybersecurity. This report summarizes key takeaways and discussion points.

Electric vehicles are becoming a part of the transportation and mobility industry in the United States. It is during this initial development and deployment period for the EV environment that the opportunity exists to mitigate cybersecurity issues before they become widespread, ingrained, difficult, and expensive to remedy. The EV environment is a mix of multiple stakeholders, domains, hardware, and software. As the communication, electricity, and transportation systems become more integrated, cybersecurity vulnerabilities that would normally be localized, now have the ability to cause disruptions across these multiple sectors.

Modern day automobiles have cybersecurity vulnerabilities that the industry and government are working on addressing.[1] This report, and the preceding technical meeting, focuses on the cybersecurity vulnerabilities that are unique to electric vehicles and electric vehicle supply equipment:

- The two-way communication between the EVSE and the vehicle
- The connection between EVs, EVSE, and other systems (e.g., grid, telecommunications, buildings, etc.)

These differences could potentially lead to three main types of issues:

1) Public safety hazard to the vehicle operators and/or those in the immediate vicinity
2) Mobile, highly connected malware vectors
3) Initiating and/or exacerbating electric grid disruption

As a result of discussions during the Electric Vehicle and Charging Infrastructure Cybersecurity Technical Meeting, participants identified gaps and vulnerabilities in this threat space (see Chapter 7: Gaps and Conclusions for more detail on the gaps). The table below is a prioritized list of the gaps identified and provides a short description of each:

[1] https://www.nhtsa.gov/technology-innovation/vehicle-cybersecurity

Identified Gap	Gap Description
EVSE Charging Infrastructure Lacks Cybersecurity Best Practices	The EV industry does not have secure software design and development methodology guidance to design and build "secure" EVSE capabilities. Purchasing agents who buy EVSEs do not typically specify cybersecurity protections (e.g. secure OTA firmware update capability, authentication) for their EVSE products due to lack of EVSE cybersecurity guidelines for the EVSE acquisitions.
End-to-End EV and Charging Infrastructure Lacks a Trust Model	There is no consensus on end-to-end trusted communication standards for securing communications between the electric vehicle and the charging infrastructure.
EV/Charging Infrastructure Lacks Cybersecurity Testing	There is a lack of formal cybersecurity testing and assessment applied to the entire EV charging infrastructure.
Wireless Chargers Lack Common Cybersecurity Guidelines	Light passenger EVs, electric buses and electric trucks have similar wireless charging communications paths, and none of them have guidance on the unique cybersecurity requirements specifically for wireless charging.
EV Over-the-Air (OTA) Infrastructure Update Capability Is Immature	Current EV infrastructure (i.e. EVSEs, Smart Meters, Advanced Metering Infrastructure-AMI, Demand Energy Response equipment, etc). OTA update capability is immature and insecure and vulnerable to cyberattacks. Insecure legacy equipment will need to be addressed at the same time as new EV equipment is designed to have better and more secure OTA capabilities.
Commercial EVSE Lack of Common Physical Security Guidelines	Physical damage to commercial EVSEs can result in non-operational units which could have an adverse effect on consumer confidence in EVs in general. Some types of physical damage whether intentional or not, may expose the public to harmful electric current levels. There is a lack of common Physical Security Guidelines for Commercial EVSE Physical Security.

Throughout the technical meeting, participants particularly focused on two of these gaps as critical for government and industry to address:

1. The lack of security best practices for EVSE charging infrastructure
2. The lack of an end-to-end trust model for validating communications

Addressing these critical gaps should help focus and frame coordination between the relevant stakeholders in the energy, transportation, and communication sectors.

1 Background/Introduction

The global electric vehicle stock surpassed one million vehicles in 2015 and grew to more than two million electric vehicles in 2016.[2] Growing at a similar rate, the number of EV charging stations deployed globally reached two million in 2016.[3] In the United States, the EV stock was nearly 600,000 vehicles and EVs made up nearly one percent of total vehicle sales in 2016.[4] As EV and EVSE deployment continue their growth, research and development of technologies that ensure safe and secure operating conditions of the electric vehicle fleet would be cost effective and beneficial.

1.1 Structure of the Report

On November 29-30 2017, the U.S. Department of Energy's (DOE) Office of Policy (OP), in collaboration with DOE's Vehicle Technology Office (VTO), the U.S. Department of Homeland Security's (DHS) Science and Technology Directorate (S&T) Cyber Security Division (CSD), and the U.S. Department of Transportation's (DOT) John A. Volpe National Transportation Systems Center (Volpe), held a technical meeting on key aspects of electric vehicle (EV) and electric vehicle supply equipment (EVSE) cybersecurity. The object of the technical meeting was not to obtain any group position or consensus. Rather, the organizers were seeking as many recommendations as possible from all individuals at the meeting.

The meeting brought together diverse stakeholders from the EV environment: vehicle manufacturers, charging station manufacturers and operators, academia, and federal and state governments. The purpose of the meeting was to explore current and future research and development in EV and EVSE cybersecurity. In their discussions at this meeting, the participants identified the takeaways and gaps contained in this report. The report also includes some background information and contextual information added for the convenience of the reader.

Section 1 gives a brief background on general vehicle cybersecurity and discusses unique electric vehicle cybersecurity concerns. Section 2 summarizes discussion and provides information on how organizations within this space can improve their cybersecurity preparedness through the structure of their organizations. Section 3 summarizes ideas expressed throughout the technical meeting on how to improve EV cybersecurity before deployment in order to increase security and save costs. Section 4 digs into the importance of establishing trust through verification, across and within systems. Section 5 discusses challenges around the supply chain of EV charging equipment and liability. Section 6 discusses how to improve sector cooperation and communication to address cybersecurity concerns early and effectively.

---

[2] International Energy Administration. Global EV Outlook 2017: Two Million and Counting. 2017. https://www.iea.org/publications/freepublications/publication/GlobalEVOutlook2017.pdf

[3] International Energy Administration. Global EV Outlook 2017: Two Million and Counting. 2017. https://www.iea.org/publications/freepublications/publication/GlobalEVOutlook2017.pdf.

[4] International Energy Administration. Global EV Outlook 2017: Two Million and Counting. 2017. https://www.iea.org/publications/freepublications/publication/GlobalEVOutlook2017.pdf.

Section 7 of the report contains gaps that were identified during the recent cybersecurity technical meeting, as well as through information gleaned from discussions with Energy Sector SMEs.

1.2 General Vehicle Cybersecurity Concerns Background

Today's automobiles are complex machines that can contain many embedded electronic control units (ECUs), networks to support these units, and a host of wired and wireless external interfaces. Wired interfaces include Universal Serial Bus (USB), compact disks (CDs), and secure digital cards (SD cards). Wireless interfaces include short range and long range connectivity through Bluetooth, Wi-Fi, radio frequency (RF), near-field communications (NFC), Global System for Mobile Communications (GSM), coded-division multiple access (CDMA), and Universal Mobile Telecommunications System (UMTS).

The wireless interfaces can support a host of features, including remote tire pressure monitoring systems (TPMS), telematics, and smart key/keyless entry/ignition start. They also enable vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications (collectively referred to as V2X communications), which could improve vehicle/driving efficiency, comfort, and safety. The continuing trend in vehicle architecture is a shift towards more open systems and away from the traditional closed/proprietary system type of architecture. This increased connectivity creates a number of potential security vulnerabilities in vehicles.

Supported by grants from the U.S. National Science Foundation, collaborations between researchers at the University of California San Diego and the University of Washington in 2010 and 2011 identified vehicle cybersecurity vulnerabilities:

- **Experimental Security Analysis of a Modern Automobile (2010)**[5]: The analysis assumed that unauthorized parties had (at least temporary) physical access to the vehicle's computer networks (e.g. able to plug their own hardware into a port underneath the dash). The researchers analyzed and evaluated the computers within the internal networks of a modern vehicle and described the range of security issues discovered in the process.
- **Comprehensive Experimental Analyses of Automotive Attack Surfaces (2011)**[6]: The major objective of this work focused on three key classes of remote attack vectors without physical contact with the vehicle: indirect physical, short-range wireless, and long-range wireless. The cybersecurity testing evaluated representative examples of each of these classes of remote attack vectors and clearly found it possible to exploit these vectors.

In 2017, the U.S. Department of Transportation's National Highway Safety Administration (NHTSA) took a proactive safety approach to protect vehicles from malicious cyber-attacks and unauthorized access by releasing proposed guidance for improving motor vehicle cybersecurity.[7] To ensure a comprehensive approach to cybersecurity, NHTSA has adopted a multi-faceted research approach that leverages the U.S. National Institute of Standards and Technology Cybersecurity Framework[8] and

[5] http://www.autosec.org/pubs/cars-oakland2010.pdf
[6] http://www.autosec.org/pubs/cars-usenixsec2011.pdf
[7] https://www.nhtsa.gov/technology-innovation/vehicle-cybersecurity
[8] https://www.nist.gov/cyberframework

encourages industry to adopt practices that improve the cybersecurity posture of vehicles.

1.2.1 Telematics

Telematics in the automobile industry refers to the embedded system on board a vehicle that tracks the vehicle and combines wireless telecommunications and information processing to send, receive, and store information related to vehicles. For example, telematics include original equipment installed by the manufacturer, after-market add-on systems, and/or mobile device applications and programs. In addition, telematics involve a variety of applications such as GPS tracking, engine diagnostics, vehicle monitoring and drive identification, in-vehicle recording, and instant driver feedback. As the advancement in vehicle telematics/infotainment systems and integration of numerous technologies in them rapidly grow, the security vulnerabilities in vehicles equipped with telematics/infotainment systems expand exponentially.

In a basic telematics system, vehicles gather and send data on location and vehicle status to a telematics service center that stores the data which can be accessed by the account owners of that data (see Figure 1). Telematics should be thought of and treated as a system, from the vehicle to the on-board telematics devices to the communications cloud to the data management and storage systems.

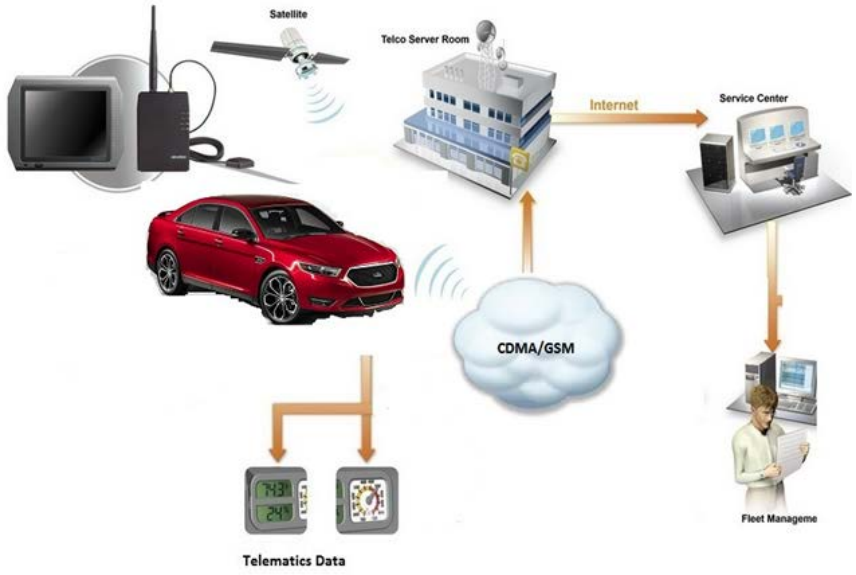


Image credit: Haulage Report Now

Figure 1. Typical Telematics System

The signal path of the data from the telematics device is also an area of concern as it is vulnerable to man-in-the-middle attacks. Cybersecurity penetration testing of after-market telematics devices has uncovered multiple vulnerabilities such as:

- Accepted unauthenticated administrative commands via Short Message Service (SMS)
- Loaded a home-grown trojan firmware
- Unauthenticated services on the Internet

- No encryption of data in transit

Of particular interest to the government fleet community is Executive Order 13693, which states:[9]

> *"If the agency operates a fleet of at least 20 motor vehicles, improve agency fleet and vehicle efficiency and management by … collecting and utilizing as a fleet efficiency management tool, as soon as practicable but not later than 2 years after the date of this order, agency fleet operational data through deployment of vehicle telematics at a vehicle asset level for all new passenger and light duty vehicle acquisitions and for medium duty vehicles where appropriate."*

Since most government fleet vehicles are older models, few, if any, have original equipment manufacturer (OEM) installed telematics, after-market telematics devices must be employed to meet the Executive Order.

From the federal perspective, the telematics system is considered an information system requiring Federal Information Security Management Act (FISMA) compliance. FISMA requires compliance with NIST standards. To help government fleet managers comply with FISMA, the U.S. Department of Transportation's Volpe Center, in cooperation with the U.S. Department of Homeland Security's Science and Technology Cybersecurity Division, created a document entitled *Cybersecurity Primer for Fleet Managers* which identifies 31 security controls for telematics from *Draft NIST 800-53: Security and Privacy Controls for Information Systems and Organizations*[10]. FedRAMP program provides requirements for cloud-based IT, which is relevant for telematics as well.[11]

1.2.2 Controller Area Network (CAN) Bus

The most common embedded network in a vehicle is the Controller Area Network (CAN) bus. All traffic to and from the components on the network is broadcasted simultaneously. Each component "listens" to all message traffic but only acts on messages explicitly addressed to it and ignores all others.

The CAN bus connects almost all of the components responsible for the operation of the vehicle and was originally designed with maintenance in mind. Maintenance personnel focused on the operations, troubleshooting, and fine-tuning of the automobile must have access to the network. This access is provided via an on-board diagnostics (OBD) port located within the cabin of the vehicle, usually under the steering wheel. Starting in 1996 in the United States, and 2001 in Europe, every vehicle is required to contain a standardized common access port to the CAN, such as OBD-II.

Anyone can control the flow of data by sending a data packet to a target electronic control unit (ECU) through the CAN bus. This method of injecting data packets can match any data packet transmitted

[9] Executive Order 13693: Planning for Federal Sustainability in the Next Decade. March 19, 2015. https://www.gpo.gov/fdsys/pkg/FR-2015-03-25/pdf/2015-07016.pdf

[10] National Institute of Standards and Technology. NIST 800-53: Security and Privacy Controls for Information Systems and Organizations. August 2017. https://csrc.nist.gov/CSRC/media//Publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf

[11] https://www.fedramp.gov/

across the network, including data packets that control functions like vehicle speed, braking, and steering. Since all CAN data packets are passed unauthenticated across the network, all messages are assumed to be legitimate messages originating from within the vehicle. With an open access port such as the OBD-II, any entity or device with access to that port can influence the vehicle systems on the network. Currently, there are many software and hardware tools that allow a user to broadcast custom CAN messages through the OBD-II port.

One of the greatest dangers with any kind of attack is repeatability. Once an attacker develops an attack, they can publish the attack steps on the web, or produce a "canned" version of the attack. A cursory search of the Internet will illustrate the extensive breadth of information shared and vehicle hacks performed utilizing the OBD-II port and CAN bus. This gives potential actors with less technical expertise the ability to carry out the attack.

Integrating after-market features, often used in fleet management, results in an expansion of the access points into the CAN bus. Many, if not all, of these devices allow external access directly to the vehicle's CAN bus, and, thus, all vehicle components connected to it.

1.3 Cybersecurity Considerations for the Electric Vehicle

In addition to the vulnerabilities present in newer vehicle models, EVs present unique cybersecurity vulnerabilities because of their connections to other infrastructure and communication systems. When an EV refuels, it is physically and electronically connected to and exchanges information with EVSE (see Table 1.). The EVSE is an additional external interface into the internal network of the vehicle and to the electricity grid. While there are standards for the communications between the vehicle and the grid (Appendix A), further work could ensure that EVSE and EV cybersecurity is not compromised.

Information	Description
Customer/vehicle/charger ID	Unique identifying numbers for the user, vehicle, and charging station (may also include charging station location)
Control commands	Commands issued or received by the vehicle or charger
Software/firmware downloads/updates	Software downloaded or uploaded to vehicle or charger to facilitate charging process

Table 1. Typical Data Elements Exchanged Between an EV and Charging Station

Compromised EVs and EVSE could be a potential public safety concern, similar to other compromised vehicles or utility distribution equipment.

Power flow between EVSE and electric vehicles need not (necessarily) flow in only one direction. Vehicle-to-grid (V2G) technology is being studied by DOE, the national labs,[12] and the Energy Sector as a

[12] https://www.anl.gov/energy-systems/group/vehicle-grid-interoperability

way to improve the grid's resiliency, reliability, and flexibility in load management. Future EVs could send electricity from their batteries back into the grid via smart chargers during peak times and also reverse the flow during off-peak hours to charge the EV. [13] Ensuring cybersecurity protections are in place is an important part of utilizing this potential use of EVs.

Compromised EVs could spread malware to the EVSE they connect to. This could then be used to spread malware to other EVs connected to that network should the network architecture not be adequately segmented. The mobility of the EVs then could then be leveraged to "infect" other EVSE and, ultimately, other connected systems. Participants at the technical meeting mentioned that the EVSE could be used as a potential entry point for malware to spread to other systems, networks, and grid components.

In many cases, the EVSEs are connected to building energy management systems (BEMS), the electricity grid, telecommunications networks, and billing systems. Participants discussed at the meeting that due to these connections, EVs and EVSE could potentially be leveraged to cause electricity load management disruptions for buildings or the electric grid. For example, traditionally in the BEMS environment power draw is spread across multiple devices making the instance of rapid cycling of large power demands a rare if not impossible occurrence. The advent of large EVSE systems being integrated into the BEMS environment creates a concentrated system with a relatively large power draw. The accessibility and power draw of an EVSE system is a potential mechanism for disrupting the power of a building, or the electricity distribution service in a specific area. In addition, if the attacker installs persistent malware in the EVSE, the duration of the grid disruption can be extended even further.

Listed below are some potential cybersecurity issues which pertain to EVs:

- **Man-in-the-middle at charging station** - Attacker inserts themselves between the EV and the EVSE leading to possible tracking issues, monetary issues, and other privacy issues
- **Payment fraud** at charging station
    - The charger cycle does not last the full amount of time paid for
    - The charger is spoofed into providing free service
- **Privacy/tracking issues** with using EVSEs linked into Smart Grid
- **Intentional overcharging of batteries** via a cybersecurity attack causing possible severe damage to batteries/EV
- **Intentional discharging of batteries** taking the EV out of service/degrading range
- **Denial of service (DOS) attack at EVSEs** - Taking vehicles out of service if unable to re-charge
- **A malware infected EV** - A vehicular "Typhoid Mary" which passes its malware to other EVs via the EVSE
- **Malware infected EV** that passes onboard malware through an EVSE to the Smart Grid or onboard malware through networked EVSEs
- **Rapid cycling of heavy loads** to the grid through multiple compromised EVSEs in order to cause grid failure

[13] https://www.anl.gov/energy-systems/project/ev-smart-grid-interoperability-center

There has been a body of EVSE security testing research conducted by DOE's Idaho National Laboratory (INL):

- **2014-2015**[14]: INL conducted unbiased and independent EVSE testing for efficiency, reliability research, and cybersecurity posture (i.e. remote compromise, unauthorized access, firmware modifications, potential grid impact) on four (4) pre-production systems delivered by Siemens, Eaton, GE, and Delta. Listed below are some potential cybersecurity issues which pertain to EVs:
    - Software Development mistakes (i.e. implementation of "complex" code on a small embedded device leads to poor decision making)
    - Sanity checking of remote input lacking
    - Processes are executed with extensive privileges (i.e. root)
    - Memory corruption vulnerabilities (i.e. ARM, X86)
    - Poor web application implementation SQL injection, cross-site scripting (XSS), input validation, and insecure credentials
    - Billing and price information were manipulated
    - Remote updating was very poorly implemented
    - Malicious firmware lead to full compromise of all units from one vendor

- **2016-2018**[15]: INL conducted cybersecurity testing on two production Level 2 EVSEs and the testing results were only shared with the vendors. INL also conducted cybersecurity testing on a DC Level-2 Fast Charger (DCFC) with both a CHAdeMO and a SAE J1772-Combo cordset. Cybersecurity testing revealed the following findings:
    - A compromised Plug-In Electric Vehicle (PEV) charge module can infect the DCFC vehicle controllers and local servers and vice versa
    - A compromised PEV is not only a potential safety concern, but it is also a grid network access concern. The biggest potential problem is for a coordinated charging event that causes widespread disruption of the grid
    - The cybersecurity testing identified some unknown issues that need to be resolved (e.g. who owns the EVSEs and network connections, are EVSEs considered part of the Utilities network perimeter, and can Utilities handle increased electrical loads)

In addition, there have been two hacker conferences discussions on EVSE hacking and vulnerabilities. In December 2017, the Chaos Communication Congress (CCC) Conference in Germany featured a talk titled "Charging Infrastructure for Electric Cars: Expansion Instead Of Security."[16] The security researcher probed different components of the EVSE system and found security problems, such as:

- Insecure third-party ID tokens that allow copying personal card data and successfully charging with the copy
- Outdated versions of the OCPP protocol based on HTTP that allow setting up a man-in-the-middle attack by relaying the transaction
- Insecure EVSE USB ports that allow logs and configuration data to be copied to the drive via an empty flash drive which provide access to the login/password for the OCPP server via spoofed token numbers

In 2013, the Hack in-the-Box (HITB) conference in Malaysia, featured a talk titled "Who Can Hack a Plug: Infosec risk of Charging Electric Cars." The security researcher identified potential EVSE vulnerabilities

[14] https://www.energy.gov/sites/prod/files/2014/03/f13/vss096_francfort_2013_o.pdf
[15] https://avt.inl.gov/sites/default/files/pdf/presentations/VSATTOctober2015CANBusOverview.pdf
[16] https://www.v3.co.uk/v3-uk/news/3024499/kaspersky-warning-over-electric-car-charging

based on public information (e.g. vendor web sites):[17]

- Firmware can be extracted to identify eavesdropping points and access encryption keys
- RFID and protocol analysis to determine vulnerabilities
- Short range communications (RS-485) bandwidth and latency limits encryption and makes eavesdropping and man-in-the-middle attacks easier
- RFID short range communication is easy to eavesdrop and costly to patch
- If the same symmetric key is used for all EVSEs and payment cards does not scale and is open to relay and card attacks
- Internet of Things (IoT) protocols and web/mobile control are typically insecure
- Charge station Owners charging configuration and Driver payment methods need to be secured

1.3.1 Stakeholders

There many stakeholders in the EV environment (see Table 2). Section 6 of this document addresses the importance of coordination and harmonization of research and development efforts between stakeholders.

[17] https://conference.hitb.org/hitbsecconf2013ams/materials/D2T2%20-%20Ofer%20Shezaf%20-%20The%20Infosec%20Risks%20of%20Charging%20Electric%20Cars.pdf

Stakeholder Type	Examples	Links to the EV environment
Government agencies	- Departments of Energy (DOE) - Department of Transportation (DOT) - Department of Homeland Security (DHS) - State, local, and international governmental agencies	Vehicle and human safety; protection of critical infrastructure; advanced research on EV and EVSE technologies and cybersecurity
Standards bodies	- Institute of Electrical and Electronics Engineers (IEEE) - National Institute of Standards and Technology (NIST) - Society of Automotive Engineers (SAE) - International Organization of Standardization (ISO) - National Electrical Code (NEC)	Implementation of standards and best practices for safety, security, and interoperability
OEMs and Tier 1 Suppliers	- Automobile manufactures	Design and build safe and reliable EVs
Grid owners	- Regional Transmission Organizations (RTOs)/Independent System Operators (ISOs) - Utilities	Produce and transmit electricity, load balance the grid
Technology suppliers	- EVSE vendors and operators - BEMS suppliers - Information and communications technologies (ICT) - Central Energy Management Systems (CEMS) - Payment systems - DER Vendors	Supply the hardware and software systems that allow the EV environment to operate
Researchers	- Academics - White hat hackers - Independent researchers	Study the EV environment for possible vulnerabilities and mitigations, design the next generation EV environment
EV consumers	- General public - Commercial fleets - Government fleets	End users of EV environment technologies

Table 2. EV and Charging Infrastructure Stakeholders

2 Organizational Structure

Cybersecurity should be incorporated into every stage of electric vehicle and EVSE development. To build secure products and then manage identified vulnerabilities, organizations must have structures and corporate policies that support cybersecurity awareness throughout the design, development, and deployment of their devices and systems.

During the design process, domain architects, engineers, and security personnel should coordinate to create secure systems. Once electric vehicles and EVSE leave the manufacturer's floor, they could be monitored regularly to detect irregular behavior. This can help identify vulnerabilities being exploited. If a vulnerability is identified, that information should be shared with the owner, manufacturer, appropriate Information Sharing and Analysis Center (ISAC), and those who can provide solutions to address the vulnerability in a timely manner.

To accomplish the aforementioned goals, some organizations have created an executive position in the c-suite who is in charge of product and/or information security. This officer's responsibilities may include the following functions:[18]

- **Protect, shield, defend and prevent:** Taking preemptive measures to ensure products and information are proactively secured from cyber threats.
- **Monitor, detect, and hunt:** Identifying irregular activity as it occurs.
- **Respond, recover, and sustain:** Minimizing the impacts of the exploited vulnerability and restoring the system to normal operations.
- **Govern, manage, comply, educate, and manage risk:** Creating a work environment where security is a concern in all parts of operation, rather than an afterthought when an incident occurs.

While an executive who oversees security is an important step for integrating cybersecurity into the core of an organization, it is also necessary to define clear paths of information flow. Quick information sharing between security and engineering teams allows identified problems to be remedied quickly which can prevent vulnerabilities from being widely exploited.

An example scenario that a vehicle manufacture or EVSE vendor could think through:

How would our company respond to a compromised charger, charging system, or EVSE vendor?

Relevant sub-questions may include:

- Could our company simply deny any attempt for a vehicle trying to charge at that vendor's stations?
- How would we communicate the denial of charging ability to vehicle owners and operators?
- What happens internally at our company when making these decisions that could potentially impact the reputation of our company?
- Who would need to be brought in on the decision making process?

By testing how an organization responds to an identified vulnerability, the flow of information can be

[18] https://resources.sei.cmu.edu/asset_files/TechnicalNote/2015_004_001_446198.pdf

mapped out and the process for how information gets to those who need to act can be refined. An efficient information sharing procedure will enable an organization to respond in a timely manner to an identified vulnerability. Threat modelling is another way through which an organization can systematically evaluate, identify, assess and address the security risks and vulnerabilities associated with a process or an application. It is one of the ways to map out the attack surface of the application which can assist personnel in devising effective strategies to mitigate those attacks.

3 Incorporating Cybersecurity into Design

Cybersecurity incorporated into the design of EVs and EV charging infrastructure equipment from the onset reduces product vulnerabilities and risk of exploitation far greater than addressing cybersecurity after a system is deployed. Having cybersecurity protections from the start may help prevent basic attacks and provide a solid foundation for improving security and mitigations within the EV environment in the future.

With each addition of a new system, whether software or hardware related, security should be considered a crucial factor in the system development. Since no platform is protected from all vulnerabilities, a way to safely and securely patch the platform is needed. Developers could also establish a vulnerability disclosure program in case vulnerabilities are discovered after production has begun on the system in order to quickly respond to vulnerabilities before they are exploited.

3.1 Segmentation

Separating and securing key components with in a system is an essential element of secure design. Segmentation can prevent a vulnerability from compromising the whole system, by limiting an attacker's access to a small portion of the system. If the attacker wants to move to another part of the system they would need to find another vulnerability to exploit. The attacker will be unable to move freely throughout the network which will limit the damage caused from an exploit.

Segmentation in EVs is crucial because most of the important operational functions of the vehicle communicate through the CAN bus, which can easily be compromised or misused. ECUs are allowed to communicate freely with vehicle systems by broadcasting messages throughout the CAN bus. These messages reach every component in the vehicle that is connected to the network, even if the message is not intended for that component. The correct component responds if the message was addressed specifically to it. This allows for any compromised ECU within the network to broadcast messages to other ECUs it was not intended to interact with. An example of this behavior would be an attacker gaining access to the vehicle's CAN bus through the infotainment system, then broadcasting a message to the vehicle's headlamps turning on the high beams. Segmentation will prevent unrelated communications between components and systems from reaching each other, such as the infotainment system communicating with critical components in the vehicle. If a component or system needs to send information to another within the network, security checks would need to be in place to authenticate the sender, its receiver, and the message itself.

3.2 Chipsets

The use and integration of newer chipsets (integrated circuits that manage data flows) could improve

cybersecurity within a system. Older chipsets are generally basic and only provide features to carry out the task given, excluding cybersecurity. Newer chipsets provide added resources which can include extensive cybersecurity solutions as well as cybersecurity features built in on the chipset. Sometimes, when a vulnerability is found on an older chipset, it can be mitigated by adding an additional process within the chipset; however, it can be difficult to implement additional processes due to the lack of resources on the chipset.

EVs and EVSEs contain many chipsets to communicate within themselves and with each other. One of the most important chipsets is the chipset responsible for communication between the EVSE and the EV related to charging the vehicle. It is important to protect theses communications because they can provide the charging rate, vehicle identification, and billing information. Whether it's through a chip in the chipset or processes to authenticate and check the communication, chipsets that handle this sensitive information should have security features to keep the data safe.

3.3 Penetration Testing

Penetration testing is an important step when incorporating cybersecurity into a system. Penetration testing is used by the manufacturer/designer to find and exploit vulnerabilities in a system before being released to the public. If a vulnerability is discovered, it shows the developers if the mitigations put in place were effective and where improvements can be made in the system to prevent a future attack. Vulnerabilities could be corrected through a patch if the issue is software related or through a redesign if the hardware contains the vulnerability.

It is best to address cybersecurity during the design phase, when it is easier to make changes with the system. Mitigations for identified vulnerabilities can be incorporated into the system and retested with another penetration test to ensure the issue has been resolved. In order to improve cybersecurity in system design most effectively, penetration testing could be done when designing the system as well as to test systems after they have been patched or redesigned in order to maintain the strongest level of security from cyberattacks. Periodic tests should also be conducted to ensure vulnerabilities weren't missed in previous tests.

Within the EVSE, BEMS, and electrical grid network, penetration testing can help ensure the whole system is more secured against attacks and if each system has an effective mitigation solution. The test could also demonstrate that an exploited system will not have a negative impact on other systems and cause issues that can impact public safety. The results of the test will show a level of competency in the whole system to deal with vulnerabilities and the exploits used against them.

The National Electric Sector Cybersecurity Organization Resource (NESCOR) wrote a guide for penetration testing electrical utilities which can be applicable to both electric vehicles as well as electrical vehicle supply equipment.[19] NESCOR's guide breaks down penetration testing into six major

[19] http://smartgrid.epri.com/doc/NESCORGuidetoPenetrationTestingforElectricUtilities-v3-Final.pdf

segments: Penetration Testing Scope, Architecture Review, Target System Setup, Penetration Tasks, End-to-End Penetration Test Analysis, and Result Interpretation and Reporting.

Penetration Testing Scope determines which part of the system the penetration test should focus on. Architecture Review allows the team performing the penetration test to understand the system and possible vulnerabilities in the system. Target System Setup is setting up the test environment in a non-production system that operates as closely to the production system as possible to provide the most accurate test and results possible. Penetration Tasks is testing of each critical component in the system and can be broken down into four categories: server OS, server application, network communication, and embedded device. End-to-End Penetration Test Analysis is a communication gap analysis throughout the system. Result Interpretation and Reporting is the documentation of vulnerabilities discovered and possible mitigation solutions inside a report for future referencing.

3.4 Vulnerability Assessment

The NESCOR Guide to Vulnerability Assessment for Electric Utility Operations Systems can also help provide guidance in mitigating vulnerabilities found within an EVSE or BEMS.[20] The use of the guide could help ensure that the network, system, and system applications are prepared to deal with attackers. The guide explains the methodology the assessors should follow and how they should analyze, interpret, and report their findings. Like penetration testing, not all possible vulnerabilities will be found, but a vulnerability assessment would help mitigate a possible attack and keep the EVSE or BEMS safe.

3.5 EVSE Cybersecurity Procurement Guidelines

Cybersecurity procurement guidelines specify security requirements for new EVSE systems. These guides will tell buyers what cybersecurity measures to look for in EVs, EVSEs, and other systems related to the EVSE when acquiring them for their own use.

Two guides related to cybersecurity procurement language have already been written, though they are not directly related to EVSE systems. The Department of Homeland Security wrote the *Cyber Security Procurement Language for Control Systems*[21] Guide and the Energy Sector Control Systems Working Group (ESCSWG) wrote the *Cybersecurity Procurement Language for Energy Delivery Systems*[22]. It is recommended that both documents are used to produce procurement language for cybersecurity in EVSE systems as they cover both software and hardware security.

[20] http://smartgrid.epri.com/doc/nescor%20vuln%20scan%2006-26-14.pdf
[21] https://ics-cert.us-cert.gov/sites/default/files/documents/Procurement_Language_Rev4_100809_S508C.pdf
[22] https://energy.gov/sites/prod/files/2014/04/f15/CybersecProcurementLanguage-EnergyDeliverySystems_040714_fin.pdf

In August 2017, the European Network for Cyber Security (ENCS), Commissioned by ElaadNL developed a document titled *EV Charging Systems Security Requirements*.[23] In addition, an EVSE Threat Assessment for Secure EV Charging Systems (April 2016) and EV Charging Systems Security Architecture (April 2016) documents were developed. These requirements can be used as part of the security requirements when new EVSE server systems are procured or set up.

[23] https://www.elaad.nl/uploads/files/Security_Requirements_Charge_Points_v1.0_april2016.pdf

4 Trust

Electric vehicles and charging infrastructure need a method to ensure secure trusted communication between the EV and EVSE. An essential concept in cybersecurity, trust is when computers prove their identities to each other through the use of applied cryptography. Key aspects of trusted communications include authentication, data integrity, and data secrecy.

- **Authentication** – The sending and receiving parties identities are verified
- **Data integrity** – Data is not able to be altered by a 3rd party during the transmission process
- **Data secrecy** – Data is not able to be read by a 3rd party during the transmission process

EVSEs and the networks that will carry the communications (e.g. demand response, price charging, authentication and authorization) between the EVSE, the utility and other connected devices like CEMS, smart meters, etc. must have a secure trusted end-to-end communications path. If the malware/attacks can be propagated from one node to another node (e.g. EVSE), it will be only a matter of time before all the nodes are compromised. Options to secure these interfaces will be encryption and authentication:

- **Encryption** – In cryptography, encryption is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot. Encryption does not itself prevent interference, but denies the intelligible content to a would-be interceptor. In an encryption scheme, the intended information or message, referred to as plaintext, is encrypted using an encryption algorithm – a cipher – generating cipher text that can be read only if decrypted
- **Authentication** – For a positive authentication, elements that could be verified include:
    - **Knowledge factors**: Something the user knows (e.g., a password, partial password, pass phrase, or personal identification number (PIN), challenge response, security question)
    - **Ownership factors**: Something the user has (e.g., wrist band, ID card, security token, implanted device, cell phone with built-in hardware token, software token, or cell phone holding a software token)
    - **Inherence factors**: Something the user is or does (e.g., fingerprint, retinal pattern, DNA sequence, signature, face, voice, unique bio-electric signals, or other biometric identifier).

In effect, trusted communication allows two parties, such as a customer and a store, to use an untrusted medium, such as the Internet, for a specific purpose, such as buying or selling goods, without fear that a third party will manipulate their order (violate data integrity) or steal their financial information (violate data secrecy). Currently, there is no consensus on a trusted communication standard for securing communications between electric vehicles and charging infrastructure. However, there are a number of existing standards and technology for securing end to end communications in use today (see Appendix A). Instead of creating a new standard, existing Internet security standards and best practices can be adapted for use in the EV and EVSE domain.

The Internet, and the range of mature security technologies which support it, is one of the best places to look for existing technologies to adapt to electric vehicle charging networks. One common security concept which the internet relies on is the concept of zero-trust, or that the network itself is untrustworthy. This means that communications over that network are secured in an end-to-end

manner (through encryption and/or authentication), and that the end devices themselves are responsible for authenticating, and ensuring integrity and secrecy of their communications. Some of the standards and technologies that enable this are X.509, which defines the format of public key certificates, a common method of authentication, and Transport Layer Security (TLS) which allows the two endpoints to establish a secured session which ensures data integrity and secrecy. TLS enables protocols, such as HTTP, to be run in a secure manner, such as HTTPS. This robust system for exchanging keys, validating identities, and establishing a secure session is the keystone which supports e-commerce, and can be adapted to the electric vehicle charging ecosystem to enable secure communications between any combinations of stakeholders in the industry. The World Wide Web Consortium (W3C) has expressed interest in adapting web protocols and technology for use in the automotive domain and is a potential partner for this effort. In order to use this technology, industry must adopt a trust anchor or root of trust, upon which the rest of chain of trust is derived.

In cryptographic systems with hierarchical structure, a trust anchor is an authoritative entity for which trust is assumed and not derived. For example in X.509 certificates, a "root certificate" is the trust anchor from which the whole chain of trust, and therefore authentication process, is derived. The trust anchor must be in the possession of the trusting party beforehand to make any further certificate path validation possible. Vehicles and charging infrastructure have unique trust challenges related to their physical properties. Unlike personal computers and servers, which are usually kept behind locked doors, charging stations and automobiles are frequently left unattended in public and need periodic maintenance. These properties make secure storage of trust anchors a significant challenge. Both devices need some form of tamper-proof storage for keys and a method to revoke keys which have been compromised. The Society of Automotive Engineers (SAE) is currently in the process of developing *Standard J3101*: *Requirements for Hardware-Protected Security for Ground Vehicle Applications* which addresses the need for hardware-based trust anchors in the car. It is possible to leverage the trust anchors proposed in this standard to address electric vehicles. The Hybrid Communication and Interoperability Task Force has also published the *Technical Information Report J2931/7*: Security for Plug-In Electric Vehicle Communications. The report establishes the security requirements for digital communication between Plug-In Electric Vehicles (PEV), the Electric Vehicle Supply Equipment (EVSE) and the utility, ESI, Advanced Metering Infrastructure (AMI) and/or Home Area Network (HAN).

5 Ownership and Maintenance

In the EV environment, ownership, maintenance, customization, and repair of hardware and software can be a complex issue. For EVSEs, the multitude of ownership models for charging stations makes it difficult to know who is responsible for physical and software upkeep, especially if the installer, owner, and operator are different entities. For PEVs, repairs can require specially trained personnel due to the high voltages involved in the batteries, and some owners may want to customize the software of their vehicle.

Physical maintenance issues will be relatively easy to detect (e.g. frayed or broken cables, non-functioning displays). The electric current levels associated with EVSE can be harmful if not handled properly, an important consideration for technicians.

Cyber monitoring and anti-tamper hardware, such as an intrusion detection system (IDS) and video surveillance, could be used to detect abnormalities in the operation of the EVSE. When an abnormality has been detected, a software patch needs to be applied. This is often accomplished by remotely applying the patch using a secure over-the-air (OTA) download method. In the event of a catastrophic failure of an EV or EVSE, forensics for analysis requires a means to record the device's data.

Vehicle software updates present another ownership issue. If consumers need to accept or opt into an update, software in the vehicles on the road may not be uniform, even within a certain make and model year, because of time delays in accepting the update. Another issue arises when consumers make modifications to vehicles after they have purchased them. These aftermarket changes to the vehicles may create unique vulnerabilities to those vehicles. While a customer likely voids any warranty with the car manufacturer when this is done, these modified vehicles may not respond the same way to software updates issued by a vehicles manufacturer, leaving identified vulnerabilities in cars. Finally, software issues may be much more difficult to detect, whether the issue is caused by a cyber attack or bug in the vendors update.

6 Coordination

In order to address the unique cybersecurity challenges in electric vehicle cybersecurity, coordination and harmonization among stakeholders is essential. Coordination helps to reduce parallel research efforts, define clear roles and responsibilities for various stakeholder groups, and maximize return on investment for the greater research community. The cross-domain nature of electric vehicle cybersecurity, which bridges two critical infrastructure groups, energy and transportation, places an even greater emphasis on inter-organizational and interdisciplinary approaches to information sharing, research and development activities, standards development, and technology transfer than is seen in other large scale cybersecurity programs.

Coordination efforts can be broken into three major categories: public sector coordination, private sector coordination, and public-private coordination. Public sector coordination involves all stakeholders representing a government entity, including federal agencies, international governments, and state or local governments. Private sector coordination involves stakeholders from the electric and automotive industries, including OEMs, trade associations, and standards bodies. Public-private coordination involves the necessary communication between these two groups.

6.1 Standards Coordination

Standards are the basic building blocks for interconnectivity and interoperability. Even voluntary standards make it easier to develop unambiguous requirements. Without standards (even competing ones) there would be no hope of achieving interoperability within the EV environment. Appendix A contains a brief overview of some of the more technical standards found in the EV environment that address EV and charging infrastructure cybersecurity.

6.2 Public Sector Coordination

Public sector coordination involves stakeholders from all levels of government, from state and local governments, to federal agencies, and to international partners. Each of these public sector organizations have a unique role regarding electric vehicle cybersecurity and the communication and coordination between these organizations is essential.

One of the major challenges in public sector coordination is the lack of a centralized hub for communication between public sector stakeholders, such as: DOE, National Labs, NIST, DOT (i.e. NHTSA, FHWA, FMCSA and the Volpe Center), DHS (Cybersecurity Division), OSTP's National Science and Technology Council (NSTC), and DoD. This lack of coordination results in confusion about stakeholders roles and responsibilities regarding cybersecurity for electric vehicles and the infrastructure on which they depend. Coordination requires dedicated understanding of the complex challenges underpinning electric vehicle cybersecurity and the response effort to those challenges.

It may be beneficial to develop a joint task force across relevant agencies to help support public sector coordination. A coordinating body could help align strategic objectives through:

- Defining, prioritizing, and funding key research gaps in electric vehicle and infrastructure cybersecurity
- Establishing and disseminating industry best practices and standards
- Addressing and defining regulatory and enforcement concerns

6.3 Private Sector Coordination

Private sector coordination involves stakeholders from the electric and automotive industries. Both are mature industries with complex supply chains. Currently, each industry has its own set of industry standards bodies, such as IEEE for electricity and SAE for automotive.

In the automotive domain, original equipment manufacturers (OEMs) integrate components manufactured by Tier 1 suppliers. The OEM then sells the vehicle on the primary market to the primary consumer, which may be an individual or a company with a fleet. After a period of time, the vehicles can be resold on the secondary market, generally to individual consumers. Once a vehicle is sold, there is an entire industry dedicated to aftermarket enhancements, such as up-fits and fleet management technology.

Another challenge in the private sector is that there are a number of nascent businesses which are developing, installing, and maintaining EVSE. Since the EVSE segment of the electric industry is relatively new, they have a limited amount of resources to dedicate to solving EVSE cybersecurity concerns individually. EVSE providers can address this concern by working with existing trade associations, like NEMA, which can leverage resources from its members to establish industry best practices for cybersecurity.

6.4 Public-Private Coordination

Public-private coordination is necessary in order to address electric vehicle and infrastructure cybersecurity concerns both nationally and internationally. Agreeing upon and setting international standards is frequently a time consuming and difficult task. One of the greatest challenges is determining which organizations and government agencies should be a part of the standards making process.

In addition to working together to set standards, government and industry in the automotive and electricity sectors have established their own Information Sharing and Analysis Centers, which are organizations dedicated to sharing and analyzing threat intelligence and vulnerability information with their stakeholders in a timely manner. Below is information on both ISACs:

- **Automotive ISAC**[24] - The Automotive Information Sharing and Analysis Center (Auto-ISAC) is a non-profit information sharing organization that provides a trusted environment and platform for automotive manufacturers and suppliers to collaborate on cybersecurity. Founded by a global group of automakers in 2015, the Auto-ISAC is the central hub for industry-wide sharing of cyber threats, vulnerabilities, and best practices related to the connected vehicle. Members embrace a working together model, engaging across the community with automotive strategic partners, trade associations, researchers and universities, and government. Membership is open to light and heavy-duty automotive manufacturers, suppliers, carriers, and fleet operators.
- **Electricity ISAC**[25] - The E-ISAC establishes situational awareness, incident management, coordination, and communication capabilities within the electricity sector through timely, reliable, and secure information exchange. The E-ISAC, in collaboration with the Department of Energy and the Electricity Subsector Coordinating Council (ESCC), serves as the primary security communications channel for the electricity sector and enhances the sector's ability to prepare for, and respond to cyber and physical threats, vulnerabilities and incidents.

One way to close the communications gap between these industries is to leverage organizations which are common to both industries, such as the ISACs, trade associations, and standards bodies. Formal communications between these entities improve response and coordination during a cyber incident and could also help each industry stay aware of cross-sector threats.

[24] www.automotiveisac.com
[25] www.eisac.com

7 Gaps and Conclusions

7.1 Identified Gaps

One of the goals of the EV and EVSE Cybersecurity Technical Meeting was to identify gaps, challenges, and opportunities in cybersecurity R&D around the interdependencies between the transportation, electricity, and communications sectors. This section of the report contains gaps that were identified during the technical meeting and gleaned from discussions with subject matter experts.

7.1.1 EV Charging Infrastructure Lacks Cybersecurity Best Practices

Hundreds of thousands of electric vehicle charging stations currently exist for public and residential charging. EVSEs are a key element in the EV infrastructure; however, their use in the EV environment presents several unique cybersecurity vulnerabilities. EVSEs, particularly DC fast charging stations, could be used as a potential entry point for malware to spread to other systems, networks, and grid components. Compromised EVs and EVSEs not only present potential public safety concerns similar to other compromised vehicles or utility distribution equipment, but are also potential malware vectors to other systems because of the shared connectivity and mobility of EVs. In many cases, an EVSE is connected to a BEMS, the electric grid, telecommunications networks, and back-end billing systems. Using these connections, EVs and EVSEs could be leveraged to cause electricity load management disruptions for buildings or the grid. Corrupted EVSEs could cause damage not only to the EV that is directly connected but also to other EVSEs on the same network. In addition, EVSE have physical security vulnerabilities that can allow attackers access to interior components.

With thousands of EVSEs in service, acting as not only loads but also potentially as distributed energy resources, quick notification of a compromised EVSE is important. It is currently unknown how many manufacturers provide Intrusion Detection System (IDS)[26] monitoring both for technical and financial intrusion events. After an event, forensic data can be used to determine the method of attack which can provide the basis for designing mitigations. It is currently unknown what post event forensic data, if any, manufactures collect for after-event analysis.

Participants stated that in today's environment, purchasing agents who buy EVSEs do not typically specify cybersecurity protections (e.g. secure OTA firmware update capability, authentication) for their EVSE products due to lack of EVSE cybersecurity guidelines for the EVSE acquisitions. In August 2017, the European Network for Cyber Security (ENCS), Commissioned by ElaadNL developed a document titled *EV Charging Systems Security Requirements* which can be leveraged by the US Energy Sector.[27]

Also, another gap mentioned is the EV industry lacks secure software design and development

[26] An Intrusion Detection System is a device or software application that monitors a network or systems for malicious activity or policy violations.

[27] https://www.elaad.nl/uploads/files/Security_Requirements_Charge_Points_v1.0_april2016.pdf

methodology guidance to design and build “secure” EVSE capabilities.

7.1.2 End-to-end EV and Charging Infrastructure Lacks a Trust Model

The connected infrastructure for electric vehicles goes beyond the electric vehicle and electric vehicle supply equipment. Connections to BEMS, smart metering systems, utility billing, and, ultimately, the grid itself are all a part of the EV environment. In this environment, electric vehicles, the charging infrastructure, and other stakeholder groups exchange information which is critical to maintaining interoperability. This information needs to be exchanged in a secure environment to ensure quality and creditability.

There is no consensus on a trusted communication standard for securing communications between the electric vehicle and the charging infrastructure. In the future it is likely that legacy equipment updates and interoperability will also be a concern.

7.1.3 EV/Charging Infrastructure Lacks Cybersecurity Testing

Penetration testing is an important aspect of cybersecurity for any device in development. Today, there is a lack of formal cybersecurity penetration testing and assessment applied to the entire EV environment. Existing EV/EVSE penetration testing has been piecemeal and not necessarily thorough. This lack of formality makes it difficult to design a functional reference security architecture as there is no clear picture of the EV and charging infrastructure’s vulnerabilities.

Participants discussed a number of areas in the EV environment which could benefit from additional and more robust penetration testing between:

- The EV and EVSE
- The EVSE and EVSE networks
- The EVSE and BEMs
- The EVSE and electric utility

Participants stressed that in today’s environment, EVSE and connected networks could be utilized to propagate malware/attacks from one node to another node, leading to potential impacts on grid operations. In addition, participants discussed the possibility that persistent malware could be utilized to increase the duration of the grid disruption. The attacker could take advantage of:

- The inadequate integrity protections for code in the protocol translation module
- The absence of cybersecurity monitoring tools to detect the malicious activity

7.1.4 Wireless Chargers Lack Common Cybersecurity Guidelines

While industry works to develop new types of charging for electric buses, electric trucks, and light passenger EVs, there is no clear guidance on the unique cybersecurity requirements for wireless power transfer (WPT) charging systems specifically.

WPT charging systems utilize an electromagnetic field to transfer energy via electromagnetic induction. A typical wireless charging system consists of a fixed unit, which supplies an alternating electrical field to a fixed induction coil. On-board the vehicle, a second induction coil receives the power from the electrometric field which is converted back into electric current and used to charge the electric vehicle's battery pack. To charge efficiently, the vehicle coil needs to be positioned over the fixed coil within a tolerance of a few inches in the X and Y directions and several inches in the Z direction. To maintain the convenience that wireless charging offers, all communication between the EV and EVSE occurs over-the-air.

WPT charging systems face the same issues as traditional wired charging systems, but because a physical wired connection is not available in a WPT charging system, unique issues need to be considered such as:

- Additional remote attack vector to the EV where a malicious actor could potentially compromise the safety, privacy, or operation of not only charging, but other vehicle functions without physically interacting with the EV.
- Similarly, additional remote attack vector to the EVSE where a malicious actor could compromise the safety, privacy, or operation of not only charging, but other infrastructure functions without physically interacting with the EVSE.
- The physical and cyber security mitigations used for a traditional, wired charging system need to be redesigned because the same threat model does not apply. Two-way communication between the EV and EVSE is exposed to eavesdroppers and vulnerable to denial of service, message injection, and Man-in-the-middle (MITM) over the air. It is harder to detect a remote attack due to lack of physical evidence (e.g. surveillance cameras can be avoided and equipment does not need to be damaged/modified). Critical remote software updates can be sent over the air via the two-way communication either from the EV to the EVSE or from the EVSE to the EV depending on the implementation and deployment needs.
- Different attacker goals including influencing the positional information of the vehicle, dangerously enabling energy transfer when a vehicle isn't present or when a human is between the vehicle and the fixed coil, and eavesdropping on vehicle charge status or payment information need to be considered.

7.1.5 Security of EV Over-the-Air (OTA) Infrastructure Update Capability

EVs and EVSEs have external connectivity, such as:

- Wi-Fi technology to allow for remote power monitoring and control of the charging state of the connected vehicle
- Gateway cellular modems and cell phone applications
- Over-the-air (OTA) firmware update capability,
- Building Energy Management Systems BEMS interfaces

Today's EV infrastructure (i.e. EVSEs, Smart Meters, Advanced Metering Infrastructure-AMI, Demand Energy Response equipment, etc.) currently has or will have OTA firmware and software update (such as

remote flash capabilities) to quickly distribute software changes and security patches.[28] OTA in the context of the EV infrastructure includes distributing new software/firmware, configuration settings, and updating encryption keys. The OTA technology generally is immature and vulnerable to cyber attacks. For example, many of the major IT companies in the world, like Microsoft, Adobe, and Apache have had their OTA repositories attacked.

Participants were uncertain about how secure the update methods for EVSE are and suggested that research is needed to address potential OTA update insecurities. The following are potential vulnerabilities that participants discussed:

- Man-in-the-middle (MITM) attacks outside or inside the EVSE
- Manipulations of EVSE configuration and firmware updates via USB ports. Since this update mechanism is frequently insecure, arbitrary code could be inserted into the EVSE. By this method, an attacker for example can make charging free for all or can steal customers' card numbers to make charges at their cost
- Compromised keys used to sign updates or servers that store these keys
- For EVSEs with OTA upgrade capability for downloading software files, an attacker could make the EVSE download malicious software files
- Attackers could target the EVSE to achieve one or more of the following goals:
    - *Read updates*: Attackers aim to learn the contents of software updates in order to reverse-engineer the EVSE firmware and/or steal intellectual property
    - *Deny functionality*: Attackers try to stop the EVSE from functioning correctly, thus causing the EVSE to fail abnormally, either temporarily or permanently
    - *Control*: Attackers try to modify the EVSE performance and functionality
- Physical access, such as an attacker manually tampering with the EVSE (e.g. ports)
- Firmware updates not digitally signed or encrypted
- Weak or no authentication (e.g. default credentials), authorization or encryption for firmware updates and use of insecure internet protocols

Insecure, legacy equipment will need to be addressed at the same time as new EV equipment is designed to have better and secure OTA capabilities.

There are secure OTA frameworks the sector could investigate or utilize. For example:

- Internet Engineering Task Force (IETF) develops and promotes voluntary Internet standards, in particular the standards that comprise the Internet protocol suite (TCP/IP).[29]
- Uptane is a compromise-resilient software update security system for the automotive industry that was funded by DHS Science and Technology (S&T) Cybersecurity Division (CSD) developed by New York University's Tandon School of Engineering, the University of Michigan's Transportation Research Institute, and the Southwest Research Institute.[30]

[28] For example, ChargePoint (https://www.chargepoint.com/products/commercial/ct4000/) and Siemens (https://www.downloads.siemens.com/download-center/Download.aspx?pos=download&fct=getasset&id1=BTLV_44824)
[29] https://tools.ietf.org/html/draft-moran-suit-architecture-00
[30] https://ssl.engineering.nyu.edu/papers/kuppusamy_escar_16.pdf

- NEMA Smart Grid Standards Publication SG-AMI 1-2009 - *Requirements for Smart Meter Upgradeability* (December 2016) defines functional and security requirements for the secure Smart Meter/AMI upgrade—both local and remote for industry stakeholders such as regulators, utilities, and vendors.[31]
- NISTIR 7823: Advanced Metering Infrastructure Smart Meter Upgradeability Test Framework (March 2015) describes conformance test requirements that may be used voluntarily by testers and/or test laboratories to determine whether Smart Meters and Upgrade Management Systems conform to the requirements of NEMA SG-AMI 1-2009.[32]

7.1.6 Commercial EVSE Lack of Common Physical Security Guidelines

There are many differing types of EVSEs each having their own unique properties. Commercial EVSEs are public facing devices which have unique physical security challenges. Unlike personal computers and servers, which are usually kept behind locked doors, commercial charging stations are situated in public areas and are frequently left unattended and open to physical damage. Commercial EVSE equipment is often placed in public places with low to zero security. In such instances, there are windows of opportunity for potential attackers to tamper and damage the EVSE equipment physically.

Intentional physical attacks on EVSEs can occur to gain access to the EVSE's electronics to perform a cyber-based attack, to steal components such as cabling which have a high re-sale value, or to vandalize the equipment.

In addition to intentional attacks, unintentional physical damage to EVSEs can be caused by vehicles striking the EVSE, charging cabling being cut or torn out, and miscellaneous damage to user interfaces located on the EVSE such as displays and payment systems.

Physical damage to commercial EVSEs can result in non-operational units which could have an adverse effect on consumer confidence in EVs in general. Some types of physical damage whether intentional or not, may expose the public to harmful electric current levels.

7.2 Conclusions and Critical Gaps

The EV and charging infrastructure cybersecurity environment is a complex mix of many sectors and stakeholders. The joint DOE/DHS/DOT-Volpe Center EV and Charging Infrastructure Cybersecurity Technical Meeting was a first of its kind to bring together these disparate entities. Through presentations, breakout sessions, and general discussions, participants were able to discuss the issues at hand, identify gaps within the industry, talk about possible solutions, and establish connections between all the different stakeholders in attendance.
As these gaps identified in Section 7.1 illustrate, there are multiple challenges to securing the EV

[31] https://www.nema.org/Standards/Pages/Requirements-for-Smart-Meter-Upgradeability.aspx#download
[32] http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.7823.pdf

environment. Throughout the technical meeting, participants particularly focused on two of these gaps as critical for DOE and private industry to address:

1. The lack of security and security best practices for EVSE charging infrastructure
2. The lack of an end-to-end trust model for validating communications

There areas are critical because they have potential implications for the entire EV environment. Addressing these critical gaps should help focus and frame coordination between the relevant stakeholders in the energy, transportation and communication sectors.

Security analysis of this large and complex problem is necessary and requires coordinated and collaborative research across the different systems impacted by EVs and EVSE. Several federal agencies and offices (including DOE, DHS, and DOT) and industry are pursuing R&D in this space, with potential for further collaboration with each other and other entities. As transportation, telecommunications, and electricity system become more interconnected and interdependent, it is necessary to take a comprehensive look at the threat space and vulnerabilities and coordinate various efforts to reduce technical and policy gaps and ensure the effectiveness of existing programs.

Appendix A - Electric Vehicle Technical Standards Overview

There are many standards to be found in the EV environment such as those that apply to EVSEs e.g. type of charger (DC or AC), type of charging plug etc. However without standards (even competing ones) there would be no hope of achieving interoperability within the EV environment and the table below contains a brief overview of some of the more technical standards found in the EV environment that could be impacted by EV and charging infrastructure cybersecurity. Standards also make it easier to develop requirements that can be unambiguous.

Standards Body	Standard	Standard Title	Remarks
Deutsches Institut für Normung e.V. (the German Institute for Standardization)- (DIN)	70121:2014-12	Electromobility - Digital communication between a D.C. EV charging station and an electric vehicle for control of D.C. charging in the Combined Charging System	(For DC charging) that has no security but it is communication only from the vehicle to the off-board inverter in the EVSE. This has options for payment and authentication but not widely used.
The Charging Interface Initiative (CharIN e. V.)	Combined Charging System (CCS)1.0	Combined Charging System Specification 1.0	DIN 70121:2014-12 Harmonized with SAE J2847/2
The Charging Interface Initiative (CharIN e. V.)	CCS 2.0	Combined Charging System Specification 2.0 (Mid 2018, introduction)	Retains DIN 70121:2014-12 but adds ISO 15118 ED 1. Has security but is optional.
The Charging Interface Initiative (CharIN e. V.)	CCS 3.0 (Under Development)	Combined Charging System Specification 3.0	Under development to include existing SAE and ISO standards plus updating for more Wireless Power Transfer (WPT) features such as adding more control and communication for vehicles approaching the ground assembly (starting from 10-50 meters out) than currently exist.

			Security will be required (not optional).
Society of Automotive Engineers (SAE)	J2847/2	Communications between Plug-In Vehicles and Off-Board DC Chargers	Establishes requirements and specifications for communication between Plug-in Electric Vehicle (PEV) and the DC Off-board charger.
Society of Automotive Engineers (SAE)	J2931/7	Security for Plug-In Electrical Vehicle Communications	Establishes the security requirements for digital communication between Plug-In Electric Vehicles (PEV), the Electric Vehicle Supply Equipment (EVSE) and the utility, ESI, Advanced Metering Infrastructure (AMI) and/or Home Area Network (HAN).
Society of Automotive Engineers (SAE)	J2836	Use Cases for Communication Between Plug-in Vehicles and the Utility Grid	Establishes use cases for communication between plug-in electric vehicles and the electric power grid, for energy transfer and other applications.
International Organization for Standardization (ISO)	15118 (ED 2 expected end of 2018)	Road vehicles-Vehicle to grid communications Interface	Specifies the communication between Electric Vehicles (EV), including Battery Electric Vehicles and Plug-In Hybrid Electric Vehicles, and the Electric Vehicle Supply Equipment (EVSE).
IEEE	2030.5 (formally SEP 2.0)	Adoption of Smart Energy Profile 2.0	Defines the mechanisms for exchanging application messages, the exact messages exchanged

			including error messages, and the security features used to protect the application messages.
Underwriters Laboratories	UL2202	Standard for Electric Vehicle (EV) Charging System Equipment	Conductive charging system equipment intended to be supplied by a branch circuit of 600 volts or less for recharging the storage batteries in over-the-road electric vehicles (EV). The equipment includes off board and on board chargers
Underwriters Laboratories	UL2231	Standard for Personnel Protection Systems for Electric Vehicle (EV) Supply Circuits	Requirements cover conductive charging system equipment intended to be supplied by a branch circuit of 600 volts or less for recharging the storage batteries in over-the-road electric vehicles (EV). The equipment includes off board and on board chargers
Underwriters Laboratories	UL2251	Standard for Plugs, Receptacles and Couplers for Electric Vehicles	Requirements cover EV plugs, EV receptacles, vehicle inlets, vehicle connectors, and EV breakaway couplings, rated up to 800 amperes and up to 600 volts ac or dc. These devices are intended for use with conductive electric vehicle supply equipment (EVSE), and are intended to facilitate the

			conductive connection from the EVSE to the vehicle.
Underwriters Laboratories	UL2271	Batteries for use in Light Electric Vehicle (LEV) Applications	Requirements cover electrical energy storage assemblies (EESAs) such as battery packs and combination battery pack-electrochemical capacitor assemblies and the subassembly/modules that make up these assemblies for use in light electric-powered vehicles (LEVs) as defined in this standard.
Underwriters Laboratories	UL2594	Electric Vehicle Supply Equipment	Conductive electric vehicle (EV) supply equipment with a primary source voltage of 600 V ac or less, with a frequency of 50 or 60 Hz, and intended to provide ac power to an electric vehicle with an on-board charging unit.
Open Automated Demand Response (ADR) Alliance	Open ADR 2.0	Open ADR 2.0	OpenADR 2.0a and b Profile Specifications provide specific implementation related information in order to build an OpenADR enabled device or system.
Open Charge Alliance (OCA)	OSCP 1.0	Open Smart Charging Protocol	Protocol between charge point management system and energy management system of the site owner or the

			Distribution System Operator's (DSO) system.
North American Electric Reliability Corporation (NERC)	CIP-002-51.a	Cybersecurity-Bulk Electrical System Categorization	Identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to mis-operation or instability in the BES.
North American Electric Reliability Corporation (NERC)	CIP-005-5	Cybersecurity-Electronic Security Perimeter(s)	Manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to mis-operation or instability in the BES.
NIST	7628	Guidelines for Smart Grid Cybersecurity	Analytical framework that organizations can use to develop effective cyber security strategies tailored to their particular combinations of Smart Grid-related

			characteristics, risks, and vulnerabilities.
NIST	Handbook 44-Section 3.40	Electric Vehicle Fueling Systems (Tentative Code)	Code applies to devices, accessories, and systems used for the measurement of electricity dispensed in vehicle fuel applications wherein a quantity determination or statement of measure is used wholly or partially as a basis for sale or upon which a charge for service is based.
NIST	Handbook 44-Section 5.55	Timing Devices	This code applies to devices used to measure time during which services are being dispensed This code also applies to Electric Vehicle Supply Equipment (EVSE) when used to assess charges for time-based services in addition to those charged for electrical energy.

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).

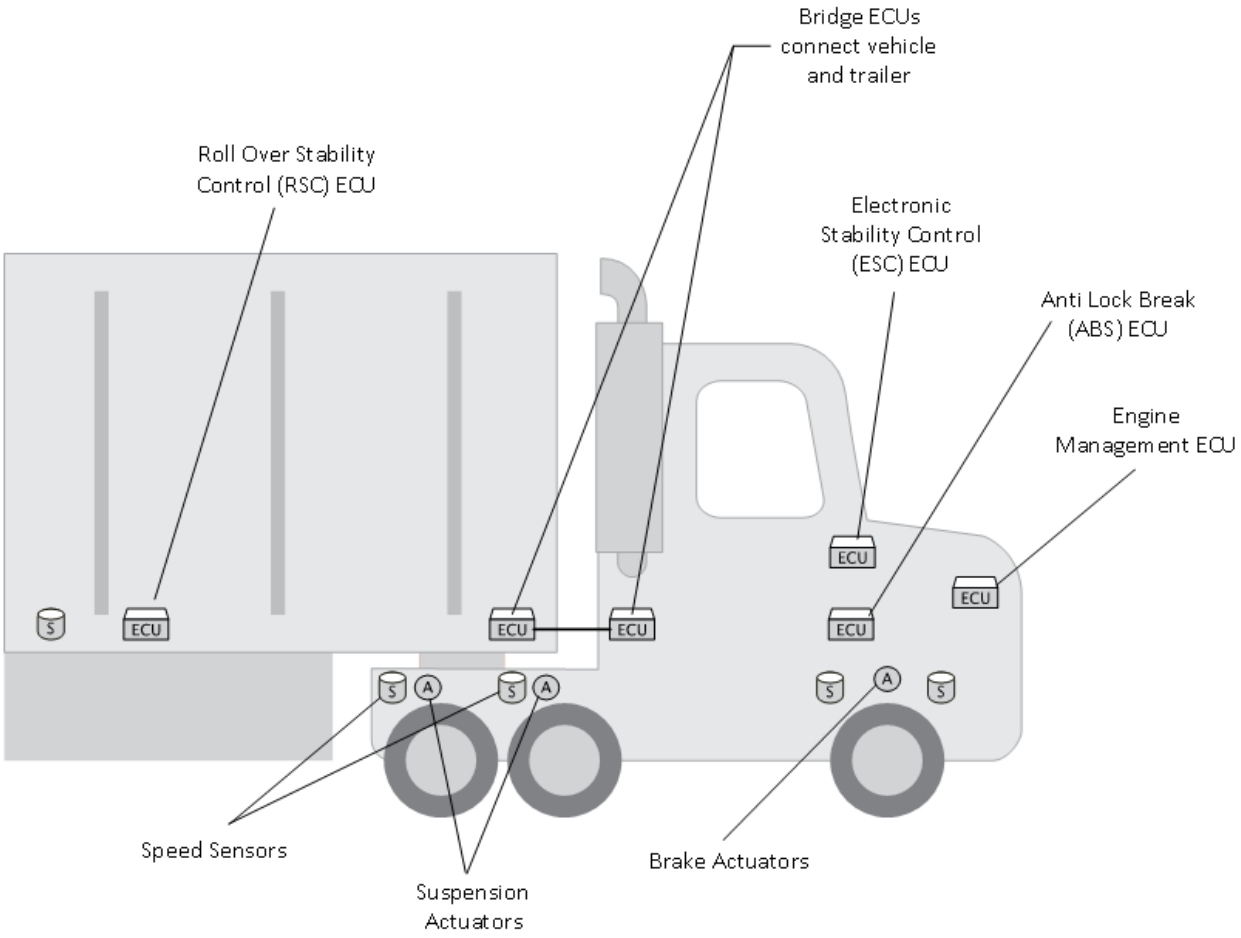
OBD standards progressed slowly until the OBD-II California Air Resources Board (CARB) standard was mandated in 1994 for all model year (MY) 1996 vehicles to be sold in California. The EPA extended the OBD-II requirement to *all* MY 1996 cars sold in the United States. European regulators would adopt 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.

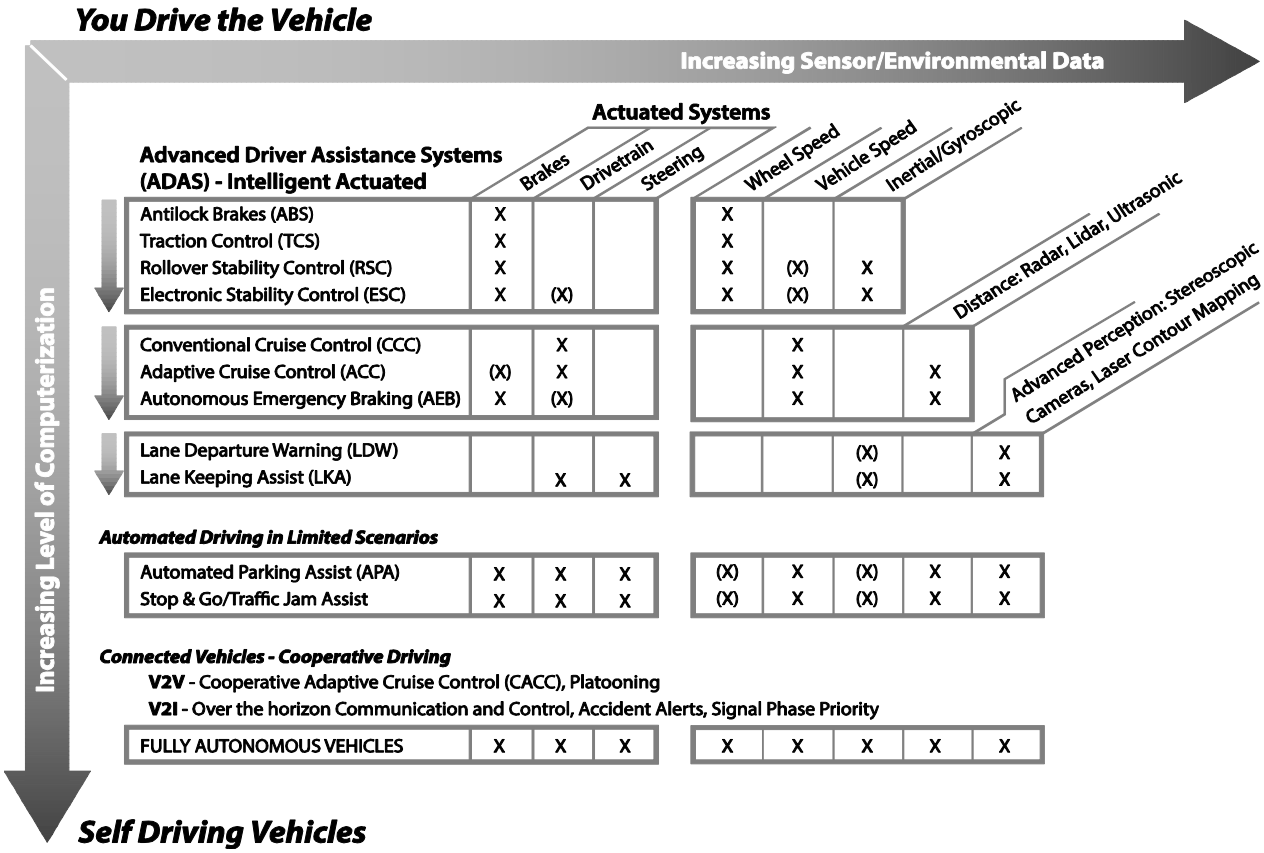
Examples of Vehicle to Vehicle (V2V) communication systems include Forward Collision Warning (FCW), Lane Change Warning (LCW), and Curve Speed Warning (CSW). These are extensions of existing features already in the automobile market such as automatic emergency braking and adaptive cruise control. In 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.