Medium and Heavy Duty Electric Vehicle and Charging Infrastructure Cyber Security Executive Summary

May 21, 2018

Motor freight transportation is a critical industry that keeps many other industries and modern conveniences of life working. The effects and risks of compromise of the motor freight industry at a large scale can cause widespread systemic and societal issues. It is therefore important for us all to consider the security of the motor freight transportation industry seriously when contemplating the electrification of heavy vehicles. The combination of power grids and transportation industry through the use of electric trucks creates a nexus of mission critical systems and services whose disruption can have significant impacts on national security.

Cyber Security Challenges for the Medium and Heavy Duty Electric Vehicle

According to a recent report by Lisa Jerram, a principal research analyst for Navigant Research, the number of hybrid-electric and electric trucks is set to grow almost 25% annually, from 1% of the market in 2017 to 7% in 2027, a jump from about 40,000 electric trucks worldwide this year to 371,000. Others have concerns as well.

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."*

Unlike their traditional fossil fuel counterparts, when Medium Duty/Heavy Duty Electric Vehicles (MD/HDEV) "refuel," they are both physically and electronically connected to, and exchange information with, Electric Vehicle Supply Equipment (EVSE), which is also connected to the electrical utility Smart Grid and local energy management systems. This communication nexus presents "unique" challenges for the MD/HDEV in regards to cyber security, such as:

- **MITM (Man In the Middle) attack at charging station** - Attacker inserts themselves between the MD/HDEV and the EVSE leading to information theft and authorized system access
- **Money from credit card 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
    - 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** taking the MD/HDEV out of service/degrading range
- **Denial of Service (DoS) attack at EVSEs** - Taking vehicles out of service if unable to re-charge

1001 North Fairfax Street, Suite 600 ♦ Alexandria, VA 22314-1798 ♦ ph: 703.838.1810 ♦ fax: 703.683.6296
web: www.nmfta.org ♦ email: customerservice@nmfta.org

- **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

Identifying the Key Cyber Security Issues

Recognizing the unique challenges of cyber security for electric vehicles, 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. Several key issues were identified during the meeting:

- Lack of a practical baseline document to educate all of the disparate EV stakeholders and interested parties on each other's domains and cyber security issues and concerns
- Lack of representation from the heavy vehicle industry that has different use cases and concerns for electric vehicles especially Class 7 and 8 trucks
- A need to explore current and future research for cyber security principles, risks/threats, and best practices for MD/HDEV and charging stations

Recommended Actions

There are a number of actions, activities, and projects that stakeholders can take to close gaps, reduce risks and, in general, improve their cyber security posture. 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 networks; many of these same principles can also be applied to vehicles.[1] We also recommend the development of incident response plans. Planning before an event takes place helps ensure you know how you can recover and is critical to surviving a breach or attack. More recommendations and information sources are provided in the full document.

Immediate identified 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.
- An inventory of existing capable and near capable research facilities are needed that can be upgraded to allow for further research and development.

[1] Center for Internet Security, *Powerful Best Practices*, CISsecurity.org, (n.d.). https://learn.cisecurity.org/20-controls-download

- Cyber security best practices need to be developed for MD/HDEV OEMs, EVSE vendors, and fleet operators.
- Additional research into maintenance and operations of heavy vehicles needs to be conducted to allow carriers to get more operational data on MD/HDEVs to make more informed decisions regarding electrification.

Working together with DOT/Volpe and other stakeholders, we also developed some specific recommendations for a few initial research and pilot projects. The table below contains a summary listing.

Project Title	Project Goals
xFC/DC Chargers Cyber Security Threat and Risk Assessment	Develop and validate techniques and technologies that provide cyber resilience to Extreme Fast Charging (xFC) units with power transfer rates of 300kW and above, as well as other vehicle chargers
Secure EVSE Over-the-Air (OTA) Firmware Update Pilot	EVSEs have or will have Over-the-Air (OTA) firmware update and remote flash capabilities and OTA update capability is typically insecure. 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.
Development of MD and HD Charging Station Intrusion Detection System (based on INL's Diagnostic Security Modules (DSMs) Program)	In the event of a cyber-incident involving a MD or HD 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 in real-time and prevent hacking attempts. INL has an on-going IDS EVSE Project called "Diagnostic Security Module" (DSM) that can be leveraged/tailored to meet this gap for Heavy Truck Chargers.
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 and HD Chargers can be used as a potential entry point for malware to spread to Building Energy Management Systems (BEMS), Power Grid, telecommunications networks, and billing systems. This project will determine the state of cyber security mitigations of current and future MD and HD Chargers. Based on the findings, Cyber Security Best Practices for MD/HDEV Chargers document will be developed.

Incident Response	Develop an incident response plan that is specific to the MD/HDEV environment and 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.
Cyber Security Design Best-Practices for MD/HDEV Wireless Charging Systems	Develop a 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.

Conclusion

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.