Pacific Northwest
NATIONAL LABORATORY

PNNL-34280

A Threat Model of High-Power Electric Vehicle Charging Infrastructure

March 2022

TE Carroll
GB Dindelbeck
RM Pratt
LR O’Neil

U.S. DEPARTMENT OF
ENERGY

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor Battelle Memorial Institute, 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, or Battelle Memorial Institute. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

**Available to DOE and DOE contractors from
the Office of Scientific and Technical
Information,
P.O. Box 62, Oak Ridge, TN 37831-0062**
www.osti.gov
**ph: (865) 576-8401
fox: (865) 576-5728
email: reports@osti.gov**

**Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
or (703) 605-6000
email: info@ntis.gov
Online ordering: http://www.ntis.gov**

PNNL-34280

A Threat Model of High-Power Electric Vehicle Charging Infrastructure

March 2022

TE Carroll
GB Dindelbeck
RM Pratt
LR O’Neil

Prepared for
the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99354

Abstract

While electric vehicle powertrains have inherent efficiencies over their conventional counterparts, recharge time remains a significant concern. High-power charging (HPC) alleviates the concerns by delivering greater power to speed charging. HPC requires communication among the vehicle, charging infrastructure, and electric supply to facilitate charging. Consequently, the transformation extends the reach and heightens the risks posed by cyberattacks, as an incident may threaten both the power grid and transportation systems. In this paper, a novel consequence-centric methodology is used to formulate an HPC infrastructure threat model. By linking threats to electricity and transportation impacts, broad understanding of consequences is acquired.

A Threat Model of High-Power Electric Vehicle Charging Infrastructure

Abstract: *While electric vehicle powertrains have inherent efficiencies over their conventional counterparts, recharge time remains a significant concern. High power charging (HPC) alleviates the concerns by delivering greater power to speed charging. HPC requires communication among the vehicle, charging infrastructure, and electric supply to facilitate charging. Consequently, the transformation extends the reach and heightens the risks posed by cyberattacks, as an incident may threaten both the power grid and transportation systems. In this paper, a novel consequence-centric methodology is used to formulate a HPC infrastructure threat model. By linking threats to electricity and transportation impacts, a broad understanding of consequences is acquired.*

Keywords: *Electric Vehicle, Electric Vehicle Charging, Security*

Introduction

Advancements in electric vehicle (EV) technologies are rapidly accelerating the electrification of transportation systems; however, the time required to recharge remains a legitimate concern among EV operators as it presently takes longer than refuelling conventional internal combustion engine vehicles. In an effort by EV manufacturers to achieve competitive parity and accelerate EV adoption, a high priority has been placed on rapidly charging EVs. High power charging (HPC) significantly narrows the time difference between refuelling conventional vehicles and recharging EVs. Moreover, HPC accommodates the charging of large-capacity battery packs that are integral to the electrification and adoption of medium- and heavy-duty trucks, buses, and regional jets. HPC electric vehicle supply equipment (EVSE) provides variable direct current (DC) power to the EV and the EV commands the EVSE to provide the appropriate power levels to satisfy the battery charging constraints. Unlike lower power charging (and proportionally slower charging times) which employs a simple pulse-width modulated signal to sequence the charging process, HPC charge control uses high-level communication built on digital communications and Internet Protocol v6 networking. High-level communication among vehicles, charging infrastructure, and the power grid underlie managed charging and grid services (e.g. smart charging and ancillary services) information and decision exchanges that mitigate adverse charging-at-scale effects and contribute to the stable operation of power grids (Kintner-Meyer, Schneider and Pratt 2007). Economy-wide transportation system electrification will significantly increase electricity demand and create strong and substantial interdependence between the historically disparate electric supply and transportation systems. The transformation will extend the reach and heighten the risks posed by cyberattacks as an event may bring wide-ranging consequences to vehicles, electric supply, and transportation systems.

Security must not be an afterthought as large-scale HPC may impart deleterious effects and reduce the resiliency of the electric supply and transportation systems. In preparation for the eventual large-scale deployment, the security implications and ramifications of HPC should be investigated. As HPC remains in development and has yet to be fielded in large numbers, there exists an opportunity to influence standards, architectures, and designs so that HPC is built on a secure foundation, assuring confidence in HPC to safely and securely dispense power. To this end, the authors develop and analyse a threat model of high-power electric vehicle charging infrastructure in this paper. Threat modelling is the systematic process to identify weaknesses, such as structural vulnerabilities and the absence of appropriate security safeguards. The first step of threat modelling is creating a system model over which threats are derived. A system model characterises the system under study and describes the components, processes, and functions, and the interrelationships among them. The system model design was informed by ISO 15118, an open-communication standard that governs the vehicle-to-grid communication interface. The STRIDE threat modelling methodology was initially applied to systematically analyse the models for structural vulnerabilities. The authors' early attempts proved unsatisfactory, as consequences to the electric supply or transportation system went undiscovered. The modified methodology discussed in this paper establishes ties that assist in identifying threats to these sectors.

Related Work

The models proposed in this paper build on existing work that has analysed vehicle charging infrastructure security. These works are important as security incidents of charging infrastructure may impair the safe, reliable, and efficient operation of the power grid (Ahmed and Dow 2016). The arrival of HPC and related need for managed charging requires vehicle charging infrastructure security (Pratt and Carroll 2019). Harnett *et al.* (2018) identified deficiencies in charging station cybersecurity. Falk and Fries (2012) developed charging infrastructure use cases and showed how various charging standards securely address them. In subsequent work (2013), they enumerated basic requirements to securely operate charging infrastructure. Gottumukkala *et al.* (2019) characterised attack types that can be used to compromise chargers. Lee *et al.* (2014) developed ISO 15118-specific uses cases and then demonstrated weaknesses in how the standard addresses them. Bao *et al.* (2018) studied ISO 15118, but took a distinct approach and developed profiles of the adversary before identifying ISO 15118 weaknesses. Hodge *et al.* (2019) developed a generalised model of charging infrastructure and then identified risks and countermeasures.

While existing work informed the decomposition of charging infrastructure into constitute components and attack-surface measurements, the threat models presented in this paper are distinguished by the work to systematically analyse charging infrastructure to identify vulnerabilities and understand how the vulnerabilities impact electric supply and electrified transportation systems. Also unique to the handling of the problem is the consideration of scale. Previous work chiefly examined the security of a single charging installation; here, the security ramifications of numerous installations are considered.

Contribution

A threat model of HPC infrastructure is built and systemically examined for threats that have potential electric supply or transportation system effects. A novel consequence-centric variant of STRIDE threat modelling methodology is derived to: (i) discover adverse consequences related to electricity, transportation, or both; and (ii) focus subsequent modelling and analysis on threats that may precipitate the consequences.

By focusing on consequences, we gain insights into the security and resiliency of the EV charging ecosystem. Importantly, the threat model analysis suggests that no single entity is ideally situated to secure the ecosystem, but instead requires the concerted effort of the ecosystem to promote and protect vehicles, infrastructure, and systems.

Organisation

The remainder of the paper is structured as follows. First, EV charging is briefly reviewed. The threat modelling methodology is then discussed, followed by the modelling and analysis of HPC infrastructure. The paper is concluded with a discussion of the analysis and identifies future work.

Vehicle Charging Primer

EV charging is briefly reviewed in this section. One of the basic components of the charging infrastructure is the EVSE, the device that delivers energy to the EV. The terms “charger” and EVSE are used interchangeably in this paper. While wireless charging technologies exist, the context of this section is constructed around *conductive* charging, which uses plugs, sockets, and cabling to transfer electrical energy. Chargers are classified by the type and amount of power they transfer to the EV. Higher power delivery translates into faster charging times and, when accompanied by high-capacity batteries, reduces charging frequency, which assists long-range travel and alleviates “range anxiety,” the fear that the vehicle will be stranded without charging means (Meintz *et al.* 2017). SAE J1772 (2017), a North American standard that specifies requirements for the conductive charge system and couplers, defines two levels of alternating current (AC) charging and two levels of DC charging, where the level is indicative of charging rate. Typical AC Level 1 and Level 2 EVSEs supply fixed-voltage AC power at charge rates up to 1.9 kW and 19.2 kW, respectively. In comparison, DC Level 2 speeds charging by transferring variable DC power at a maximum of 400 kW. HPC is a subjective term; the authors arbitrarily define it as DC charging delivering more than 200 kW and is inclusive of DC fast charging with rates in the range 50 kW to 250 kW, Extreme Fast Charging with charging rates up to 400 kW, and the Megawatt Charging System with rates exceeding 1 MW.

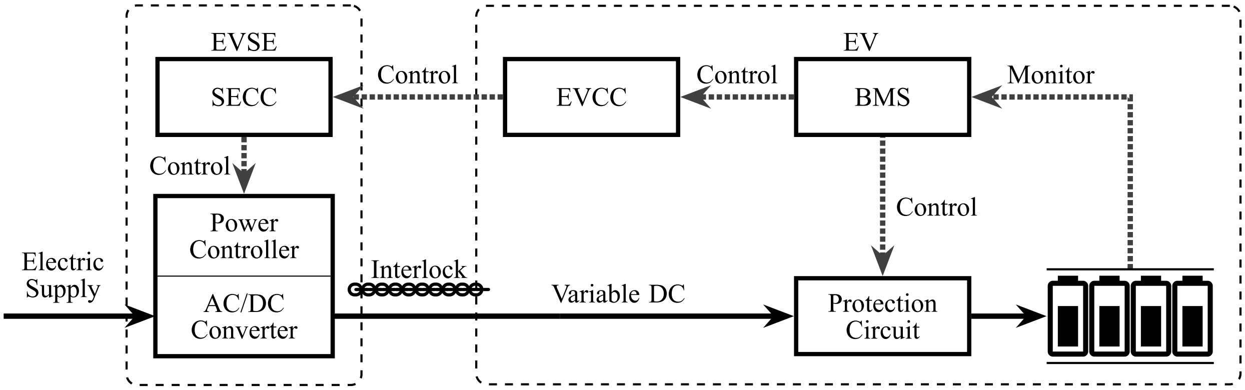

Figure 1: Logical components associated with DC charging.

Figure 1 depicts a typical DC Level 2 charger. In this configuration, the charger supplies variable-voltage DC power to the vehicle. The battery management system (BMS) monitors the battery pack, protects the battery pack from operating outside the safe operating area, controls charging state and rate by commanding the power controller, manages thermal conditions when appropriate, and calculates ancillary data such as state of health and state of charge. The supply equipment communication controller (SECC) and electric vehicle communication controller (EVCC) exchange charging sequencing and management information. The protection circuit disrupts the flow of power when overcurrent, overvoltage, electric short, and other deleterious electrical or thermal conditions are encountered. Finally, the interlock de-energises the cable and connector if the charger and EV are uncoupled.

ISO 15118, J1772, GB/T, and Tesla are competing standards governing charging plugs, connectors, and protocols. The threat models constructed in this paper assume ISO 15118, an international standard that allows EVs to automatically identify the user, authorise payment, and begin charging. Although the focus of this paper is on ISO 15118, the models and results are sufficiently general to be applicable to the other charging standards and systems. ISO 15118 uses two types of communication between EV and EVSE for charge control. The first type, basic signalling, is a simple analog pulse-width modulated signal that is used to express basic state (e.g. vehicle connected and ready to accept energy, EVSE ready to supply energy). The second type is digital high-level communication. High-level communication is used to exchange more complex information than what is possible with basic signalling. ISO 15118 adopted HomePlug GreenPHY power-line communication and Internet Protocol v6 networking for the high-level communication foundation. The high-frequency power-line communication carrier is on top of the pulse-width modulated signal, using the same control pilot wire that transfers the basic signal. The EVCC configures its network addresses once digital communications are established. A simple multicast-based network discovery protocol is used to identify the SECC. The EVCC opens a transmission control protocol connection to the SECC using the address and port provided in the discovery response. Depending on the charging authorisation scheme, Transmission Layer Security (TLS) may be required to authenticate the EVSE and ensure communication security (TLS is mandatory in the next major revision of ISO 15118 (Mültin 2021)). Once connected, the EVCC and SECC exchange XML-based messages.

The EV charging market participants are identified by roles. The roles relevant to the exercise are charging station operator (CSO), charging network operator (CNO), and distribution system operator (DSO). The CSO operates and maintains the EVSE and related infrastructure. The CNO is responsible for contracting, authentication, authorisation, and billing. The DSO is responsible for the safe, stable, and reliable operation of a regional electric grid. The DSO coordinates with the CNOs and CSOs to manage electric system capacity and constraints. The threat models presented later in this paper document the CSO but not the CNO. This is done for two reasons. First, the U.S. market is dominated by vertically integrated corporations performing both the CSO and CNO roles. Second, the charging equipment and infrastructure are the focus.

Methodology

Threat modelling is an industry-recognised approach to enumerate and characterise potential threats and vulnerabilities that, absent the appropriate safeguards, may lead to a security incident or compromise. Subsequent analysis of the threat model guides and informs countermeasures and prioritises mitigations to prevent or reduce the impact of incidents.

Numerous threat modelling methodologies exist. Approaches can be generally categorised by focus. Bao *et al.* (2018) employs an adversary-centric approach, profiling the adversary by identifying types, capabilities, and motivations. Other work (Lee *et al.* 2014) focuses on use cases and how the relevant standards address them. In this paper, a component-centric approach based on STRIDE was applied. STRIDE is a mature approach to threat modelling invented by Kohnfelder and Garg (1999) while at Microsoft to identify computer security threats. Other researchers (Khan *et al.* 2017; Shevchenko 2018) have successfully applied STRIDE to the threat modelling of cyber-physical systems.

STRIDE considers six categories of security threats Shostack (2014): (i) Spoofing: masquerading as a legitimate user, process, or system element; (ii) Tampering: modification/editing of legitimate information; (iii) Repudiation: denying or disowning a certain action executed in the system; (iv) Information disclosure: data breach or unauthorised access to protected information; (v) Denial of service: disruption of service for legitimate users; and (vi) Elevation of privilege: gaining higher privilege access to a system element by a user with restricted authority.

One begins STRIDE by identifying and modelling the in-place system along with appropriate system boundaries. The system is then decomposed into its constituent components. A flow diagram is then constructed, dividing components into functional blocks and then illustrating the exchange or "flow" of information between the blocks. The vehicle charging infrastructure is a cyber-physical system, demanding more than information exchanges to be considered. Consequently, the system models were amended with electric power flows that illustrated how power moves between the components in the system. The second step is to identify trust boundaries that aid in the reasoning of trust domains and how they may influence one another (Miller 2008). Flows that operate across trust domains deserve special attention as they suggest exposure to untrusted data. The third step is to analyse threats in flow diagrams to help find system threats. For each of the six threat categories, the authors consider how the threat manifests as a security incident and the consequences that may occur. System modelling and threat modelling are iterative, where observations in one model may inform modifications in the other. The threat modelling process is complete once the system is sufficiently expressed.

The authors' initial attempts proved unsatisfactory. They observed that identified consequences were in the context of components and the impacts to electric supply and the transportation sector went unrecognised. Recognising impacts was important to the authors as there was an explicit goal to relate the threat model to ongoing work modelling large-scale HPC charging and its effects on electric distribution and transmission grids, bulk electricity generation, and the transportation sector. The issue was that the consequences were outside the definition of the system model. This quality can also be observed in (Volpe National Transportation Systems Centre 2019, Appendix A), where consequences are bounded by the component presently under exploration. To bridge the gap, the authors inserted steps to explicitly connect threat modelling to the external concerns. First, impacts were identified. Impacts were broad statements, bringing to light downstream effects on electricity or transportation, along with their associated security requirements. The security requirements, listed in no particular order, are to maintain (i) human safety and environment, (ii) availability of the electric supply, (iii) availability of the transportation system, (iv) availability and integrity of vehicles, (v) privacy (confidentiality of personal data), (vi) integrity and nonrepudiation of financial and energy transactions, and lastly (vii) confidentiality of corporate information. When considered as a whole, the security requirements assure people's continued faith in EVs and charging infrastructure, continued adoption of EVs, and the ongoing electrification of transportation mode, for example electrifying aeroplanes, helicopters, and cargo ships.

To inform the threat model, consequences were then linked with impacts and requirements. If a connection could not be established, then the consequence was deemed outside the scope of concern and excluded from the exercise. The flow diagrams were then analysed to identify threats that may precipitate the selected consequences. Threats were analysed to ensure they were subjugated to or facilitated by the infrastructure. If the threat materialised without involving the infrastructure, it was reasoned the conditions to manifest the threat existed at present, and therefore was deemed out of scope for this exercise. Several rounds of impact, consequence, system, and threat modelling were performed. Modelling was subjectively deemed complete once the model's explanatory powers did not further elucidate electricity or transportation impacts.

Threat Model

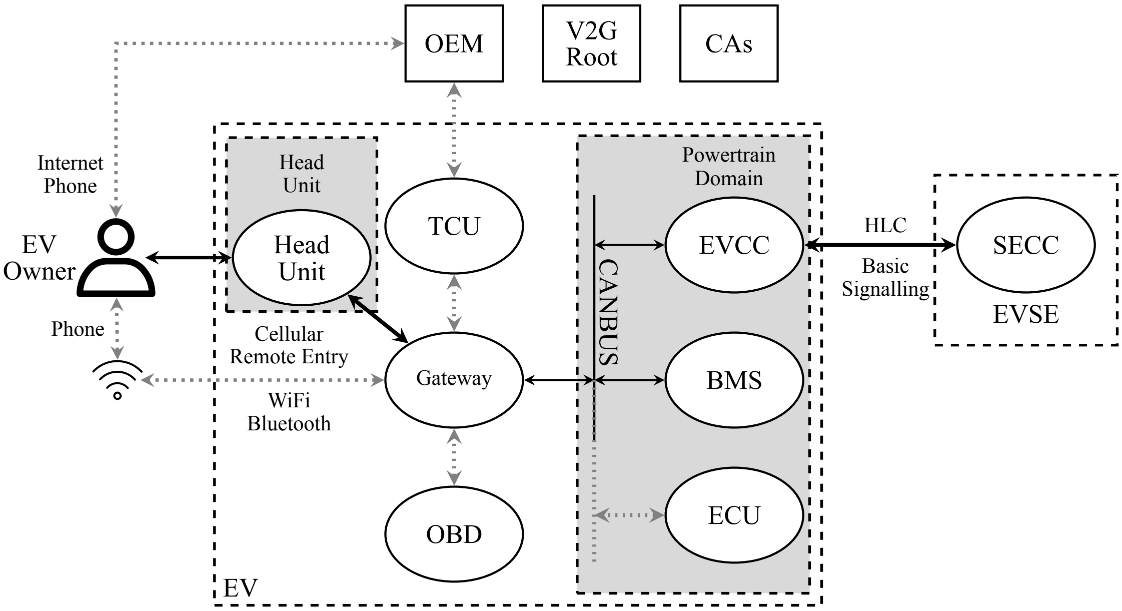

Figure 2: The EV data flow diagram.

This section describes the construction and analysis of the threat models. The section begins by describing the three flow diagrams that comprise the system models. In **Figure 2**, a data flow diagram of an EV is shown. A flow diagram is a graph and represents the system decomposed into a set of elements and the relationships between them. The relationships are induced by data or power flows. The representation is logical, meaning functions can be combined when implemented in the context of controllers. The shapes have meanings: an oval represents a unit of function, a block is an external entity, and two parallel lines represent storage. One may think of a function unit as process, controller, or subsystem. An external entity is a person, organisation, etc. that interacts with, affects the operation of, or is affected by the system. A connection between entities represents flow. The arrow indicates the direction of flow, pointing from source to receiver. Connection labels provide additional context, identifying aspects such as communication protocols, circuit types, and voltages. While data flows can be bidirectional, a power flow will likely be unidirectional. A dashed rectangle indicates a trust boundary; entities in the boundary operate in a trust domain. Attention needs to be given to flows crossing trust boundaries as the data originate from an untrusted source. While all data should be checked, input and data validation are particularly important for handling data from untrusted sources.

In **Figure 2**, the diagram is divided into three broad areas. The lower left presents the EV in detail; the lower right is a coarse representation of the charging station; and the top lists external entities. The dark solid connections are data flows that occur during the charging process. The light dotted connections are data flows that may occur in addition with charging, but are not critical exchanges for the charging itself. The vehicle representation is divided into three trust domains.

The “Powertrain Domain” comprises the power plant, power transfer mechanisms, and electronic control units (ECU in the figure) necessary for the generation and delivery of power to the driving wheels. It is reasonable to assume that the EVCC and BMS will be part of this domain. The EVCC facilitates communication between the EV and charging station SECC. As the reader may recall, the BMS is a controller that monitors and protects the battery packs, controls charging, and calculates important ancillary data critical to the operation of the powertrain. The BMS and batteries likely comprise tens to hundreds of other controllers (Brandl *et al.* 2012), communicating using wired or wireless interfaces (Ulrich 2020). It is reasoned that documenting each controller is unnecessary; therefore, battery management, charge controlling, and related functionality are mapped to the BMS.

Much of the vehicle controller communications occur over controller area network bus, which is a multimaster, message-based, broadcast-type intra-vehicle network designed to allow resource-constrained electronic control units to efficiently communicate in real time. The controller area network bus is open and flexible, but lacks robust security (Hartzell and Stubel 2017). The “Head Unit” comprises a user interface to control audio, navigation, and passenger cabin climate. It typically operates in a trust domain separate from other vehicle controllers. Current vehicles have several interfaces to communicate externally. The on-board diagnostic unit (OBD in the figure) is a diagnostic interface that allows access to vehicle subsystems. Additionally, the telematic control unit (TCU in the figure) sends diagnostics and other related information to the vehicle’s original equipment manufacturer (OEM in the figure). As shown in **Figure 2**, contemporary vehicles are typically equipped with WiFi, Bluetooth, 4G/5G air modems, and other wireless communication interfaces. The interfaces substantially expand the vehicle’s attack surface, allowing external attackers to access and influence its operation (Sommer, Dürrwang and Kriesten 2019). The gateway is responsible for mapping, translating, and routing messages between domains (such as between the powertrain controller area network bus, telematic control unit, and the passenger cabin network). Gateways are integral for secure vehicle communications, performing such functions as intrusion detection and prevention, firewalling, access control, key management, and secure time synchronisation (AUTOSAR 2018).

The *V2G Root* and subordinate certificate authorities (CAs in the figure) are external entities that identify and authenticate parties. Additionally, the certificates identify the market roles of parties. The V2G Root certificate authority is the top-level authority that anchors the chain of trust. The V2G Root issues and digitally signs certificates for subordinate authorities; subordinates then issue certificates for secondary subordinates. The hierarchy establishes a trust relationship from any subordinate to the trusted V2G Root certificate authority. The subordinate serves a role similar to publicly trusted certificate authorities that facilitate secure communications on the internet. The secondary subordinates perform all the necessary administrative functions to issue certificates to end users.

The charging station data flow diagram is presented in **Figure 3**. The diagram can be divided into four regions. The left is the vehicle, the bottom centre is the charging station, the right is the service provider, and the top provides a list of external entities with charging infrastructure responsibilities. The charging station likely comprises multiple controllers. The System is the main charging station controller, providing the overall functionality of the charging station. The Power module controls and monitors the AC-to-DC conversion power electronics and protection circuits. The SECC is the charging station ISO 15118 communication endpoint. High power transfers will generate large

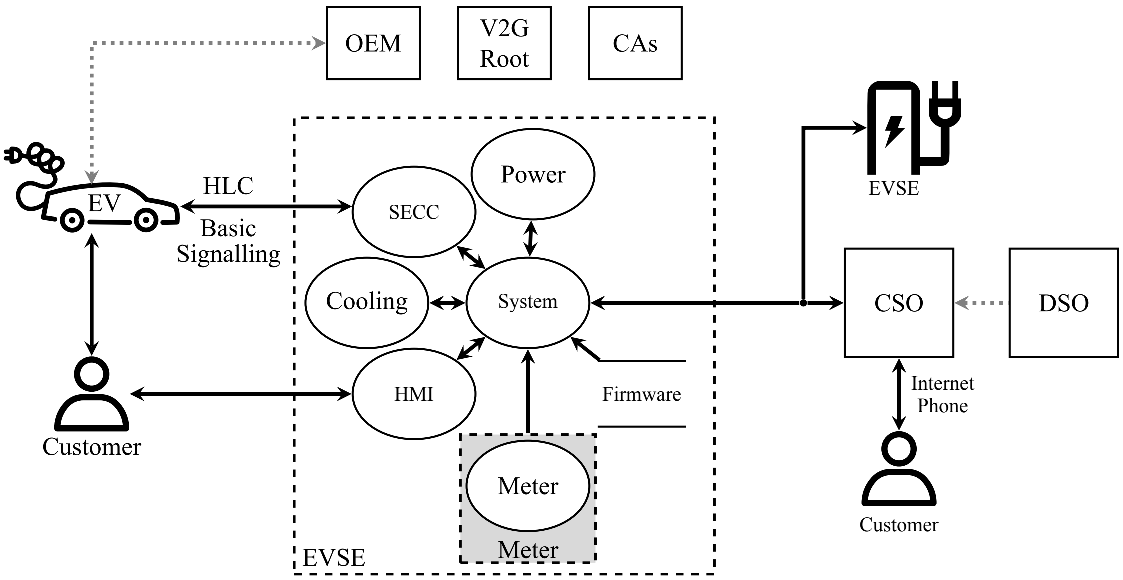

Figure 3: EVSE data flow diagram.

heat loads, so the Cooling controller is instrumental for thermal management of the EVSE and ancillary components. The high-current power supply ($\geq$ 400 A) necessitates large gauge cabling. To reduce bulk and make it less cumbersome, the cabling will likely be liquid cooled (Howell *et al.* 2017). A human-machine interface (HMI in the figure) assists customer authorisation and payment processing, and reports charging session metrics such as the amount of power delivered and incurred fees. The meter reports usage and operates in a trust domain distinct from the System. Wireless communication (in particular, cellular) or a wired field network connect the EVSE to the CSO. The CSO will adjust its electric demand based on congestion and other smart charging signals received from the DSO.

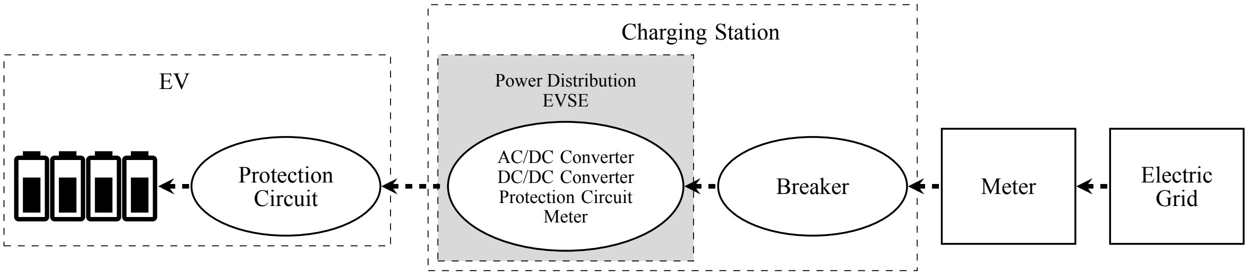

Figure 4: Charging infrastructure electric power flow diagram.

The final system model, **Figure 4**, illustrates the relationships imposed by power connections. An HPC charging station is likely supplied by a 480 V to 35 000 V electric grid (distribution network) feeder. A utility monitors the electricity consumption at the station meter, which is distinct from the EVSE meters that measure the power transferred to the vehicle and is used to bill the customer. The station's power distribution unit supplies power to one or more EVSEs, which in turn transfers power to EVs. A remote-controllable breaker (independent or incorporated in the power distribution unit) can disrupt power to the station. Additional local protection circuits may trip and disrupt a charging session. While not depicted in the figure, it is reasonable to assume that onsite storage and generation will supplement the electric grid supply (Bohn 2020).

The system models were analysed independently and combined using the threat modelling methodology described in the previous section. The consequences and threats are enumerated in Table **1**. The table contents are edited and compressed to comply with publication constraints. The threats are labelled as remote (R) or local (L). Remote is defined as a threat that can be executed entirely through internet communications. Local is defined as a threat that requires a physical presence to the targeted components to execute some portion of an attack. The remote designation suggests greater risk as the attacker can assault the systems from anywhere in the world.

Table 1: Mapping consequences and threats.

Consequence: Loss of financial/energy transaction integrity or nonrepudiation.

Attacker Payoff: Power is stolen or incorrectly billed.

Threat: An actor siphons electricity by impersonating an authorised consumer:

- Intercepting and tampering with EVCC-to-SECC data flows:
  - **(L)** Using a modified charging cable (Falk and Fries 2012,0).
  - **(L)** Inserting a false SECC that intercepts and proxies messages (especially applicable to "remote" ISO 15118 architectures).
  - **(L)** Using a software-defined radio to intercept and inject messages (Baker and Martinovic 2019).
- **(R)** Clone or replay identification/payment token.
- **(L)** Spoof the EVCC, for example by substituting the EVCC from a wrecked vehicle.

Threat: An actor tampers with the tariff schedule:

- **(R)** Intercept and tamper with the EVCC-to-SECC data flow (EVCC may optionally ignore signatures, see (ISOĨ5118-2, V2G2-307) and (ISOĨ5118-2, pp. 115, Note 6)).
- **(R)** Intercept and tamper with EVSE-to-CSO data flow or spoof the CSO.
- **(L)** Tamper with charger firmware, storage, or memory, targeting cached schedules ((ISO 2014, pp. 121, note 5) addresses schedule caching).

Threat: An actor repudiates power transfers:

- **(R)** Tamper with logs in the charger's memory or storage.
- **(R)** Tamper with the meter or meter-charger data flow.
- **(L)** Intercept charger-to-CSO data flows, tampering with transaction details (attacker accesses field network equipment).
- **(L)** Tamper with EVCC-to-SECC data flows, disabling metering receipts.
- **(R)** Spoof the EVCC, SECC, or both to manipulate and obscure transaction details.
- **(L)** Tamper with human-machine interface, accessing privileged functions.

Consequence: Trip breaker or trigger protection circuit action.

Attacker Payoff: EVs are incompletely charged, limiting their range. Transportation system availability is reduced when performed at scale.

Threat: An actor denies charging:

- **(L)** Tampers with the BMS firmware, configuration, or memory.
- Tampers with the EVCC-to-SECC data flow:
  - **(L)** Induce false charging state or settings.
  - **(R)** Impersonate charger and transmit false power measurements.
- **(L)** Physically tamper with power electronics.

Threat: An actor administratively opens breaker:

- **(R)** Compromises privileged CSO, charger vendor, or similar account via phishing.
- **(R)** Tampers with human-machine interface or controller storage, memory, or firmware.
- **(R)** Spoofs the CSO or tampers with charger-to-CSO data flows.

Continued on next page

Table 1 *—continued from previous page*

Consequence: Induce electric disturbances across the grid, such as voltage oscillations (O'Brien *et al.* 2019), undervoltage (Khan *et al.* 2019), low power factor (Rohde 2019), overfrequency (Acharya, Dvorkin and Karri 2020), and underfrequency events (Morrison 2018).

Attacker Payoff: Increase grid stress that may lead to outages.

Threat: An actor steals accounts:

- **(R)** Compromises charging application user-level accounts, commands charging halt.
- **(R)** Compromises developer account to insert malicious functions into smartphone apps, firmware, or related vector.
- **(R)** Compromises CSO, charging station equipment vendor, or breaker privilege account to update equipment with improper settings or firmware, or invokes immediate stop charge function. As an example consider: Fairley (2015) reports a vendor rapidly updating a large number of devices. Carlson and Rohde (2020) and Lyngaas (2019) discuss a relevant stop charge attack and the consequences. When both elements are considered together, a large-scale attack is conceivable.

Threat: An actor tampers with EV electronic control units:

- **(R)** Compromised telematic control unit provides vector to tamper with BMS or other electronic control unit (Oyler and Saiedian 2016).
- **(R)** EVCC commands incorrect voltage or current setpoints.
- **(R)** Modified electronic control unit firmware at supply chain source.

Threat: An actor alters the charger behaviour or state:

- **(R)** Tampers with controller firmware, storage, or memory.
- **(R)** Accesses privileged interface to alter setpoints.

Threat: An actor coordinates the disruption of the charging processes:

- **(R)** Denial-of-service attack against the CSO or charger-to-CSO data flow.
- **(R)** Denies trust store update, certificate revocation list update, or time synchronisation.

Consequence: Insufficient power delivery to EVs.

Attacker Payoff: EVs are incompletely charged leading to the unavailability of transportation.

Threat: An actor tampers with power delivery:

- **(R)** Compromised developer or admin account pushes invalid configuration.
- **(R)** Compromises EVSE's system shell and disrupts communication among EVSE power electronic modules (Rohde 2019).
- **(L)** Tampering with charger's memory, storage, and firmware or compromising system shell to modify configuration parameters or code.
- **(L)** Tampering with chargers to introduce electrical conditions (e.g. electrical shorts).

Threat: An actor interferes with the SECC:

- **(L)** Denies or intercepts and tampers with the EVCC-SECC or the charger-CSP dataflows.
- **(R)** Spoofs the charger or the CSP.
- **(R)** Denies CSP certificate revocation distribution or secure time synchronisation.

Consequence: Degraded or compromised vehicle powertrain, braking (Miller and Valasek 2015), steering (Miller and Valasek 2016), or batteries (Sripad *et al.* 2017).

Attacker Payoff: EVs are disabled, possibly permanently. Potential for vehicle accidents and injuries.

Threat: An actor compromises EV function:

- Compromised charger tampers with the EVCC, BMS, or other electronic control units:
    - **(R)** Overdischarging batteries, for example by modulating headlights (Sripad *et al.* 2017).
    - **(R)** Overcharging batteries by altering BMS controller setpoints.
    - **(L)** Disrupting thermal management and overheating of battery packs.
- **(R)** Tampers with the EVCC-SECC data flow, specifying values that exceed limits.

Consequence: CSO staff or EV driver receives bodily injury.

Continued on next page

Table 1 *—continued from previous page*

Attacker Payoff: People are injured while utilising an EVSE.

Threat: An actor tampers with the charger:

- **(L)** Tampered cooling controller causes customer to burn hand when touching connector or cabling.
- **(L)** Tampered circuit contactor is welded closed, causing electric shock.

Consequence: Employ infrastructure for purposes other than charging.

Attacker Payoff: Gain access to additional computational and network resources.

Threat: An actor repurposes CSP or charger computing and network resources:

- **(R)** Tampering with the charger or related systems to mine cryptocurrency.
- **(R)** Exploiting CSP or CSO systems to execute distributed denial of service attacks.

Consequence: Information disclosure and loss of privacy.

Attacker Payoff: Information that can be sold for money.

Threat: An actor illicitly accesses business-competitive information, such as customer data:

- **(L)** Tampers with CSO database using charging station field network access.
- **(R)** EV vulnerabilities or misconfigurations allow remote access to driver/vehicle information.

Discussion

The authors have presented the threat models of the EV infrastructure, investigating the security of HPC and the potential effect on the electric grid and transportation. The methodology was developed to establish the context to successfully identify relevant consequences and map them to threats. This was critical as HPC infrastructure is expansive, connected, and interdependent. Without context, we observed that the threats to essential exogenous systems, such as the electric grid, went unexplored. The systems were decomposed into logical blocks and may not be representative of real-world charging station system organisation. Nevertheless, threat modelling was valuable because the exercise illuminated weaknesses and security issues that appear in ISO 15118 and would likely be encountered in any vehicle charging infrastructure.

The ISO 15118 committee deliberately limited the scope of the standard to normalising the EV-to-charger interfaces. Infrastructure is more than just chargers and charging stations; it comprises a multitude of secondary actors to handle charging session authorisation, billing and payment processing, charging station operation and maintenance, vehicle registration, electric grid congestion and capacity management, station reservation, roaming, and smart charging. Roles and responsibilities of secondary actors and the associated interactions are addressed informally in ISO 15118. While addressing the entire vehicle infrastructure would certainly be ambitious, it would not provide the flexibility to address emerging technical and business requirements and challenges. Instead, complementary standards must fill in the gaps. Given the limited scope, the charging station is assumed to be trusted and is the hub of all communications between the EV and infrastructure. Consequently, end-to-end communication security is unavailable (van den Broek, Poll and Vieira 2015) as the charging station must route messages between the vehicle and, for example, the CSO. Some of the concerns are ameliorated with data security mechanisms. Contracts, tariff schedules, and metering receipts are signed and provide a means for the EV and third parties to ensure the authenticity and integrity of the data. Unfortunately, data security is not extensive because many necessary interactions are outside the purview of ISO 15118. Moreover, while communication and data security are required for “plug-and-charge”, their use remains optional when alternate authorisation schemes are employed. This remains an issue because plug-and-charge capability is not widely available, with most charging sessions authorised with external identification means.

EV charging security presents a significant challenge that is complicated by capital-intensive infrastructure, long vehicle service lifetimes (ten years and longer), and memory and computationally constrained devices that participate in charging regulation. Technical design had to balance the tradeoffs among functionality, interoperability, cost, and security. The choices made may have security repercussions. The ISO 15118-2 digital signature scheme is NIST P-256, an elliptic-curve digital signature algorithm extensively used in many compute-constrained applications. The algorithm and long lifespan of V2G root certificates (which are valid for 40 years) will collide headlong with quantum computing. An estimate of the number of qubits needed to factor P-256 is 2,330 (Roetteler *et al.* 2017), an accomplishment that may be achievable this decade (Chow and Gambetta 2020). ISO 15118-20, the communication standard designed to supplant ISO 15118-2, has adopted the elliptic-curve digital signature algorithms NIST P-521 and Ed448 (ISO/FDIS 1̃5118-20), both of which increase the difficulty to break the cryptography. Unfortunately, the changes are not backward compatible with ISO 15118-2 and still may not offer sufficient margin of security given vehicle lifespans and anticipated quantum computing advancements. Cryto-agility, the capacity to switch to alternate cryptographic primitives without inducing significant system changes, is seen as an imperative to prepare for the coming quantum computing era (Chen *et al.* 2016). ISO 15118 exhibits limited crypto-agility; instead, it specifies hard requirements and parameters. As ISO 15118 lacks a meaningful future-proofing mechanism (such as algorithm negotiation for digital signature schemes), protocol, and parameter substitutions that will need to be in subsequent revisions of the standard, which will bring incompatibilities. Manufacturers, vendors, and operators will face an intractable choice: either prevent some vehicle models from charging as they cannot be modified to interoperate; or allow vehicles to charge using vulnerable algorithms, protocols, and parameters, a practice that is widely considered to be highly insecure. Migration to TLS 1.3 (and possibly quantum-safe digital signature algorithms and hybrid certificates) will serve to highlight the challenges of transitioning current EV charging to a more secure variant.

Charging infrastructure security cannot be an afterthought as cyberattacks will have severe consequences to individuals and societies. The threat model activity was undertaken to recognise, identify, and characterise security objectives, threats, and vulnerabilities. Work is underway to investigate and develop relevant countermeasures and safeguards to prevent or mitigate the threats. Technology alone cannot solve the issue. As vehicles become more connected, EVs, charging infrastructure, and the electric grid can no longer assume that they are isolated from the outside world. Due to the tight coupling between charging infrastructure and electric grid, and since no entity is ideally positioned to address security challenges, electric utilities, vehicle manufacturers, charging station equipment vendors, operators, and service providers will need to collaborate in assuring electric supply and EV charging services. Establishing a consortia to define and demarcate responsibilities and roles, facilitate information sharing, and coordinate activities would support the undertaking of the enterprise beyond the resources of any single member. Moreover, the collaboration could support the development of components critical to the safe and secure operation of charging infrastructure, such as the design and fielding of a public key infrastructure platform that is embraced internationally (Metere *et al.* 2021).

Research is required to develop countermeasures and safeguards to mitigate the novel threats identified in this work and that account for the character of charging infrastructure and services. Work conducted by the community is actively underway. For instance, Fuchs *et al.* (2020) proposes a hardware security module for EVs to ensure the secure generation and storage of credentials. Idaho National Laboratory (Carlson 2021) is developing a safety instrumented system framework to monitor EV charger operation and properties. van den Broek, Poll and Vieira (2015) propose securing the information instead of the communication channel. Additionally, secondary actor confirmations can thwart spoofing (Lee *et al.* 2014). Charging security research is critical as the United States sets a 2030 target for half of all new light-duty vehicle sales as EVs (United States, Executive Office of the President 2021).

References

Acharya, S, Dvorkin, Y, & Karri, R 2020, 'Public Plug-in Electric Vehicles + Grid Data: Is a New Cyberattack Vector Viable?', *IEEE Transactions on Smart Grid*, vol. 11, no. 6, pp. 5099–5113.

Ahmed, S & Dow, FM 2016, 'Electric vehicle and charging station technology as vulnerabilities threaten and hackers crash the smart grid', *Int. J. Innov. Sci. Eng. Technol.*, vol. 3, no. 10, pp. 98–103.

AUTOSAR 2018, Specification of secure onboard communication, Specification CP v4.4.0, AUTOSAR.

Baker, R & Martinovic, I 2019, 'Losing the car keys: Wireless PHY-layer insecurity in EV charging', *Proc. of the 28th USENIX Security Symposium SEC '19*, pp. 407–422.

Bao, K, Valev, H, Wagner, M, & Schmeck, H 2018, 'A threat analysis of the vehicle-to-grid charging protocol ISO 15118', *Comput. Sci. Res. Dev.*, vol. 33, pp. 3–12.

Bohn, T 2020, *Multi-port, 1+MW charging system for medium- and heavy-duty EVs: What we know and what is on the horizon?*

Brandl, M, Gall, H, Wenger, M, Lorentz, V, *et al.* 2012, 'Batteries and battery management systems for electric vehicles', *Proc. of the Design, Automation Test in Europe Conference Exhibition (DATE)*, pp. 971–976.

Carlson, B 2021, *Consequence-driven cybersecurity for high-power EV charging infrastructure*, viewed 28th August 2021, <https://www.energy.gov/sites/default/files/2021-06/elt199_carlson_2021_o_5-12_351pm_LR_TM.pdf>.

Carlson, B & Rohde, K 2020, *Consequence-driven cybersecurity for high power EV charging infrastructure*, viewed 8th July 2021, <https://www.energy.gov/sites/default/files/2020/06/f75/elt199_Carlson_2020_o_5.1.20_1.12PM_JL_0.pdf>.

Chen, L, Jordan, S, Liu, YK, Moody, D, *et al.* 2016, Report on post-quantum cryptography, NISTIR 8105, NIST.

Chow, J & Gambetta, J 2020, *Quantum takes flight: Moving from laboratory demonstrations to building systems*, <https://www.ibm.com/blogs/research/2020/01/quantum-volume-32/>.

Fairley, P 2015, *800,000 microinverters remotely retrofitted on oahu—in one day*, viewed 11th August 2021, <https://spectrum.ieee.org/in-one-day-800000-microinverters-remotely-retrofitted-on-oahu>.

Falk, R & Fries, S 2012, ‘Electric vehicle charging infrastructure: Security considerations and approaches’, *Proc. of the 4th Int. Conf. on Evolving Internet (INTERNET)*, IARIA.

—— 2013, ‘Securely connecting electric vehicles to the smart grid’, *Int. J. Adv. Internet Technol.*, vol. 6, no. 1 and 2, pp. 57–67.

Fuchs, A, Kern, D, Krauß, C, & Zhdanova, M 2020, ‘HIP: HSM-based identities for plug-and-charge’, *Proceedings of the 15th International Conference on Availability, Reliability and Security*, pp. 1–6.

Gottumukkala, R, Merchant, R, Tauzin, A, Leon, K, *et al.* 2019, ‘Cyber-physical system security of vehicle charging stations’, *Proc. of the 2019 IEEE Green Technologies Conference (GreenTech)*, pp. 1–5.

Harnett, K, Harris, B, Chin, D, & Watson, G 2018, DOE/DHS/DOT Volpe technical meeting on electric vehicle and charging station cybersecurity, Technical Meeting Report DOT-VNTSC-DOE-18-01, US DOT.

Hartzell, S & Stubel, C 2017, *Automobile CAN bus network security and vulnerabilities*, <https://canvas.uw.edu/files/47669787/download>.

Hodge, C, Hauck, K, Gupta, S, & Bennett, JC 2019, Vehicle cybersecurity threats and mitigation approaches, Technical Report NREL/TP-5400-74247, 1559930, NREL.

Howell, D, Boyd, S, Cunningham, B, Gillard, S, & Slezak, L 2017, *Enabling fast charging: A technology gap assessment*, <https://www.energy.gov/eere/vehicles/downloads/enabling-extreme-fast-charging-technology-gap-assessment>.

ISO 2014, *ISO 15118-2: Road vehicles: Vehicle-to-Grid: Communication Interface—Part 2: Network and application protocol requirements*.

—— 2021, *ISO/FDIS 15118-20: Road vehicles—Vehicle to grid communication interface—Part 20: Network and application protocol requirements*.

Khan, OGM, El-Saadany, E, Youssef, A, & Shaaban, M 2019, ‘Impact of Electric Vehicles Botnets on the Power Grid’, *2019 IEEE Electrical Power and Energy Conference (EPEC)*, pp. 1–5, viewed 9th August 2021, <http://arxiv.org/abs/2103.09153>. arXiv: 2103.09153 version: 1.

Khan, R, McLaughlin, K, Laverty, D, & Sezer, S 2017, ‘STRIDE-based threat modeling for cyber-physical systems’, *Proc. of the IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*.

Kintner-Meyer, M, Schneider, K, & Pratt, R 2007, *Impacts assessment of plug-in hybrid vehicles on electric utilities and regional U.S. power grids, part 1: Technical analysis*.

Kohnfelder, L & Garg, P 1999, ‘The threats to our products’, *Microsoft Interface*, <https://adam.shostack.org/microsoft/The-Threats-To-Our-Products.docx>.

Lee, S, Park, Y, Lim, H, & Shon, T 2014, ‘Study on analysis of security vulnerabilities and countermeasures in ISO/IEC 15118 based electric vehicle charging technology’, *Proc. of the 2014 International Conference on IT Convergence and Security (ICITCS)*.

Lyngaas, S 2019, *Power struggle: Government-funded researchers investigate vulnerabilities in EV charging stations*, viewed 11th August 2021, <https://www.cyberscoop.com/ev-charging-stations-hacked-idaho-national-laboratory/>.

Meintz, A, Zhang, J, Vijayagopal, R, Kreutzer, C, *et al.* 2017, 'Enabling fast charging–vehicle considerations', *Journal of Power Sources*, vol. 367, pp. 216–227.

Metere, R, Neaimeh, M, Morisset, C, Maple, C, *et al.* 2021, 'Securing the electric vehicle charging infrastructure', *CoRR*, vol. abs/2105.02905, <https://arxiv.org/abs/2105.02905>.

Miller, C & Valasek, C 2015, *Remote exploitation of an unaltered passenger vehicle*.

—— 2016, *Advanced CAN injection techniques for vehicle networks*, viewed 13th August 2021, <https://infocon.org/cons/Black%20Hat/Black%20Hat%20USA/Black%20Hat%20USA%202016/Advanced%20CAN%20Injection%20Techniques%20for%20Vehicle%20Networks.mp4>.

Miller, M 2008, 'Modeling the trust boundaries created by securable objects', *Proc. of the 2nd USENIX Workshop on Offensive Technologies (WOOT)*.

Morrison, G 2018, Threats and mitigation of DDoS cyberattacks against the U.S. power grid via EV charging, Master's thesis, Wright State University.

Mültin, M 2021, *The new features and timeline for ISO 15118-20*, viewed 27th August 2021, <https://www.switch-ev.com/news-and-events/new-features-and-timeline-for-iso15118-20>.

O'Brien, JG, Maloney, PR, Agrawal, U, Carroll, TE, & Pratt, RM 2019, Electric vehicle infrastructure consequence assessment, Technical Report PNNL-29514, Pacific Northwest National Laboratory.

Oyler, A & Saiedian, H 2016, 'Security in automotive telematics: a survey of threats and risk mitigation strategies to counter the existing and emerging attack vectors', *Security Comm. Networks*, vol. 9, pp. 4330–4340.

Pratt, RM & Carroll, TE 2019, 'Vehicle charging infrastructure security', *Proc. of the IEEE Int. Conf. on Consumer Electronics (ICCE)*.

Roetteler, M, Naehrig, M, Svore, KM, & Lauter, K 2017, *Quantum resource estimates for computing elliptic curve discrete logarithms*, Cryptology ePrint Archive, Report 2017/598, <https://eprint.iacr.org/2017/598>.

Rohde, KW 2019, Cyber security of DC Fast Charging: Potential impacts to the electric grid, Technical Report INL/CON-18-52242-Revision-0, Idaho National Laboratory.

SAE 2017, *J1772: Electric Vehicle and Plug in Hybrid Electric Vehicle Conductive Charge Coupler*.

Shevchenko, N 2018, *Threat modeling: 12 available methods*, viewed 26th May 2020, <https://insights.sei.cmu.edu/sei_blog/2018/12/threat-modeling-12-available-methods.html>.

Shostack, A 2014, *Threat Modeling: Designing for Security*, 1st edn, Wiley.

Sommer, F, Dürrwang, J, & Kriesten, R 2019, 'Survey and classification of automotive security attacks', *Information*, vol. 10, no. 4.

Sripad, S, Kulandaivel, S, Pande, V, Sekar, V, & Viswanathan, V 2017, 'Vulnerabilities of electric vehicle battery packs to cyberattacks on auxiliary components', *CoRR*, vol. abs/1711.04822, <http://arxiv.org/abs/1711.04822>.

Ulrich, L 2020, 'Exclusive: GM can mange an EV's batteries wirelessly—and remotely', *IEEE Spectrum: Technology, Engineering, and Science News*.

United States, Executive Office of the President 2021, *Executive Order on strengthening American Leadership in clean cars and trucks*.

van den Broek, F, Poll, E, & Vieira, B 2015, 'Securing the Information Infrastructure for EV Charging', *Wireless and Satellite Systems*, pp. 61–74.

Volpe National Transportation Systems Centre 2019, *Extreme fast charging (XFC) cybersecurity threats, use cases and requirements for medium and heavy duty electric vehicles*, viewed 26th August 2021, <https://github.com/nmfta-repo/nmfta-hvcs-xfc>.

Pacific Northwest
National Laboratory

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99354

1-888-375-PNNL (7665)

www.pnnl.gov