energies

Review

Review of Electric Vehicle Charger Cybersecurity Vulnerabilities, Potential Impacts, and Defenses

Jay Johnson *, Timothy Berg , Benjamin Anderson and Brian Wright

Sandia National Laboratories, Albuquerque, NM 87123, USA; tberg@sandia.gov (T.B.); brander@sandia.gov (B.A.); bjwrigh@sandia.gov (B.W.)
* Correspondence: jjohns2@sandia.gov; Tel.: +1-505-284-9586

Abstract: Worldwide growth in electric vehicle use is prompting new installations of private and public electric vehicle supply equipment (EVSE). EVSE devices support the electrification of the transportation industry but also represent a linchpin for power systems and transportation infrastructures. Cybersecurity researchers have recently identified several vulnerabilities that exist in EVSE devices, communications to electric vehicles (EVs), and upstream services, such as EVSE vendor cloud services, third party systems, and grid operators. The potential impact of attacks on these systems stretches from localized, relatively minor effects to long-term national disruptions. Fortunately, there is a strong and expanding collection of information technology (IT) and operational technology (OT) cybersecurity best practices that may be applied to the EVSE environment to secure this equipment. In this paper, we survey publicly disclosed EVSE vulnerabilities, the impact of EV charger cyberattacks, and proposed security protections for EV charging technologies.

Keywords: cybersecurity; electric vehicle supply equipment (EVSE); electric vehicle (EV); EV chargers; power system security

Citation: Johnson, J.; Berg, T.; Anderson, B.; Wright, B. Review of Electric Vehicle Charger Cybersecurity Vulnerabilities, Potential Impacts, and Defenses. *Energies* **2022**, *15*, 3931. https://doi.org/10.3390/en15113931

Academic Editor: Mario Marchesoni

Received: 10 May 2022
Accepted: 24 May 2022
Published: 26 May 2022

1. Introduction

Electric vehicle charging is expected to drastically increase in the next decade. Charging points in the EU and UK increased from approximately 34,000 in 2014 to 250,000 in September 2020, and the European Commission has set a target of 1 million charging points by 2025 to curb greenhouse gas emissions [1]. Similarly, the United States experienced a 9.2% quarterly growth rate in public chargers in 2020 Q4 [2] and recently passed the 100,000 public charger mark in March 2021 [3]. In the U.S., a bipartisan infrastructure bill passed in November 2021 in which USD 7.5B was allocated for developing an EV charging network across the country [4]. In addition to the expanding prevalence of electric vehicles and chargers in the passenger vehicle area, there is also an increased adoption of electric vehicles for medium and heavy duty (i.e., freight) applications [5].

Even with growing vehicle battery capacities, users are expecting faster turnarounds at chargers. As a result, chargers are becoming increasingly powerful. Extreme fast charging (XFC) draws 350–400+ kW to provide 200 miles of range in about 15 min [6]. For medium and heavy duty applications ranging from school and city buses to commercial delivery and over-the-road trucks, current designs are supporting more than 1 MW per vehicle [7–9].

Charging providers and users alike seek to optimize their use of the growing network of fast chargers through a variety of highly interconnected and internet-enabled tools. EVSE must communicate with cloud services, EVs and their battery management systems, and much more. For example, EV chargers may be integrated into distributed smart grid EV charging, or interconnected with Building Automation Systems (BAS) or Building Energy Management Systems (BEMS) [10]. On a larger scale, EV chargers are taking a role in smart city technologies to help ensure the sustainability of urban living [11]. Automated and networked connections to grid and microgrid power management and controls round out the picture of the complexity of EVSE connectivity.

The breadth and complexity of EVSE connections create a large cybersecurity profile and raise concerns that bad cyber actors could use insecure chargers as an unauthorized access point to abuse charging equipment, vehicles, buildings, or grid resources. Each of these systems represents a set of interconnected attack vectors. EVs, for example, interface with dealerships, mobile phones, navigation, mapping, telemetry, entertainment, vehicle-based web browsers, other vehicles, driver assist systems, over-the-air software updates, and more [12,13], using an array of protocols, including Bluetooth, GSM Mobile, and Wi-Fi. Autonomous-driving electric vehicles add further cybersecurity complexity [14,15]. Malicious actors are increasingly targeting smart phones (e.g., an iOS TCP exploit published by Google's Project Zero [16,17]) and vehicle systems [18] to circumvent keyless entry and remote starting [19–21]. Researchers have highlighted the manipulation of onboard, safety-critical electronic control units (ECUs) to interfere with braking, steering, engine and battery controls [22]. Vehicle data are also at risk, including telematics, tracking [22–24], customer, dealer and insurance data [25–27]. EVSE interfaces with highly connected EVs and vendor systems, charger owners, and grid operator systems.

Fortunately, there have been several efforts to map out the risks within the EVSE ecosystem [28,29]. Based on these threat models, trucking industry stakeholders, including the National Motor Freight Traffic Association (NMFTA) and Volpe Laboratory have studied the potential impacts of cyberattacks on electric vehicle charging, and provided the community with guidance across the lifecycle of EVSE [7,30–34]. ElaadNL has created detailed EV charging security requirements [35], a UK consortium created a list of smart charging and V2G recommendations [36], and Sandia National Laboratories created a reference for EVSE cybersecurity best practices [37]. New efforts to address security gaps have recently started too. The Trusted Computing Group (TCG) Vehicle Service Work Group is investigating EV charging cybersecurity and Southern California Edison established a cybersecurity gap analysis project for EVSE products [38]. Additional resources include cybersecurity frameworks, standards, and best practices that are general [39–41] or tailored to related areas such as operational technology (IEC 62443) [42]; information technology enterprise [43–45]; vehicles and EVs [46–55]; smart buildings [56]; and the electrical grid [57,58].

In this paper, we present a review of cybersecurity vulnerabilities, risks, and defenses for the EVSE ecosystem. This paper seeks to refine the strategy for mitigating cybersecurity risks by categorizing the types of charger interfaces that can serve as attack vectors, identifying the potential attacks that might utilize these interfaces, and determine mitigations that may be effective against these attacks in the future. We also review potential cyber impacts on the power system, billing functions, and interrelated systems. Finally, we survey mitigation suggestions and best practices based on ideas presented in the literature.

2. Methodology

This review categorizes EVSE cybersecurity assessments and vulnerabilities by interface type. This approach was taken to create an easy-to-reference map that directly relates EVSE cybersecurity research to the architecture of fielded systems. EVSE interfaces that were considered in the creation of these categories include, internal charger ports; vehicle-to-EVSE communication interfaces; EV owner access points (e.g., RFID); external maintenance ports; wireless access (cellular, Wi-Fi, Bluetooth, etc.); and wired ports. Cloud services that interact with the EVSE via these interfaces were also considered.

While implementations, topologies, and data exchanges vary between vendor and jurisdiction, there are some common features among many EVSE devices. As depicted in Figure 1, the EVSE includes external EV connectors, an authentication terminal (e.g., the front console), and a maintenance terminal(s) that may be internal to the EVSE housing. The EVSE also often has a cellular or other internet connection for the EVSE operator or service provider to capture data on charging sessions, push new firmware, and collect prognostics and user data using Open Charge Point Protocol (OCPP), IEEE 2030.5, or proprietary protocols.

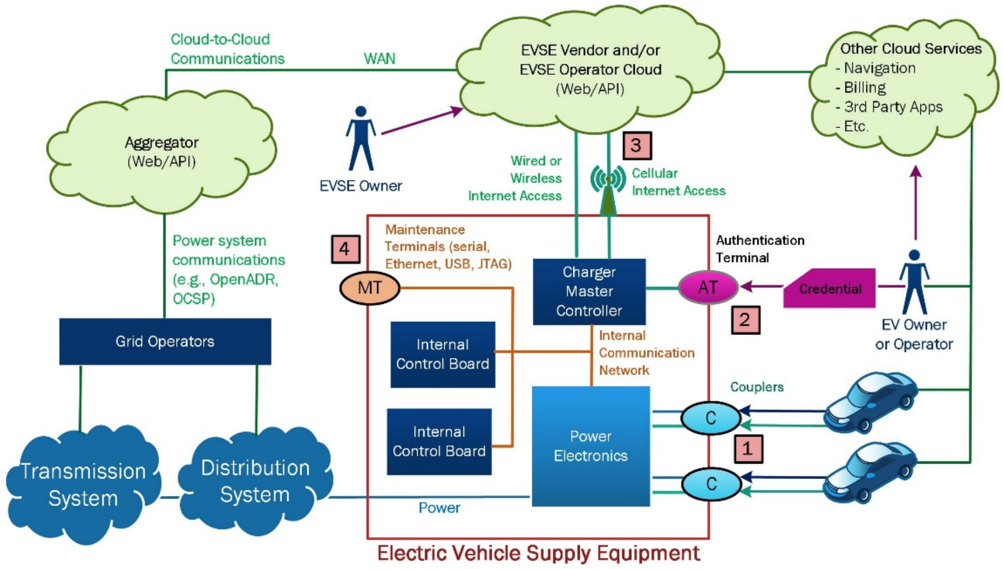

Figure 1. Electric vehicle communication ecosystem with EVSE components and external entities.

Within the vehicles, there are services connected to different cloud services to support music; browsing; navigation; emergency services (e.g., OnStar); telematics; infotainment; etc. Some of these systems may be connected to third-party cloud environments to support billing and other services. The service provider may connect to other service provider backend networks to verify charging transactions on chargers they do not own using Open Clearing House Protocol (OCHP), or to grid operators using Open Smart Charging Protocol (OSCP), OpenADR, or some other protocol.

In Figure 1, there are four numbered boxes that represent attack vectors for adversaries seeking to affect EVSE operations. These include, (1) EV connectors; (2) user terminals; (3) internet connections; (4) maintenance terminals from physical access or disassembly. In some cases, the lines between these interfaces were blurry (e.g., a web interface was used for maintenance). In these cases, the authors selected the interface category that they believed to be the most representative of the attack vector, as discussed in the following subsections.

2.1. EV-to-EVSE Interfaces

EVSE connectors (i.e., the couplers or plugs) range in terms of power level, type, and underlying communication technology [59]. IEC 61851-1 defines four conductive charging "modes" for EV chargers based on the current and voltage:

- Mode 1 is a passive AC connection up to 16 A at 240 V single phase or 480 V three-phase;
- Mode 2 includes an in-cable control and protection device (IC-CPD) which performs control and safety functions. It operates up to 32 A at 240 V single phase or 480 V three-phase;
- Mode 3 includes the IC-CPD but increases the max current to 250 A;
- Mode 4 is DC connection up to 600 V at a current $\leq$ 400 A.

In the U.S., 120 Vac chargers are often colloquially referred to as *Level 1* chargers, 240 Vac chargers are *Level 2*, and direct current charging is called *Level 3* or DC Fast Charging (DCFC). Charging above 400 kW, which uses a cooled charging cable, is sometimes referred to as Extreme Fast Charging (XFC) [60]. Traditionally, most chargers in the United States were Level 1 or 2 chargers that would be powered domestically, but now it is common to find higher power DCFCs with CCS, CHAdeMO, or Tesla connectors in public places or in the workplace.

Conductive connectors, or couplers, in the US market that are defined in IEC 62196-1 [61], -2 [62], and -3 [63], include:

- Type 1—A 5-pin, single-phase connector defined in SAE J1772 [64] and IEC 62196 [61]. SAE J1772 and IEC 61851-1 [65] define a 1 kHz Pulse Width Modulation (PWM) square-wave signal to communicate status and current capacity between charger and vehicle.
- Type 2—A 7-pin, three-phase connection defined in SAE J3068 [66]. This uses a Local Interconnect Network on the Control Pilot (LIN-CP) for digital communications between charger and vehicle.
- AA—A Mode 4 DC CHAdeMO coupler defined in Japanese standard JEVS G105-1993 [67–69]. This Japanese standard uses a Controller Area Network (CANbus) for EVSE-EV communications as defined in IEEE 2030.1.1 [70] and ISO 11898 [71].
- EE—A Mode 4 DC Combined Charging System (CCS) Combo 1 coupler. This connector superimposes two communication protocols on the cordset to communicate between EV and EVSE. The first is ISO/IEC 15118 [72] which uses a power line communication (PLC) internet protocol (IP) stack built on the HomePlug Green PHY (HPGP) [73] Data Link and Physical layers. The second protocol is the IEC 61851-1 pulse-width modulation (PWM) signal [65].

There are other couplers and associated communication protocols, including the Tesla connectors based on single-wire CAN defined in SAE J2411 [74] and the Guobiao (Chinese national) standard GB/T 20234.2-2015 [75] connectors which communicate a CAN network protocol based on the SAE J1939 series [76]. Each represent a set of communication capabilities that could transfer falsified charging parameters or malware to the EVSE, because modern vehicles—including semi- and fully-autonomous vehicles—provide attack vectors into the EV/EVSE ecosystem [14,46,77–80]. The compromise of vehicle systems may also allow the attacker an initial foothold in the environment from which they could pivot to the EVSE device through wired or wireless communications. The cordset and communication protocol may also expose the charging session to side-channel attacks. Each of these scenarios is covered in more detail in Section 3.

2.2. EV Operator Interfaces

Public EVSE devices offer a range of methods for authenticating a charging session. These methods include using Radio Frequency Identification (RFID) tags, smart phone Near Field Communication (NFC), or credit card chip/swipes. These methods link the EV operator (i.e., owner or driver) or their account information to the charging session for billing and tracking purposes. Many DCFCs now also include touch screen front panels that allow the driver to determine the cost of electricity and vehicle status (charging rate, state of charge, etc.). Some EVSE vendors also include the ability to display custom messages or run advertisements on their EVSE devices.

Notably, plug-and-charge functionality that is developed in ISO 15118-20 [81] will allow the vehicle to automatically authenticate over the charging cable. This is achieved with a public key infrastructure (PKI) that uniquely identifies each of the vehicles. The setup, operation, governance of this PKI ecosystem, and the generation and storage of cryptographic materials has been the source of significant debate within the industry. It is likely that this will be an area of active cybersecurity research in the future.

The driver–user interfaces on the EVSE are a significant attack vector for the charger. In addition to the standard functionality, there are commonly hidden maintenance menus or password protected service options on these interfaces. The compromise of these systems would allow adversaries to disable charging, change prices, or otherwise affect the operations of the equipment.

2.3. EVSE Internet Interfaces

Modern EVSE connects to one or more internet services. These connections typically exchange telemetry data and extend control to EVSE vendor or third-party cloud environments. Cloud-to-cloud communications then enable billing operations and grid operators to interact with EVSE equipment as shown in Figure 1. In many cases, the EVSE communications are proprietary for the EVSE vendor, but Open Charge Point Protocol (OCPP) [82];

Open Smart Charging Protocol (OSCP) [83]; IEEE 2030.5 [84]; OpenADR [85]; Message Queue Telemetry Transport (MQTT) [86]; and Building Automation Control network (BACnet) [87] are also in use by EVSE devices on the market [88,89]. OCPP is widespread and used to connect EVSE to third-party EVSE monitoring and control networks. OCPP is currently on Version 2.0.1, but Version 1.6 is widely used in the field. Unfortunately, OCPP did not include PKI encryption until Version 1.8 [90], so many EVSE rely on running this older, unencrypted protocol which requires the use of virtual private networks (VPNs), isolated cellular networks, or other protections to avoid reconnaissance and hacking attempts.

Generally EVSE are firewalled from the internet, but multiple devices have been found using the Shodan and other targeted searches [88]. Not only do these internet connections create the potential for the EVSE to be exploited from the internet, but there is also a risk that EVSE vendors or operator systems could be compromised by using the EVSE as an entry vector into their networks. This would result in an attacker potentially controlling large fleets of EVSE devices which could impact power grid operations, transportation systems, or other critical infrastructure. The ability to pivot between vehicle, EVSE, and cloud interconnected domains was the focus of previous attack tree research [91].

2.4. EVSE Maintenance Interfaces

Based on hands-on penetration tests of a dozen EVSE devices, Sandia National Laboratories determined that modern EVSEs, especially DCFCs, are constructed using multiple circuit boards which communicate together over ethernet, serial, analog, or other connections [92]. These inter-module communications are rarely encrypted. In many cases, ethernet switches are located within the enclosure and access to the internal network can be achieved by simply connecting to this switch. In other cases, USB serial ports, JTAG headers, or other physical ports are available for EVSE vendors to debug the equipment; however, these ports are often left open in production equipment which may allow adversaries to monitor or disrupt equipment operations. EVSE also commonly hosts Telnet, SSH, or local website services to allow owners to configure the device or collect maintenance/usage data.

3. EVSE Vulnerabilities

Potential EVSE vulnerabilities have been identified through risk and threat modeling efforts, e.g., [93–99]. In these theoretical studies, the researchers identified potential areas where vulnerabilities could result in consequences of concern such as data loss, spoofing, and denial of service. In this work, we focus on publicly disclosed vulnerabilities and demonstrated exploits. This section presents a survey of EVSE vulnerabilities to better understand the threat landscape for EV charging, separated by the four interfaces described above. Chronological summaries of these vulnerabilities are presented for each of the interfaces in Tables 1–4.

3.1. EV-to-EVSE Interface Vulnerabilities

There have been multiple demonstrations of stealing credentials or influencing charging sessions via the EV-to-EVSE connection. Oxford researchers, Baker and Martinovic, demonstrated that they could sniff radiated HomePlug Green PHY data on a CCS connection using unencrypted ISO 15118/DIN 70121 [100] traffic, using a software defined radio (SDR) [101]. Köhler et al. subsequently showed that charging sessions could be wirelessly aborted by disrupting the PLC communications in their *Brokenwire* attack demonstrations [102]. The researchers found that they could abort CCS charging sessions at distances of 47 m using SDRs with less than 1 W of power, and this attack was successful on all seven vehicles and 18 EVSEs that they investigated.

CCS communications do not provide mutual authentication, so there is a risk of MITM attacks; this presents risks to billing data privacy and, by stealing MAC addresses, creates a possible avenue for user tracking. Idaho National Laboratory (INL) indicated that there was a risk that EVs could spread viruses to EVSE which would then further propagate the malware [103]. Rohde demonstrated disruptions to charging, including a changing power level and increased high total harmonic distortion in a DCFC charging session using a CHAdeMO connector when malware on the EV or EVSE falsified the EV battery's state-of-charge (SOC) [104]. Another team of researchers created the *V2G Injector*, an open-source tool to read and write HomePlug Green PHY data. They demonstrated that a malicious actor could collect network keys and inject data into the CCS Efficient XML Interchange (EXI) network sessions [105]. In some follow-on work, a Trend Micro combined the *V2G Injector* with an Apache logging package (Log4j) vulnerability to escalate access privileges on a simulated EVSE running a V2G Java stack [106].

The ISO 15118 protocol has garnered extensive security and threat analyses [95,107–109]. Lee et al. found that the ISO 15118 communications may expose the risk of an EV spoofing another vehicle, stealing power, falsifying meter data to gain free charging, or forging the malfunction status to prevent operations [107]. Bao et al. had similar concerns of session hijacking; charging repudiation; and machine-in-the-middle (MITM), denial-of-service (DoS), and masquerading attacks [108]. The CCS Plug-and-Charge (PnC) PKI approach and credential management that were defined in ISO 15118-2 [110] have been the source of detailed studies. Siemens investigated the proposed ecosystem and noted challenges when EVSE devices are offline and the importance of managing cryptographic material, as well as emphasizing the need to secure other EVSE functions, such as multimedia services, firmware updates, and remote diagnosis [95,109]. Höfer et al. considered the privacy risks associated with ISO 15118 and found that they were inadequate for the authentication and authorization of payment and billing operations [111].

3.2. *EV Operator Interface Vulnerabilities*

Early-generation EVSE infrastructure was vulnerable to RFID cloning and other authorization bypass mechanisms with local access to the equipment. In 2017, Fraunhofer Institute for Industrial Mathematics (ITWM) researcher Mathias Dalheimer presented weak security practices in billing transactions and RFID card data storage in public charging infrastructure at the Chaos Communication Congress [112]. He demonstrated how RFID cards could be cloned in a way that other debit or credit cardholder accounts would be billed for charging sessions. Similar EVSE operator privacy and identification concerns were shared by Achim Friedland for RFID; smart phone; and MIFARE Classic (13.56 MHz contactless smart cards) authorization mechanisms [113]. There have also been warnings about credit card skimmers on EVSE equipment [114].

INL performed six Level 2 SAE J1772 EVSE assessments between 2014–2017. Two of these products were prototypes. They found that some of the EVSE devices included iOS and Android apps that were designed for customers to manage their charging session. These applications could easily be reverse-engineered to reveal weaknesses in the EVSE management and vendor cloud interfaces [115]. Many EVSE web service vulnerabilities have also been disclosed; these will be covered in the next section.

3.3. *EVSE Internet Interface Vulnerabilities*

EVSE devices often include a local web server or connect to cloud environments to relay information from the charge point operator, EVSE owner, or driver. We survey the vulnerabilities associated with internet communications in this section and break these vulnerabilities into (a) local web interfaces, (b) remotely accessible EVSE devices, and (c) EVSE communication to backend systems. In the case of the latter two, the remote communications over the public internet are especially concerning because of the scalability risk.

3.3.1. Web Services

One common issue with EVSE equipment is the presence of insecure web services that can be accessed locally from a smart phone or computer. In many cases, these are designed for EVSE configuration or maintenance via Wi-Fi. In home and enterprise environments, these services should be shielded by a firewall from the wider internet, but these vulnerabilities may expose home and corporate networks to a breach via the EVSE.

In the Pen Test Partners report there were multiple local web service issues: Wallbox included insecure direct object references in their web API; an EVBox web API vulnerability allowed account hijacking; and the EO mini pro was running the insecure Telnet protocol on port 2000, allowing an attacker to change the configuration data without any authentication [116]. A Shenzen Growatt Application Programming Interface (API) allowed firmware updates that could give access to home networks, and credentials were unchecked after the first login request [116]. In the INL assessment, they found unauthorized access to configuration files, and data were provided via insecure wireless web servers [115]. In a Hack in the Box presentation, Shezef reported finding DIP switches left in configuration mode and an open configuration web server on a GE EVSE [96].

Nasr et al. analyzed 16 EV Charging Station Management Systems (EVCSMS) by inspecting five EVSE firmware packages, three mobile applications, and eight web applications. As part of this work, multiple web server vulnerabilities were disclosed for the Schneider Electric EVlink City, EVlink Parking, and EVlink Smart Wallbox products, including Cross-Site Scripting (XSS); Cross-Site Request Forgery (CSRF); Server-Side Request Forgery (SSRF); and JavaScript information exposure [117–120]. Additionally, they found multiple vulnerabilities that affected charging processes, settings/firmware, billing, PII, and user data, as well as botnet recruitment opportunities and the potential for DoS and brute force attacks on web endpoints [120].

Kaspersky Lab found that the ChargePoint smart-phone application could remotely tamper with a charging session via Wi-Fi using a buffer overflow in the web server Common Gateway Interface (CGI) binaries [121]. The risk that was presented with this website vulnerability was that charging sessions could be stopped, or the maximum charging current could be increased to amperages above the circuit rating, tripping the breaker, overheating the wiring, or, in the worst case, causing a fire [122].

3.3.2. Internet-Accessible EVSE Services

The Argonne National Laboratory (ANL) and Illinois Institute of Technology (IIT) were able to locate multiple EVSE chargers on the public internet using Shodan, Nmap and Exploit Database's SearchSploit tool based on specific signatures [88]. ANL and IIT found that some devices were running unnecessary or outdated services, using weak credentials, or missing login timeout functions. Previously, INL found that Level 2 EVSE devices were not accessible via the public internet but could be reached by other devices that were connected to the same cellular provider [115]. The Shenzen Growatt network with 2.9 million devices on it only required the predictable serial number and an unvalidated username to lock and unlock the charger, and Pen Test Partners indicated that the locking action could stop all charging [116]. The Spanish Circontrol CirCarLife web service software exposed system software information, statuses, and critical setup information which could be accessed or exfiltrated by unauthenticated or unprivileged users [123,124].

Hille and Allhoff showed that several vulnerable services running on an EVSE could be accessed from the mobile network interface [125]. They found a weak key-exchange algorithm and no brute force protections on the SSH service; the web service used an unencrypted channel for logging in that could be bypassed by forging a Session Storage cookie; passwords were hashed using the insecure MD5 algorithm, and the HTTPS port used a SHA-1 self-signed certificate; and, lastly, the SQL server was vulnerable to data exfiltration.

3.3.3. Communications to Backend Server or Cloud Systems

Multiple issues associated with EVSE vendors, e-mobility service providers, and charge service-provider backend systems have been identified. These are typically hosted in the cloud using Amazon Web Services, Google Cloud, Azure, or another cloud platform to provide, (a) EV owners monitoring and control functionality; (b) EVSE owners pricing, billing, advertisement, and other functions; (c) other EVSE providers with cross-billing APIs; (d) utilities with demand management functions. These installations often expose insecure, remote management functions.

In the INL assessments identified that a management application lacked appropriate authentication methods, such as client-side validation, unencrypted HTTP service for logon credentials, and unsanitized logon fields that were vulnerable to SQL injection attacks [115]. INL also reported compromising a File Transfer Protocol (FTP) server that then pushed out modified firmware to all EVSE devices from this vendor in the next update cycle. They further noted the potential for command injection and XSS exploits on management servers and indicated that they discovered vulnerabilities that would allow the remote management of EVSE units that did not belong to that user account.

Cloud-to-cloud communications can be enabled through the Open Charge Point Interface (OCPI) [126]. This allows charge providers to bill other providers without downloading additional apps, etc. A ChargePoint GraphQL endpoint publicly exposed the details of their API interface, which could have acted as a first step to more severe attacks that would have impacted the 150,000 chargers connected to the ChargePoint system [116].

The Open Charge Point Protocol (OCPP) is commonly used between EVSE devices and backend or cloud networks to configure the charger and obtain charging statistics. The earlier versions of the protocol used unencrypted HTTP, so there were MITM risks for intercepting transaction data [90]. At DeepSec in 2016, Achim Friedland also pointed out the risk of network traversal once a charging station was compromised, as well as issues of missing OCPP guidance for network settings or certificate management [113]. Mathias Dalheimer and Achim Friedland further warned that it was also possible to decipher the data from the EVSE to the backend systems to intercept RFID, credit card via smart phone app, or other near-field-communication (NFC) data [112,113,127]. Rubio et al. further noted the risk of MITM attacks on OCPP [128]. In a joint white paper published by DigiCert, ChargePoint, and Eonti, the team performed a 360° maturity assessment on the ISO 15118-2 PKI system and scored the standard poorly in 85% of their governance, technical, and operations areas [129].

Supply chain vulnerabilities are also a risk for EV charging operations. During the Russian invasion of Ukraine in early 2022, Россети Злектротранспорт (Rosseti Electric Transport) EV chargers along the M-11 motorway between Moscow and Saint Petersburg were disabled and displayed anti-Putin and pro-Ukraine messages. Purportedly, a Russian EV charger provider, Gzhelprom, outsourced components, including the data controller to a Ukrainian Company, AutoEnterprise, which maintained remote backdoor access and control of the charging functionality [130,131]. This access allowed the component vendor to change the settings in the EVSE devices remotely.

3.4. EVSE Maintenance Interface and Hardware/Software Vulnerabilities

Maintenance interfaces are common on EVSE devices. These may be serial (e.g., RS485, RS232, serial over USB, or other Universal Asynchronous Receiver-Transmitter (UART) interfaces); Wi-Fi or Ethernet (e.g., SSH, Telnet, HTTP, etc.); Bluetooth; or via the front panel/screen. Cybersecurity researchers have found several vulnerabilities in the hardware and software running on EVSE. Two EVSE devices studied by Fraunhofer included USB ports that would copy logs and configuration data, including the OCPP server login and password, and authentication tokens from previous users [112]. Furthermore, modifying the configuration data on the USB drive and re-inserting it would automatically update the EVSE. This was the same behavior reported by INL in their Level 2 assessments.

INL also found (a) all the EVSE devices were running outdated Linux kernels with superfluous services (e.g., Telnet and FTP); (b) the processes were running as root, and stored passwords could be cracked "in a reasonable amount of time" because of weak hashing; (c) five devices did not include secure boot, and firmware images could be extracted; (d) firmware was unsigned; (e) there were active serial ports, ethernet jacks, and USB ports on the EVSE devices; (f) JTAG interfaces allowed direct control of the processor; (g) physical tamper-detection tools could be bypassed; (h) multiple insecure coding practices were observed [115]. Kaspersky Lab found that they could trigger a factory reset using a special blinking pattern that was picked up with the photodiode on the EVSE [121].

In a Pen Test Partners report, EO Mini Pro 2, Hypervolt, and Wallbox EVSE devices used Raspberry Pi single-board computers in their products. These inexpensive computers do not include secure bootloaders, so any data on them—such as homeowner Wi-Fi Pre-Shared Keys (PSKs) or other credentials, such as usernames, passwords, etc.—could be stolen by physically pulling the memory [116,132,133]. Schneider EV chargers included hard-coded credentials, improper verification of cryptographic signatures, encrypted credentials disclosure mechanisms, unverified user password changes, and passwords hashed without a salt [117–119].

Table 1. EV-to-EVSE interface vulnerabilities.

Researchers	Year	Vulnerability Description	Coupler	Citation
Höfer et al.	2013	Credential theft and privacy risks.	CCS	[111]
Lee et al.	2014	EV ID spoofing, power stealing, falsifying meter data, and preventing operations.	CCS	[107]
INL	2017	Malware potentially passed between EVs and EVSE.	CHAdeMO	[103]
Boa et al.	2018	Session hijacking, charging repudiation, MITM, DoS, and masquerading attacks.	CCS	[108]
Baker & Martinovic	2019	Eavesdrop on CCS charging sessions with radiated side-channel.	CCS	[101]
Dudek et al.	2019	Developed V2G Injector software to read and write CCS HPGP data allowing the theft of network keys and injection of data through replay or MITM attacks.	CCS	[105]
Rohde	2019	DCFC charging disruptions when EVSE HMI or EV is compromised and falsifies battery SOC.	CHAdeMO	[134]
Dudek	2021	Injected a Log4Shell payload in a CCS HPGP charging session.	CCS	[106]
Köhler et al.	2022	“Brokenwire” wireless/RF attack terminates CCS charging session(s) using an antenna and Software Defined Radio.	CCS	[102]

Table 2. EV operator interface vulnerabilities.

Researchers	Year	Vulnerability Description	Interface	Citation
Friedland	2016	Insecure authorization mechanisms for EVSE operators.	RFID, smart phone, and MIFARE Classic	[113]
Dalheimer	2017	RFID card cloning to falsify billing account.	RFID	[112]
INL	2018	Poorly secured smart phone apps used to manage customer charging sessions.	iOS and Android apps	[115]
Wright & Street	2019	Credit card skimmers on EVSE.	Card swipes	[114]

Table 3. EVSE internet interface vulnerabilities.

Researchers	Year	Vulnerability Description	Interface	Citation
Shezef	2013	Open configuration web server running on EVSE.	EVSE web server	[96]
Friedland	2016	Network traversal with OCPP.	EVSE/cloud	[113]
Dalheimer	2017	Interception of RFID, credit card, or other near-field-communication (NFC) data.	EVSE/cloud	[112]
Alcaraz et al.	2017	OCPP MITM vulnerabilities.	EVSE/cloud	[90]
INL	2018	Unauthorized access to configuration files and data via insecure web servers, flat EVSE networking, inappropriate authentication methods, insecure FTP firmware server, XSS, etc.	EVSE web server, cloud	[115]
Kaspersky Lab	2018	Buffer overflow in web server Common Gateway Interface.	EVSE web server	[121]
Castro	2018	View or exfiltrate software information, statuses, and critical setup information.	Internet	[124]
Hille & Allhoff	2018	Vulnerable services running on an EVSE that could be accessible from the mobile network interface.	Internet/HTTPS port	[125]
Rubio et al.	2018	OCPP MITM vulnerabilities.	EVSE/Cloud	[128]
Pen Test Partners	2021	Unauthenticated APIs, insecure direct object API references, account hijacking, insecure firmware update mechanisms, exposed OCPI endpoint.	Cloud, EVSE web servers	[116]
Nasr et al.	2021	Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), Server-Side Request Forgery (SSRF), and information exposure.	EVSE web server	[118,120]
Varriale, Crawford, & Jaynes.	2021	EVSE chargers on public internet with unnecessary/outdated services, weak credentials, or missing login timeout functions.	Open ports & services	[88]

Table 4. EVSE maintenance interface vulnerabilities.

Researchers	Year	Vulnerability Description	Interface	Citation
Dalheimer	2017	Exfiltration of logs and configuration data (OCPP credentials, authentication tokens) via USB.	USB ports	[112]
INL	2018	Weak hashing, insecure bootloaders, firmware modification, JTAG interfaces allowed direct control of the processor, etc.	Various	[115]
Kaspersky Lab	2018	Factory reset using special blinking pattern.	Photodiode	[121]
Pen Test Partners	2021	Extraction of credentials and other data from EVSE.	Memory	[116]
Schneider Electric	2021	Hard-coded credentials, improper cryptographic signatures verification, insecure password hashing, etc.	Operating system	[118,120]

4. Impacts

Calculating cybersecurity risk is challenging because this depends on equipment, customer interaction mechanisms, interconnectivity to other systems, and, in the case of power system impacts, the location and power levels of impacted installations. The primary consequence of concern involves EVSE and EV functionality and safety, personal and corporate privacy, financial operations, and electric grid operations. Negative outcomes include theft of energy, creation of hazards to people and equipment proximate to EVSE, disablement and damage to vehicles, and interference with grid functions. Here, we break down the impacts into functional, financial/privacy, safety, and grid impact areas. In all cases, consumer confidence could be damaged if news of EVSE malfunctions or risks are exposed, potentially impacting EV and EV charging markets. A summary of the impacts is provided in Table 5.

4.1. Functional Impacts

As reported by many cybersecurity researchers, cyberattacks can disable a single EVSE device, EVSE fleets, or all vendor-owned devices. As more of the transportation sector is electrified, wide-spread disruptions to EVSE run the risk of severely impacting a range of critical infrastructure: emergency and medical services, food and agriculture, manufacturing, defense, etc. INL reflected on the potential impacts of the Level 2 EVSE vulnerabilities and noted that in the case of malicious remote firmware updates, they could disable all chargers [115]. They were also able to falsify the SOC from the vehicle and the EVSE, which could prevent full charging of the vehicle (“denial-of-charging”) [134], which would delay driving or prevent the driver from reaching their destination. This type of SOC falsification attack could also potentially result in harmful and dangerous overcharging of the battery [135] if it were not for the battery management system safety features in the EV.

4.2. Financial/Privacy Impacts

Unauthorized access to EVSE devices or backend management systems could result in personally identifiable information (PII) data theft; billing falsification (e.g., free charging); or compromise of payment data (e.g., credit and debit card numbers) [112,136]. The impact of these events would affect EVSE operators and EV drivers in potentially significant ways (i.e., identity theft). As demonstrated by the Pen Test Partners research, another risk of insecure EVSE devices is corporate espionage, because insecure devices may expose corporate networks to adversaries that can then steal sensitive software or data [116].

4.3. Safety Impacts

There are safety systems present in the EV and EVSE that prevent overcurrent events, overcharging batteries, and other dangerous consequences. Redundant safety systems on each side of the charging session are designed to prevent fires, battery damage, and other electrical safety issues, such as energizing terminals when the connector is unplugged; for example, INL attempted to overcharge an EV after gaining access to a DCFC EVSE, but the EV stopped the charging event [134]. However, this risk remains if the EV-to-EVSE critical communications are compromised or the safety systems on both devices are disabled. Sagstetter et al. believed that CHAdeMO presented an attack vector to vehicle battery operations if the IEC 61851 CANbus messages were not filtered on the vehicle-side of the connection [137].

DCFC and XFC devices include thermal management systems for internal cooling. The high-amperage cables are liquid-cooled [138,139]. Wireless Power Transfer (WPT) EVSE technologies [140] are also expected to appear on the market at some point which will open new safety concerns. For instance, INL noted potential the safety risks to medical devices from WPT in their consequence analysis [141]. Full control of the device through a malicious firmware update, privilege escalation, or other attacks would potentially allow an attacker to disable networked, safety-critical protections on EVSE.

4.4. Power System Impacts

Over the last decade, there has been significant interest in the impact of EV charging on power system operations [142–146]. More recently, however, researchers have been studying how the malicious control of EVSE equipment could lead to power system maloperation. At the device level, INL disrupted the coordination between power electronic modules, produced a total harmonic distortion of >20%, and decreased the power factor to below 0.8 [134]. They were also able to conduct an emergency stop via the same method that produced a 50 kW to 0.3 kW drop in 0.020 s. Others note that cyberattacks on charging infrastructure may impact power markets [147]. For instance, Alcaraz et al. note that MITM OCPP attacks may be used for energy theft, fraud, or, at the aggregated level, disrupting power operations or generator scheduling and economic dispatch [90].

Others investigated the impact of coordinated load manipulation on distribution and transmission systems [148,149]. Using high-wattage devices to disrupt power system operations is theoretically possible with enough controllable load [150], though this would need to be a significant change in the EVSE charging load. Khan et al. studied the impact of an EV botnet on the IEEE 33-bus distribution network and an IEEE 39-bus transmission model. They found that the coordinated charging of EVs with fifty 50 kW FCDCs located on two distribution buses would exceed distribution load limits and produce a <0.95 pu undervoltage violation [151]. They also found that a 5% increase in transmission load would overload lines, tripping them offline, but a 10% increase in transmission load would trigger an outage. At the distribution level, Deb et al. noted that EV charging could result in increased peak-load demand, reduced reserve margins, voltage instability, and reliability problems [152]. Johnson et al. found that 2.25 MW of EVSE load at the end of a feeder was insufficient to cause voltages outside of ANSI C84.1 [153] Range A, unless V2G grid-support functionality was also included [154]. At the bulk system level, a discrete 8.6 GW of EV load drop (estimated to be the 2028 peak load) in a >20,000-bus Western Interconnect simulation resulted in relatively small generator (~30 MW) and load (466 MW) losses, and no stability impact to the bulk electric system [154]. Morrison estimated that an under-frequency load shedding event could be triggered if simultaneous charging occurred on ~600,000 EVSE in California [155].

There is also a potential risk of dynamic load modulation on power system stability [156]. In an analytical study of Manhattan, Acharya et al. found it improbable that an attacker could manipulate the bulk power-system frequency any time soon, but they determined that if the total EVSE load increased by 692 times current levels and an attacker could control EVSE load controller gains, an attack would theoretically be able to push the grid frequency above 62 Hz for 0.16 s [157]. A study of EVSE load manipulation on inter-area oscillation in the Western Interconnect found that 500 MW oscillating load had no significant adverse effects (no tripped generation or significant system-wide cascading outages) [154]. Nasr et al. also studied impacts from EV V2G operations and cyclic loads on a 315 MW 9-bus Western System Coordinating Council (WSCC) PowerWorld model [120]. They found that a 7.2 MW demand increase would cause the frequency to drop below 59.5 Hz; injecting 51.7 MW of power would lead to the frequency exceeding 60.5 Hz; and alternating between the two would exacerbate the frequency deviation.

Table 5. Summary of potential EVSE cyberattack impacts.

Researchers	Attack Scenario	Impact	Citation
INL	Disable chargers with malicious firmware update	EV operators cannot charge which impacts emergency and medical services, food and agriculture, manufacturing, defense, etc.	[115]
Rohde	Falsify the SOC at EVSE either directly or via the EV	Delay driving or prevent driver from reaching destinations; localized power maloperation.	[134]

Table 5. *Cont.*

Researchers	Attack Scenario	Impact	Citation
Sagstetter et al.	Inject malicious CANbus messages to vehicle via CHAdeMO connection	Damage vehicle batteries by manipulating Battery Management System (BMS) functions.	[137]
Dalheimer; Portela et al.	Unauthorized access to EVSE devices or backend management systems	PII data theft, billing falsification (e.g., free charging), or compromise of payment data.	[87,106]
Pen Test Partners	Exposed private or corporate networks	Corporate espionage, or theft of sensitive software, information, or data.	[116]
Carlson	Malicious firmware update, privilege escalation, and other attacks	Disable thermal management, WPT safety systems, or other safety-critical protections.	[141]
Alcaraz et al.; Ahmed & Dow	OCPP MITM attack; backend system compromise; malicious firmware update	Power market disruptions affecting generator scheduling and economic dispatch.	[90,147]
Khan et al.	EV botnet manipulated the load of multiple 50 kW DCFCs	Distribution undervoltage violations with 2.5 MW of load; outage with 10% load increase.	[151]
Johnson et al.	Transmission load drop and load modulation attack	Minimal loss of generation and load. Bulk system stability was maintained.	[154]
Johnson et al.	EVSE V2G control miscoordination that produced active and reactive power flows	Minimal. Distribution voltage outside of ANSI Range A at end of feeder.	[154]
Morrison	Simultaneous charging of ~600,000 EVSE in California	Under-frequency load shedding event.	[155]
Acharya et al.	Attacker could control EVSE load controller gains	Grid frequency above 62 Hz for 0.16 s, tripping distributed generation.	[157]

5. Cybersecurity Defenses and Hardening Recommendations

While the areas of OT cybersecurity protection, detection, and response are extensively studied for cloud systems [158–160]; SCADA systems [161–164]; smart grids and power systems [165–167]; and autonomous and plug-in EVs [135,168,169], there has been less attention to EVSE device and network hardening. That said, there have been multiple recent efforts to establish EV charging cybersecurity requirements. One major activity led by the U.S. DOT Volpe National Transportation Systems Center for the National Motor Freight Traffic Association created an extensive list of requirements for XFC stations for medium and heavy duty vehicles [30]. The requirements were created by stakeholders, including federal agencies, electric truck OEMs, charging station vendors, and utilities in areas that included design, logging, lifecycle and governance, cryptography, communication, assurance, hardening, resiliency, and secure operation—all mapped to specific threats and methods in the STRIDE security model for attestation.

A major component of the EU Architecture for Multi-criticality Agile Dependable Evolutionary Open System-of-Systems (AMADEOS) project involved bringing together Dutch grid operators (Enexis, Liander, and Stedin), ElaadNL, and the European Network for Cybersecurity (ENCS) to produce multiple reference documents which covered risk assessments [98], security architectures [170], procurement and security requirements for EV charging infrastructure [171], and a security test plan for EV charging stations [172]. Another ElaadNL-commissioned ENCS threat report established security requirements covering design considerations, product lifecycle and governance, cryptography, communications, system hardening, resilience, access control, and logging [35]. In a separate report from Technische Universiteit Eindhoven and Radboud Universiteit Nijmegen, the authors included recommendations for design, implementation, infrastructure, and incident issues [173]. They also noted the need for sharing EVSE cybersecurity knowledge and creating an independent organization that is responsible for security testing and assurance. The following subsections provide recommendations and research efforts to harden EVSE equipment, sorted into the four attack vector categories. A summary of the hardening recommendations is provided in Table 6.

5.1. EV-to-EVSE Interface Hardening Recommendations

Baker and Martinovic suggest a few improvements to prevent the remote sideband CCS data extraction they demonstrated. These included adding chokes and electromagnetic shielding to reduce leakage, improving the HPGP key distribution mechanism, and adding new Signal-Level Attenuation Characterization (SLAC) initialization steps to better secure CCS communications if the PKI system is unavailable [101]. Köhler et al. recommended that CCS sessions re-authenticate after disruptions to minimize the impact on customers [102].

Researchers have also designed multiple security improvements to the EV-to-EVSE communications system. Chan and Zhou created a cyber–physical challenge-response mechanism for J1772 authentication [174]. Vaidya and Mouftah recommended using Multimodal and Multi-pass Authentication (MMA) mechanisms to prevent MITM and substitution attacks on ISO 15118 communications [175].

INL developed Diagnostic Security Modules (DSM) to provide EV-to-Building security based on prior work on coprocessor-based intrusion detection systems [176]. The DSMs were designed to be integrated with the EV, EVSE, and Building Energy Management Systems (BEMS) so that suspicious or abnormal behavior could be reported to BEMS operators, who would allow/deny charging based on security snapshots (fingerprints) of the EV [103,177]. Fingerprints for the EV were derived from internal CANbus messaging; monitoring changes to Electronic Control Units (ECUs); and SAE J1772, CHAdeMO, or CCS vehicle-to-EVSE communications. EVSE fingerprints were calculated from kernel memory, CPU load and memory use, network bandwidth, and operating system statistics using Joint Test Action Group (JTAG) and Serial ports on the EVSE components [103,177].

In the DigiCert, ChargePoint, and Eonti whitepaper [129], they made several recommendations to improve the Plug-and-Charge PKI security of ISO 15118-2. They suggested creating a certificate policy for all V2G root hierarchies, improving the certificate revocation policies, creating key management and subscriber onboarding requirements, and establishing a certificate lifecycle management policy, including EV provisioning. The whitepaper argued that the ISO 15118-2 standard alone is not sufficient to address all the requirements for an operational PKI system, and the U.S. needs operational guidance and a formal certificate policy—similar to the content in the German Verband der Elektrotechnik, Elektronik und Informationstechnik (VDE) Guide, VDE-AR-E 2802-100-1 [178], and Hubject PnC Certificate Policy [179]. To address this gap, the SAE International Cooperative Research Program started the Electric Vehicle Charging Public Key Infrastructure project, which will have Eonti, DigiCert, and VerSprite design, test, and deploy an EV Ecosystem PKI solution [180–182].

In addition, modifications to ISO 15118 have been proposed by the research community. Fuchs and a team at the Fraunhofer Institute for Secure Information Technology designed a Security Module (SecMod) Protection Profile for ISO 15118 EV-EVSE communications to support the security functions in the communication protocol [183,184]. The module provided cryptographic primitives, secure key and credential generation and storage, and random number generation to provide secure boot, remote attestation, and secure firmware update processes. Lee et al. offered several suggestions to improve ISO 15118 and EV-EVSE communications, including additional authentication mechanisms, confirming message validity with anomaly detection tools, and using a third-party auditor to thwart collusion between the EV and EVSE which would prevent untracked charging [107]. Höfer et al. offered ISO 15118 protocol extensions that would provide greater privacy [111] and Bao et al. recommended adding clock synchronization, EV OCSP checks within the EVSE, and mandatory TLS encryption [108].

5.2. EV Operator Interface Hardening Recommendations

User authentication mechanisms have proved to be weak, with many researchers demonstrating RFID cloning and other privacy risks. To combat these problems, van Eekelen et al. recommend stronger authentication of customer identity through Lamport's login, challenge-response pairs based on a secret key, diversified keys, or RFIDs with private keys that are tied to a PKI [173]. After Mathias Dalheimer noted the insecurity of RFID and other nearfield authorization technologies [112], Mültin recommended moving toward ISO 15118 and associated PnC identification mechanisms [185]. ElaadNL provided user authentication requirements that included using a challenge-response protocol, mandating authentication prior to accepting user tokens, and using Secure Access Modules for keys, especially if they are shared master EVSE keys [35].

Nasr et al. exposed a large range of security vulnerabilities that were associated with EVSE firmware, mobile applications, and online web-portals. Their recommendations included suggestions to address issues with EVSE webservers and apps, such as hard-coded credentials, SQL injection, and hard-coded credentials for these user interfaces [120].

5.3. EVSE Internet Hardening Recommendations

To better secure EVSE internet interfaces, many researchers have recommended providing stronger encryption and TLS technologies. Van Eekelen et al. suggested end-to-end encryption to provide meter, billing, and charging data integrity and greater confidentiality based on NISTIR 7628 guidance on cryptography and key management [173,186]. Rubio et al. recommended adding additional IEC 62351-3 TLS profiles, IEC 62351-7 endpoint security, and IEC 62351-8 role-based access control (RBAC) security mechanisms to OCPP and the endpoint devices to defend against MITM attacks [128]. Several recommendations were provided by the Dutch Software Improvement Group regarding the Open Smart Charging Protocol (OSCP), including adding data-centric security and establishing a publish/subscribe middleware model [173]. Van Aubel et al. recommended an extension to ISO 15118, OCPP, and OCPI to provide secrecy and nonrepudiation at the individual data field level [187]. On the other hand, Vaidya and Mouftah recommended using a role-based access control system on the OCPP Control Center server [188] and Zhou et al. presented a decentralized V2G energy trading framework to secure transactions [189].

Recommendations from INL for securing remote management systems included using TLS, making username/password combinations unique for each EVSE device, improving mobile APIs, and securing sessions with a signed certificate [115]. Many researchers have commented on the need for code-signing firmware updates [115,116,173,190]. Nasr et al. recommended a number of implementation improvements, such as addressing XSS and SSRF with the sanitization of user input data; SQL and CSV injection attacks with parametrized queries and safe CSV parsing; CSRF with random tokens for all requests; DoS attacks with rate limited queries; Cross-Origin Resource Sharing (CORS); and Flash Cross-Domain Policy (FCDP) misconfigurations with strict cross-domain policies, and other information disclosure risks with authentication on all endpoints and functions [120].

Other work has been conducted in network-based intrusion detection systems. Moroson and Pop introduced a neural network that was trained on six months of data to detect malicious OCPP traffic [191]. INL has developed a safety instrumented system (SIS) intrusion detection framework to monitor EV charger operations and properties [141]. Pratt and Carol and Eekelen et al. also point to the need for logging, security monitoring, and incident response planning [149,173].

5.4. EVSE Maintenance Interface and Hardware/Software Hardening Recommendations

The National Renewable Energy Laboratory (NREL) enumerated a number of risk mitigation techniques and potential procurements requirements to secure physical access and remote access to EVSE [190]. In their recommendations, they suggest encrypting data-at-rest and data-in-flight with 256-bit cipher suites, removing all external ports, adding tamper alarms, and certifying cloud services with the Federal Risk and Authorization

Management Program (FedRAMP). These recommendations aligned with prior suggestions from ElaadNL who point out requirements for device hardening, removing unneeded interfaces, securing accounts, and physical security protections [173].

Gottumukkala et al. suggested enhancing EVSE security with secure-by-design principals, software security, hardware security, and tamper monitoring and resistance [192]. To this end, in a VTO-funded project, EPRI investigated a Secure Network Interface Card (S-NIC) which wrapped EVSE subsystem communications and included secure boot and tamper resistant technologies [193]. Additionally, privacy-preserving technologies for V2G applications have been studied to prevent the compromise of vehicle identity and location information [194–196].

In many cases, EVSE vulnerability disclosures are accompanied with suggestions that would prevent exploits in the future. For example, in INL's Level 2 EVSE assessment report, they provide an extensive list of local hardening recommendations, including removing physical and logical assess to the device, auditing code, adding secure bootloaders, removing hard-coded passwords, securing firmware updates, and securing inter-process communications and shared memory [115]. Pen Test Partners discussed the risks of using Raspberry Pi computers in EVSE devices and recommended upgrading to computers with secure boot capabilities [116].

Table 6. EVSE cybersecurity defense technologies.

Organization/Researchers	Cybersecurity Hardening Suggestions, Technologies, or Topics	Citation
Höfer et al., 2013	Add protocol extensions to provide greater privacy to ISO 15118.	[111]
Chan and Zhou, 2014	Cyber–physical challenge-response charging authentication.	[174]
Lee et al., 2014	Harden ISO 15118 with additional authentication mechanisms, confirming message validity, and using a third-party auditor to thwart EV-EVSE collusion.	[107]
Chan & Zhou, 2014	Add cyber–physical challenge-response mechanism for J1772 authentication.	[174]
Eekelen et al., 2014	Recommendations for design, implementation, infrastructure, and incident issues; stronger authentication of customer identity; end-to-end encryption; add data-centric security and publish/subscribe middleware to OSCP.	[173]
ElaadNL, 2016	Design, cryptography, communications, system hardening, resilience, access control, logging, product lifecycle, governance, assurance.	[35]
Moroson & Pop, 2017	Neural network trained to detect malicious OCPP traffic.	[190]
INL, 2017 and 2018	Deploy intrusion detection systems to allow/deny charging based on EV security fingerprints.	[103,177]
Bao et al., 2018	Add clock synchronization, EV OCSP checks within the EVSE, and mandatory TLS encryption to ISO 15118.	[108]
Mültin, 2018	Move to PnC identification mechanisms to avoid the insecurity of RFID and other nearfield authorization technologies.	[185]
Rubio et al., 2018	Adding IEC 62351 TLS profiles, endpoint security, and role-based access control (RBAC) security mechanisms to OCPP.	[128]
Vaidya & Mouftah, 2018	Use a role-based access control system on the OCPP Control Center server.	[188]
INL, 2018	Use TLS, code signing, unique username/password combinations, improve mobile APIs, and securing sessions with a signed certificate.	[115]

Table 6. *Cont.*

Organization/Researchers	Cybersecurity Hardening Suggestions, Technologies, or Topics	Citation
NREL, 2019	Encrypt data-at-rest and data-in-flight, remove external ports, add tamper alarms, and certify cloud services with FedRAMP.	[12]
ElaadNL, 2019	Access control, cryptography, communications, physical/information, operational (backup, logging, vulnerability management) security.	[170,171]
U.S. DOT Volpe Center, 2019	Collection of XFC requirements: design, logging, cryptography, communication, assurance, hardening, resiliency, secure operation, etc.	[30]
Van Aubel et al., 2019	Use extensions to ISO 15118, OCPP, and OCPI to provide secrecy and nonrepudiation at the individual data field level.	[187]
Baker & Martinovic, 2019	Prevent remote sideband CCS data extraction via electromagnetic shielding; improve HPGP key distribution; add new SLAC initialization steps.	[101]
DigiCert, ChargePoint, and Eonti, 2019	Create certificate policy for all V2G root hierarchies, improve certificate revocation policies, create key management requirements, etc.	[129]
Gottumukkala et al., 2019	Use secure-by-design principals, software security, hardware security, and tamper monitoring and resistance.	[191]
Fuchs et al., 2019; Fuchs et al., 2020	Use Security Module (SecMod) Protection Profile to support the security functions in the ISO 15118 communication protocol.	[183,184]
Vaidya & Mouftah, 2020	Employ ISO 15118 Multimodal and Multi-pass Authentication mechanisms.	[175]
Zhou et al., 2020	V2G blockchain energy trading framework for secure transactions.	[189]
Carlson, 2021	Monitor EV charger operations with intrusion detection framework.	[141]
Sandia, 2021	Broad cyber recommendations for business and EVSE network and operations, EVSE physical and logical interfaces, and EVSE ecosystem.	[154]
Ghatikar, 2021	Secure Network Interface Card (S-NIC) with secure boot and tamper resistant technologies.	[192]

Yang et al., 2011;
Liu et al., 2014;
He et al., 2014;
Chen et al., 2021
	Privacy-preserving technologies for V2G applications.	[193–196]

Köhler et al., 2022	Reduce the risk and impact of aborting CCS charging sessions with RF shielding and enabling re-authentication.	[102]

6. Discussion

Industrial control system cybersecurity involves the never-ending process of identifying and improving system weaknesses. Vulnerability research is a critical tool in demonstrating the state-of-the-art and profound need for EVSE security. As evidenced by the extensive collection of vulnerabilities in Section 3, EVSE manufacturers and network operators should establish robust cybersecurity programs. These programs will enable manufacturers and operators to continuously mitigate the risks to the EV charging ecosystem. Maintaining an active community of ethical hackers working to identify weaknesses in the EV chargers will help to safeguard EVSE systems against malicious adversaries. The responsible disclosure model provides benefits to both vendors and researchers: discovered vulnerabilities are reported to the appropriate organization for mediation and later shared with the research community to better secure EV charging systems in the future.

If unabated, the risks are significant. EVSE cyberattacks can impact multiple critical infrastructure systems, including transportation, power grid, and medical services. Adversary control of EVSE may also compromise the safety of the basic functionality of the devices, leaving the user stranded or injured. Since billing and personally identifiable information also traverses these devices and networks, personal or corporate financial damage is possible.

As presented here, many recommendations for hardening and defending EVSE devices and networks have been proposed for equipment hardware, user interfaces, and communication protocols. These must be carefully considered by standards development organizations and EVSE vendors and network operators to improve the security of EVSE assets. The only chance of securing EVSE systems is to respond to the evolving threat landscape with continuously improving defensive postures. To that end, several major technical trends and research opportunities can be identified for each of the interfaces, as shown in Table 7. For the EV-to-EVSE interface, there is a need for better identity management and authentication. For the EV operator interface, solutions to privacy loss are needed. Wired, wireless, cellular, or other connections to the internet require security solutions to protect firmware updates, PII, and EVSE control points. New anomaly detection tools would be particularly useful to detect adversary actions on these connections as well. At the maintenance level, EVSE equipment physical and logical access must be monitored, protected, and detected. The operating system, applications, and system data must also be secured appropriately to prevent the manipulation of EVSE operations.

Table 7. Major Cybersecurity research needs for EVSE interfaces.

Interface	Research Areas
EV-to-EVSE	• Techniques to prevent loss or manipulation of charging communications via side-channel attacks. • Improved authentication and authorization mechanisms for EV and EVSE equipment, including those established with PKIs.
EV Operator	• New privacy-preserving authentication solutions for EVs and EV operators. • Improved EVSE credential, data, and PII storage. • Hardened and sanitized local web services.
EVSE Internet	• Communication solutions with end-to-end confidentiality, integrity, authentication, authorization, non-repudiation, and auditing. • Novel EVSE firmware update mechanisms that account for key/certificate provisioning and storage. • EVSE network-based intrusion detection and mitigation systems. • Cloud, website, and API security solutions that prevent manipulation or information disclosure with authentication on all endpoint operations.
EVSE Maintenance	• Host-based intrusion detection systems and tamper-resistant technologies for physical and logical access. • Device-level security features, including secure storage, secure bootloaders, and other software/hardware hardening technologies.

7. Conclusions

EVSE security is essential to maintain critical mobility, shipping, and power system operations as the transportation industry is further electrified. This survey investigated public EVSE device and system cybersecurity vulnerabilities, impacts, and security recommendations. In the last decade, several vulnerabilities were found in EV-to-EVSE, EV operator, internet/cellular/cloud, and maintenance interfaces which represent significant risks to EV operator privacy, operator safety, financial systems, and power system operations.

Fortunately, several new guides, best practices, security technologies, and implementation recommendations have been proposed to address EV charging weaknesses. The cybersecurity research community, EVSE industry, and other stakeholders must continue to work together to implement practical and future-looking security solutions to address gaps in the security posture of the ecosystem. EVSE vendors must incorporate continuous processes for hardening their infrastructure through internal and external assessments and bug-bounty programs. Future research should include expanding the scope and depth of EVSE penetration testing, developing EVSE-tailored network- and host-based intrusion detection systems, incorporating zero-trust principles, and further exploring power, safety, and other impacts. Lastly, at the policy level, state and federal governments should seek legislation to improve the security of EVSE systems by creating EVSE cybersecurity requirements, expanding information sharing programs, and establishing incident-response strategies—especially in cases of coordinated or widespread attacks.

Author Contributions: Conceptualization, J.J.; methodology, J.J.; formal analysis, J.J.; investigation, J.J., T.B., B.A. and B.W.; resources, J.J. and T.B.; data curation, J.J.; writing—original draft preparation, J.J. and T.B.; writing—review and editing, J.J., T.B., B.A. and B.W.; supervision, J.J.; project administration, J.J.; funding acquisition, J.J. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the U.S. Department of Energy (DOE) Vehicle Technologies Office (VTO) "Securing Vehicle Charging Infrastructure" project under Grant #34819.

Acknowledgments: The authors wish to acknowledge their research partners, Lori Ross O'Neil, Tom Carroll, and Rick Pratt at Pacific Northwest National Laboratory, and Roland Varriale at Argonne National Laboratory for discussing the topics covered in this review. Sandia National Laboratories is a multimission laboratory managed and operated by the National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

References

1. Strauss, M. Deployment of EU Electric Vehicle Charging Stations Too Slow, Auditors Say. Available online: https://www.reuters.com/article/us-eu-autos-electric-charging/deployment-of-eu-electric-vehicle-charging-stations-too-slow-auditors-say-idUSKBN2C023C (accessed on 23 May 2022).
2. Brown, A.; Lommele, S.; Schayowitz, A.; Klotz, E. *Electric Vehicle Charging Infrastructure Trends from the Alternative Fueling Station Locator: Fourth Quarter 2020*; National Renewable Energy Laboratory: Golden, CO, USA, 2020.
3. The White House FACT SHEET: Biden Administration Advances Electric Vehicle Charging Infrastructure. Available online: https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/22/fact-sheet-biden-administration-advances-electric-vehicle-charging-infrastructure/ (accessed on 23 May 2022).
4. Halvorson, B. Infrastructure Bill: $7.5B toward Nationwide Network of 500,000 EV Chargers. Available online: https://www.greencarreports.com/news/1134092_infrastructure-bill-7-5b-toward-nationwide-network-of-500-000-ev-chargers (accessed on 15 November 2021).
5. Geotab. *Electric Vehicle Trends in 2020: Top 6 Factors Impacting Fleet Electrification*; Geotab: Oakville, ON, Canada, 2020.
6. Chehab, N. Pump up the Charge with Extreme Fast Charging. Available online: https://www.energy.gov/eere/articles/pump-charge-extreme-fast-charging (accessed on 17 October 2021).
7. NMFTA. *Medium and Heavy Duty Electric Vehicle and Charging Infrastructure Cyber Security Baseline Reference Document*; NMFTA: Alexandria, VA, USA, 2018.
8. CharIN Starts Development of Fast Charging Beyond 1 MW. Available online: https://insideevs.com/news/343058/charin-starts-development-of-fast-charging-beyond-1-mw/ (accessed on 4 October 2021).
9. CHARIN Megawatt Charging System (MCS). Available online: https://www.charin.global/technology/mcs/ (accessed on 17 October 2021).
10. Hoover, Z.; Nägele, F.; Polymeneas, E.; Sahdev, S. *How Charging in Buildings Can Power up the Electric-Vehicle Industry*; McKinsey: Chicago, IL, USA, 2021.
11. Pless, S.; Allen, A.; Myers, L.; Goldwasser, D.; Meintz, A.; Polly, B.; Frank, S. *Integrating Electric Vehicle Charging Infrastructure into Commercial Buildings and Mixed-Use Communities: Design, Modeling, and Control Optimization Opportunities*; National Renewable Energy Laboratory: Golden, CO, USA, 2020.
12. Hodge, C.; Hauck, K.; Gupta, S.; Bennett, J.; Hodge, C.; Hauck, K.; Gupta, S.; Bennett, J. *Vehicle Cybersecurity Threats and Mitigation Approaches*; National Renewable Energy Laboratory: Golden, CO, USA, 2019; pp. 1–41.
13. Burkacky, O.; Deichmann, J.; Klein, B.; Pototzky, K.; Scherf, G. *Cybersecurity in Automotive-Mastering the Challenge*; McKinsey: Chicago, IL, USA, 2020.

14. Kim, K.; Kim, J.S.; Jeong, S.; Park, J.H.; Kim, H.K. Cybersecurity for Autonomous Vehicles: Review of Attacks and Defense. *Comput. Secur.* **2021**, *103*, 102150. [CrossRef]
15. About—AVCC—The Autonomous Vehicle Computing Consortium, Inc. Available online: https://www.avcconsortium.org/about/ (accessed on 14 October 2021).
16. Beer, I. An IOS Zero-Click Radio Proximity Exploit Odyssey. Available online: https://googleprojectzero.blogspot.com/2020/12/an-ios-zero-click-radio-proximity.html (accessed on 23 May 2022).
17. Warminsky, J. *An IOS Exploit That Enables IPhone Takeover Is Cybersecurity Researcher's "Work of Art"*; CyberScoop: Washington, DC, USA, 2020.
18. Upstream Security. *Global Automotive Cybersecurity Report 2021*; Upstream Security: Herzliya, Israel, 2021.
19. Francillon, A.; Danev, B.; 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), San Diego, CA, USA, 24–28 April 2022.
20. Indesteege, S.; Keller, N.; Dunkelman, O.; Biham, E.; Preneel, B. A Practical Attack on KeeLoq. In *Advances in Cryptology—EUROCRYPT 2008, Proceedings of the 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Istanbul, Turkey, 13–17 April 2008*; LNCS; Springer: Berlin/Heidelberg, Germany, 2008; Volume 4965, pp. 1–18. [CrossRef]
21. Eisenbarth, T.; Kasper, T.; Moradi, A.; Paar, C.; Salmasizadeh, M.; Shalmani, M.T.M. On the Power of Power Analysis in the Real World: A Complete Break of the KeeLoq Code Hopping Scheme. In *Advances in Cryptology—CRYPTO 2008, Proceedings of the 28th Annual International Cryptology Conference, Santa Barbara, CA, USA, 17–21 August 2008*; LNCS; Springer: Berlin/Heidelberg, Germany, 2008; Volume 5157, pp. 203–220. [CrossRef]
22. Koscher, K.; Czeskis, A.; Roesner, F.; Patel, S.; Kohno, T.; Checkoway, S.; McCoy, D.; Kantor, B.; Anderson, D.; Snachám, H.; et al. Experimental Security Analysis of a Modern Automobile. In Proceedings of the 2010 IEEE Symposium on Security and Privacy, Oakland, CA, USA, 16–19 May 2010; pp. 447–462. [CrossRef]
23. Kawanishi, Y.; Nishihara, H.; Souma, D.; Yoshida, H. Detailed Analysis of Security Evaluation of Automotive Systems Based on JASO TP15002. In *Computer Safety, Reliability, and Security, Proceedings of the SAFECOMP 2017 Workshops, ASSURE, DECSoS, SASSUR, TELERISE, and TIPS, Trento, Italy, 12 September 2017*; LNCS; Springer: Berlin/Heidelberg, Germany, 2017; Volume 10489, pp. 211–224. [CrossRef]
24. Jo, H.J.; Choi, W.; Na, S.Y.; Woo, S.; Lee, D.H. Vulnerabilities of Android OS-Based Telematics System. *Wirel. Pers. Commun.* **2017**, *92*, 1511–1530. [CrossRef]
25. Brooks, R.R.; Sander, S.; Deng, J.; Taiber, J. Automobile Security Concerns: Challenges and State of the Art of Automotive System Security. *IEEE Veh. Technol. Mag.* **2009**, *4*, 53–64. [CrossRef]
26. Crane, C. 15 Auto Dealership Cybersecurity Statistics That Will Drive You to Action. Available online: https://cybersecurityventures.com/15-auto-dealership-cybersecurity-statistics-that-will-drive-you-to-action/ (accessed on 14 October 2021).
27. Pagliery, J. Cars Can Be Hacked by Their Tiny, Plug-in Insurance Discount Trackers. Available online: https://money.cnn.com/2015/08/11/technology/car-hacking-tracker/index.html (accessed on 14 October 2021).
28. Basmadjian, R. Communication Vulnerabilities in Electric Mobility HCP Systems: A Semi-Quantitative Analysis. *Smart Cities 2* **2021**, *4*, 405–428. [CrossRef]
29. Mustafa, M.A.; Zhang, N.; Kalogridis, G.; Fan, Z. Smart Electric Vehicle Charging: Security Analysis. In Proceedings of the 2013 IEEE PES Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 24–27 February 2013. [CrossRef]
30. NMFTA. *Extreme Fast Charging (XFC) Cybersecurity Threats, Use Cases and Requirements For Medium and Heavy Duty Electric Vehicles*; NMFTA: Alexandria, VA, USA, 2019.
31. Harnett, K.; Watson, G.; Brown, G. *Government Fleet and Public Sector Electric Vehicle Supply Equipment (EVSE) Cybersecurity Best Practices and Procurement Language Report*; Volpe National Transportation Systems Center: Cambridge, MA, USA, 2019.
32. Harnett, K.; Harris, B.; Chin, D.; Watson, G. *DOE/DHS/DOT Volpe Technical Meeting on Electric Vehicle and Charging Station Cybersecurity Report*; Volpe National Transportation Systems Center: Cambridge, MA, USA, 2018.
33. D'Anna, G. *Cybersecurity for Commercial Vehicles*; SAE International: Warrendale, PA, USA, 2018; ISBN 978-0-7680-9258-5.
34. Islam, M.; Chowdhury, M.; Li, H.; Hu, H. Cybersecurity Attacks in Vehicle-to-Infrastructure Applications and Their Prevention. *Transp. Res. Rec.* **2018**, *2672*, 66–78. [CrossRef]
35. European Network for Cybersecurity. *EV Charging Systems Security Requirements*; European Network for Cyber Security: Den Haag, The Netherlands, 2016.
36. Metere, R.; Neaimeh, M.; Morisset, C.; Maple, C.; Bellekens, X.; Czekster, R.M. Securing the Electric Vehicle Charging Infrastructure. *arXiv* **2021**, arXiv:2105.02905.
37. Johnson, J. *Securing Vehicle Charging Infrastructure*; Sandia National Laboratory: Albuquerque, NM, USA, 2020.
38. Advice Letter (AL) Suspension Notice: Southern California Edison Company's Workplan and Work Schedule for a Cybersecurity Gap Analysis of Electric Vehicle Charging Equipment Products Used in Transportation Electrification Programs. Available online: https://docs.cpuc.ca.gov/PublishedDocs/Published/G000/M388/K664/388664705.docx (accessed on 15 November 2021).
39. Publications: CC Portal. Available online: https://www.commoncriteriaportal.org/cc/ (accessed on 22 November 2021).
40. Barrett, M.P. *Framework for Improving Critical Infrastructure Cybersecurity, version 1.1*; NIST: Gaithersburg, MD, USA, 2018.
41. The STRIDE Threat Model. Available online: https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)?redirectedfrom=MSDN (accessed on 22 November 2021).
42. Understanding IEC 62443. Available online: https://www.iec.ch/blog/understanding-iec-62443 (accessed on 4 November 2021).

43. NIST SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations. Available online: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final (accessed on 22 November 2021).
44. ISO/IEC 15408-1:2009. Information Technology—Security Techniques—Evaluation Criteria for IT Security—Part 1: Introduction and General Model. Available online: https://www.iso.org/standard/50341.html (accessed on 22 November 2021).
45. MITRE ATT&CK®. Available online: https://attack.mitre.org/ (accessed on 22 November 2021).
46. Macher, G.; Armengaud, E.; Brenner, E.; Kreiner, C. Threat and Risk Assessment Methodologies in the Automotive Domain. *Procedia Comput. Sci.* **2016**, *83*, 1288–1294. [CrossRef]
47. *ISO 26262-1*; Road Vehicles—Functional Safety—Part 1: Vocabulary. ISO: Geneva, Switzerland, 2018.
48. Olsson, M.; Lautenbach, A.; Islam, M.; Sandberg, C.; Bokesand, A.; Olovsson, T.; Kleberger, P.; Söderberg-Rivkin, A.; Kadhirvelan, S.P.; Hansson, A.; et al. *HEAVENS-HEAling Vulnerabilities to ENhance Software Security and Safety, Version 2.0*; The HEAVENS Consortium (Borås SE): Vinnova, Sweden, 2016.
49. National Highway Traffic Safety Administration. *Cybersecurity Best Practices for the Safety of Modern Vehicles*; National Highway Traffic Safety Administration: Washington, DC, USA, 2020.
50. Uptane—Securing Software Updates for Automobiles. Available online: https://uptane.github.io/ (accessed on 22 November 2021).
51. *ISO/SAE 21434*; Road Vehicles—Cybersecurity Engineering. ISO: Geneva, Switzerland, 2021.
52. Auto-ISAC Best Practices Guides. Available online: https://automotiveisac.com/best-practices/ (accessed on 22 November 2021).
53. *UN Regulation No. 155—Uniform Provisions Concerning the Approval of Vehicles with Regards to Cyber Security and Cyber Security Management System*; Rev.3 Add. 154; UNECE: Geneva, Switzerland, 2021.
54. AUTOSAR—The Standardized Software Framework for Intelligent Mobility. Available online: https://www.autosar.org/ (accessed on 22 November 2021).
55. *JASO TP-15002*; Guideline for Automotive Information Security Analysis, 2016 Edition. Society of Automotive Engineers of Japan (JSAE): Yokohama, Japan, 2016.
56. UL Smart Buildings Cybersecurity. Available online: https://www.ul.com/services/solutions/cybersecurity/smart-buildings-cybersecurity (accessed on 22 November 2021).
57. IEEE 2030–2011. IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads. Available online: https://standards.ieee.org/standard/2030-2011.html (accessed on 22 November 2021).
58. FERC/NERC. Cyber and Grid Security. Available online: https://www.ferc.gov/industries-data/electric/industry-activities/cyber-and-grid-security (accessed on 22 November 2021).
59. Ronanki, D.; Kelkar, A.; Williamson, S.S. Extreme Fast Charging Technology—Prospects to Enhance Sustainable Electric Transportation. *Energies* **2019**, *12*, 3721. [CrossRef]
60. Howell, D.; Boyd, S.; Cunningham, B.; Gillard, S.; Slezak, L.; Ahmed, S.; Bloom, I.; Burnham, A.; Hardy, K.; Jansen, A.N.; et al. *Enabling Fast Charging: A Technology Gap Assessment*; Idaho National Laboratory: Idaho Falls, ID, USA, 2017.
61. *IEC 62196-1*; Ed. 3.0. Plugs, Socket-Outlets, Vehicle Connectors and Vehicle Inlets—Conductive Charging of Electric Vehicles—Part 1: General Requirements. IEC: Geneva, Switzerland, 2014.
62. *IEC 62196-2*; Ed. 2.0. Plugs, Socket-Outlets, Vehicle Connectors and Vehicle Inlets—Conductive Charging of Electric Vehicles—Part 2: Dimensional Compatibility and Interchangeability Requirements for a.c. Pin and Contact-Tube Accessories. IEC: Geneva, Switzerland, 2016.
63. *IEC 62196-3*; Ed 1.0. Plugs, Socket-Outlets, Vehicle Connectors and Vehicle Inlets—Conductive Charging of Electric Vehicles—Part 3: Dimensional Compatibility and Interchangeability Requirements for d.c. and a.c./d.c. Pin and Contact-Tube Vehicle Couplers. IEC: Geneva, Switzerland, 2014.
64. *SAE J1772*; SAE Electric Vehicle and Plug in Hybrid Electric Vehicle Conductive Charge Coupler. SAE International: Warrendale, PA, USA, 2017.
65. *IEC 61851-1*; Ed. 3.0. Electric Vehicle Conductive Charging System—Part 1: General Requirements. IEC: Geneva, Switzerland, 2017.
66. *SAE J3068*; Electric Vehicle Power Transfer System Using a Three-Phase Capable Coupler. SAE International: Warrendale, PA, USA, 2018.
67. *JEVS G105*; Japan Electric Vehicle Standard (JEVS) Connector for Eco Station Rapid EV Charging System. Japan Automobile Research Institute (JARI): Tsukuba, Japan, 1993.
68. *CHAdeMO 1.0.1*; Technical Specifications of Quick Charger for the Electric Vehicle. CHAdeMO Association: Tokyo, Japan, 2013.
69. Technology Overview—CHAdeMO Association. Available online: https://www.chademo.com/technology/technology-overview/ (accessed on 4 November 2021).
70. *IEEE 2030.1.1*; Standard Technical Specifications of a DC Quick Charger for Use with Electric Vehicles. IEEE: New York, NY, USA, 2016.
71. *ISO 11898-1*; Road Vehicles—Controller Area Network (CAN)—Part 1: Data Link Layer and Physical Signalling Technical Corrigendum. ISO: Geneva, Switzerland, 2015.
72. *ISO 15118-1:2019*; Road Vehicles—Vehicle to Grid Communication Interface—Part 1: General Information and Use-Case Definition. ISO: Geneva, Switzerland, 2019.
73. *HomePlug Green PHY*; The Standard For In-Home Smart Grid Powerline Communications. HomePlug Powerline Alliance: Portland, OR, USA, 2010.

74. *SAE J2411_200002*; Ground Vehicle Standard—Single Wire CAN Network for Vehicle Applications. SAE International: Warrendale, PA, USA, 2000.
75. The National Standard of The People's Republic of China Connection Set of Conductive Charging for Electric Vehicles—Part I: General Requirements. European Electrical and Electronics Industry: Beijing, China, 2011.
76. *SAE J1939*; Standards Collection—Hybrid and Electric Vehicle Communications. SAE International: Warrendale, PA, USA, 2021.
77. Wyglinski, A.M.; Huang, X.; Padir, T.; Lai, L.; Eisenbarth, T.R.; Venkatasubramanian, K. Security of Autonomous Systems Employing Embedded Computing and Sensors. *IEEE Micro* **2013**, *33*, 80–86. [CrossRef]
78. Argyropoulos, N.; Khodashenas, P.S.; Mavropoulos, O.; Karapistoli, E.; Lytos, A.; Karypidis, P.A.; Hofmann, K.P. Addressing Cybersecurity in the Next Generation Mobility Ecosystem with CARAMEL. *Transp. Res. Procedia* **2021**, *52*, 307–314. [CrossRef]
79. Vassallo, E.W.; Manaugh, K. Spatially Clustered Autonomous Vehicle Malware: Producing New Urban Geographies of Inequity. *Transp. Res. Rec.* **2018**, *2672*, 66–75. [CrossRef]
80. Amoozadeh, M.; Raghuramu, A.; Chuah, C.N.; Ghosal, D.; Michael Zhang, H.; Rowe, J.; Levitt, K. Security Vulnerabilities of Connected Vehicle Streams and Their Impact on Cooperative Driving. *IEEE Commun. Mag.* **2015**, *53*, 126–132. [CrossRef]
81. *ISO/FDIS 15118-20*; Road Vehicles—Vehicle to Grid Communication Interface—Part 20: 2nd Generation Network Layer and Application Layer Requirements Ed1 (under Development). ISO: Geneva, Switzerland, 2020.
82. Open Charge Point Protocol (OCPP) 2.0.1. Available online: https://www.openchargealliance.org/protocols/ocpp-201/ (accessed on 4 November 2021).
83. Open Charge Alliance. Open Smart Charging Protocol (OSCP) 2.0. Available online: https://www.openchargealliance.org/protocols/oscp-20/ (accessed on 23 May 2022).
84. *IEEE 2030.5*; IEEE Standard for Smart Energy Profile Application Protocol. IEEE: New York, NY, USA, 2018.
85. *OpenADR 2.0*; Profile Specification B Profile. Openadr Alliance: Morgan Hill, CA, USA, 2015.
86. *MQTT Version 5.0*; OASIS Standard—Message Queuing Telemetry Transport. OASIS: Burlington, MA, USA, 2019.
87. ASHRAE 135-2020 (ANSI Approved) Standard—BACnet—A Data Communication Protocol for Bulding Automation and Control Networks. Available online: https://www.techstreet.com/ashrae/standards/ashrae-135-2020?product_id=2191852 (accessed on 4 November 2021).
88. Varriale, R.; Crawford, R.; Jaynes, M. Risks of Electric Vehicle Supply Equipment Integration within Building Energy Management System Environments: A Look at Remote Attack Surface and Implications. In Proceedings of the National Cyber Summit (NCS) Research Track 2021, Huntsville, AL, USA, 28–30 September 2021; pp. 163–173. [CrossRef]
89. Myers, E.H. *A Comprehensive Guide to Electric Vehicle Managed Charging*; Smart Electric Power Alliance: Washington, DC, USA, 2019.
90. Alcaraz, C.; Lopez, J.; Wolthusen, S. OCPP Protocol: Security Threats and Challenges. *IEEE Trans. Smart Grid* **2017**, *8*, 2452–2459. [CrossRef]
91. Anderson, B.R.; Johnson, J.T. Securing Vehicle Charging Infrastructure Against Cybersecurity Threats. In Proceedings of the SAE Hybrid and Electric Vehicle Technologies Symposium, Pasadena, CA, USA, 28–30 January 2020.
92. Anderson, B.; Johnson, J. Securing Vehicle Charging Infrastructure. In Proceedings of the 2021 DOE Vehicle Technologies Office Annual Merit Review, Washington, DC, USA, 21–25 June 2021.
93. Reeh, D.; Cruz Tapia, F.; Chung, Y.W.; Khaki, B.; Chu, C.; Gadh, R. Vulnerability Analysis and Risk Assessment of EV Charging System under Cyber-Physical Threats. In Proceedings of the 2019 IEEE Transportation Electrification Conference and Expo (ITEC), Detroit, MI, USA, 19–21 June 2019. [CrossRef]
94. Acharya, S.; Dvorkin, Y.; Pandzic, H.; Karri, R. Cybersecurity of Smart Electric Vehicle Charging: A Power Grid Perspective. *IEEE Access* **2020**, *8*, 214434–214453. [CrossRef]
95. Fries, S.; Falk, R. Securely Connecting Electric Vehicles to the Smart Grid. *Int. J. Adv. Internet Technol.* **2013**, *6*, 57–67.
96. Shezaf, O. Who Can Hack a Plug? The Infosec Risks of Charging Electric Cars. In Proceedings of the Hack in the Box, Amsterdam, The Netherlands, 10–11 April 2013.
97. Van Keulen, J. Smart Charging: A Privacy and Security Analysis, Radboud Universiteit. Bachelor's Thesis, Radboud Universiteit, Nijmegen, The Netherlands, 2014.
98. ElaadNL. *EV Charging Systems Security Threats*; European Network for Cyber Security: Den Haag, The Netherlands, 2016.
99. Basnet, M.; Ali, M.H. Exploring Cybersecurity Issues in 5G Enabled Electric Vehicle Charging Station with Deep Learning. *IET Gener. Transm. Distrib.* **2021**, *15*, 3435–3449. [CrossRef]
100. *DIN SPEC 70121*; 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. German Institute for Standardisation: Berlin, Germany, 2014.
101. Baker, R.; Martinovic, I. Losing the Car Keys: Wireless PHY-Layer Insecurity in EV Charging. In Proceedings of the 28th USENIX Security Symposium (USENIX Security 19), Santa Clara, CA, USA, 14–16 August 2019; pp. 407–424.
102. Köhler, S.; Baker, R.; Strohmeier, M.; Martinovic, I. Brokenwire: Wireless Disruption of CCS Electric Vehicle Charging. *arXiv* **2022**, arXiv:2202.02104.
103. Rohde, K. Electric Vehicle Cyber Research. In Proceedings of the DOE FEMP Energy Exchange, Tampa, FL, USA, 16 August 2017.
104. Rohde, K. A Distributed Auto Charger Attack On The Grid. In Proceedings of the S4, Miami, FL, USA, 9 April 2019.
105. Dudek, S.; Delaunay, J.-C.; Fargues, V. V2G Injector: Whispering to Cars and Charging Units through the Power-Line. In Proceedings of the SSTIC (Symposium sur la sécurité des technologies de l'information et des communications), Rennes, France, 5–7 June 2019.

106. Dudek, S. Examining Log4j Vulnerabilities in Connected Cars and Charging Stations. Available online: https://www.trendmicro.com/en_us/research/21/l/examining-log4j-vulnerabilities-in-connected-cars.html (accessed on 20 January 2022).
107. Lee, S.; Park, Y.; Lim, H.; Shon, T. Study on Analysis of Security Vulnerabilities and Countermeasures in Iso/Iec 15118 Based Electric Vehicle Charging Technology. In Proceedings of the 2014 International Conference on IT Convergence and Security (ICITCS), Beijing, China, 28–30 October 2014. [CrossRef]
108. Bao, K.; Valev, H.; Wagner, M.; Schmeck, H. A Threat Analysis of the Vehicle-to-Grid Charging Protocol ISO 15118. *Comput. Sci.-Res. Dev.* **2018**, *33*, 3–12. [CrossRef]
109. Falk, R.; Fries, S. Electric Vehicle Charging Infrastructure—Security Considerations and Approaches. In Proceedings of the The Fourth International Conference on Evolving Internet—INTERNET, Venice, Italy, 24–29 June 2012; Volume 2131.
110. Klapwijk, P.; Driessen-Mutters, L. *Exploring the Public Key Infrastructure for ISO 15118 in the EV Charging Ecosystem*; ElaadNL: Arnhem, The Netherlands, 2018.
111. Höfer, C.; Petit, J.; Schmidt, R.; Kargl, F. POPCORN: Privacy-Preserving Charging for Emobility. In Proceedings of the 2013 ACM Workshop on Security, Privacy & Dependability for Cyber Vehicles, Berlin, Germany, 4 November 2013; pp. 37–48. [CrossRef]
112. Dalheimer, M. Ladeinfrastruktur Für Elektroautos: Ausbau Statt Sicherheit (Charging Infrastructure for Electric Cars: Expansion Instead of Security). In Proceedings of the 34th Chaos Communication Congress, Leipzig, Germany, 27–30 December 2017.
113. Friedland, A. Security and Privacy in the Current E-Mobility Charging Infrastructure. In Proceedings of the DeepSec, Vienna, Austria, 31 July 2016.
114. Wright, A.C.; Street, J.E. Charging in the Crosshairs: How EV Drivers Could Become Cyber Criminals' New Target. 2019. Available online: https://www.digitalcitizensalliance.org/clientuploads/pdf/Charging_in_the_Crosshairs.pdf (accessed on 23 May 2022).
115. *Cyber Security Research and Development: Cyber Assessment Report of Level 2 AC Powered Electric Vehicle Supply Equipment*; INL Technical Report INL/MIS-18-45521; INL: Hong Kong, China, 2018.
116. Smart Car Chargers. Plug-n-Play for Hackers? | Pen Test Partners. Available online: https://www.pentestpartners.com/security-blog/smart-car-chargers-plug-n-play-for-hackers/ (accessed on 4 August 2021).
117. CISOMAG Schneider Electric Patches 13 Vulnerabilities Affecting Its EVlink Charging Stations. Available online: https://cisomag.eccouncil.org/schneider-electric-vulnerabilities-fixed/ (accessed on 27 July 2021).
118. Schneider Electric Security Notification: EVlink City/Parking/Smart Wallbox Charging Stations. 2021. Available online: https://www.se.com/au/en/download/document/SEVD-2021-194-06/ (accessed on 23 May 2022).
119. Bannister, A. Schneider Electric Fixes Critical Vulnerabilities in EVlink Electric Vehicle Charging Stations. Available online: https://portswigger.net/daily-swig/schneider-electric-fixes-critical-vulnerabilities-in-evlink-electric-vehicle-charging-stations (accessed on 27 July 2021).
120. Nasr, T.; Torabi, S.; Bou-Harb, E.; Fachkha, C.; Assi, C. Power Jacking Your Station: In-Depth Security Analysis of Electric Vehicle Charging Station Management Systems. *Comput. Secur.* **2022**, *112*, 102511. [CrossRef]
121. Sklyar, D. ChargePoint Home Security Research. 2018. Available online: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/12/13084354/ChargePoint-Home-security-research_final.pdf (accessed on 23 May 2022).
122. Remotely Controlled EV Home Chargers—The Threats and Vulnerabilities. Available online: https://securelist.com/remotely-controlled-ev-home-chargers-the-threats-and-vulnerabilities/89251/ (accessed on 29 September 2021).
123. CIRCONTROL CirCarLife 2018 Vulnerabilities Are Not Fixed Yet. Available online: https://www.aegislab.com/news/2019/11/18/circarlife-vulnerability/ (accessed on 29 September 2021).
124. CirCarLife SCADA 4.3.0. Credential Disclosure—Hardware Webapps Exploit. Available online: https://www.exploit-db.com/exploits/45384 (accessed on 29 September 2021).
125. Christinan, H.; Manuel, A. EV Charging: Mapping out the Cyber Security Threats and Solutions for Grids and Charging Infrastructure. In Proceedings of the 4th Annual UtiliNet Europe Event, Brussels, Belgium, 15–17 May 2018.
126. Open Charge Point Interface. Available online: https://evroaming.org/ (accessed on 29 September 2021).
127. Expert from Fraunhofer ITWM Uncovers Security Vulnerabilities of Charging Stations. Available online: https://www.fraunhofer.de/en/press/research-news/2018/January/security-vulnerabilities-of-charching-stations.html (accessed on 29 September 2021).
128. Rubio, J.E.; Alcaraz, C.; Lopez, J. Addressing Security in OCPP: Protection Against Man-in-The-Middle Attacks. In Proceedings of the 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Paris, France, 26–28 February 2018. [CrossRef]
129. Practical Considerations for Implementation and Scaling ISO 15118 into a Secure EV Charging Ecosystem. 2019. Available online: https://www.chargepoint.com/files/15118whitepaper.pdf (accessed on 23 May 2022).
130. Jewers, C. Russian Motorway's Electric Vehicle Chargers Are Hacked to Display Message Supporting Ukraine | Daily Mail Online. Available online: https://www.dailymail.co.uk/news/article-10565697/Russian-electric-vehicle-chargers-hacked-display-message-supporting-Ukraine.html (accessed on 14 April 2022).
131. Gordon, A. Russian Electric Vehicle Chargers Hacked, Tell Users 'PUTIN IS A DICKHEAD'. Available online: https://www.vice.com/en/article/akvya5/russian-electric-vehicle-chargers-hacked-tell-users-putin-is-a-dickhead (accessed on 14 April 2022).
132. Security Flaws Found in Popular EV Chargers—TechCrunch. Available online: https://techcrunch.com/2021/08/03/security-flaws-found-in-popular-ev-chargers/amp/ (accessed on 4 August 2021).

133. Pen Test Partners Pwning a Smart Car Charger, Building a Botnet. Available online: https://www.pentestpartners.com/security-blog/pwning-a-smart-car-charger-building-a-botnet/ (accessed on 1 April 2022).
134. Rohde, K. Cyber Security of DC Fast Charging: Potential Impacts to the Electric Grid. In Proceedings of the S4x19, Miami, FL, USA, 14–17 January 2019.
135. Dey, S.; Khanra, M. Cybersecurity of Plug-In Electric Vehicles: Cyberattack Detection during Charging. *IEEE Trans. Ind. Electron.* **2021**, *68*, 478–487. [CrossRef]
136. Portela, C.M.; Geldtmeijer, D.; Slootweg, H.; Van Eekelen, M. A Flexible and Privacy Friendly ICT Architecture for Smart Charging of EVS. In Proceedings of the 22nd International Conference and Exhibition on Electricity Distribution (CIRED 2013), Stockholm, Sweden, 10–13 June 2013. [CrossRef]
137. Sagstetter, F.; Lukasiewycz, M.; Steinhors, S.; Wolf, M.; Bouard, A.; Harris, W.R.; Jha, S.; Peyrin, T.; Poschmann, A.; Chakraborty, S. Security Challenges in Automotive Hardware/Software Architecture Design. In Proceedings of the 2013 Design, Automation & Test in Europe Conference & Exhibition (DATE), Grenoble, France, 18–22 March 2013; pp. 458–463. [CrossRef]
138. Tesla Patents New Liquid-Cooled Charging Connector—Electrek. Available online: https://electrek.co/2019/09/30/tesla-patents-liquid-cooled-charging-connector/ (accessed on 28 October 2021).
139. Yoshida, M.D. *CHAdeMO for the Future*; CHAdeMO Association: Tokyo, Japan, 2018.
140. Brecher, A.; Arthur, D. *Review and Evaluation of Wireless Power Transfer (WPT) for Electric Transit Applications*; John A. Volpe National Transportation Systems Center (U.S.): Cambridge, MA, USA, 2014.
141. Carlson, R. Consequence-Driven Cybersecurity for High-Power EV Charging Infrastructure DOE Vehicle Technologies Program Annual Merit Review. In Proceedings of the DOE Vehicle Technologies Program Annual Merit Review, Washington, DC, USA, 24 June 2021.
142. Jiang, Z.; Shalalfeh, L.; Beshir, M.J. Impact of Electric Vehicle Infrastructure on the City of Chatsworth Distribution System. In Proceedings of the 2014 IEEE International Electric Vehicle Conference (IEVC), Florence, Italy, 17–19 December 2014. [CrossRef]
143. Jiang, Z.; Shalalfel, L.; Beshir, M.J. Impact of Electric Vehicles on the IEEE 34 Node Distribution Infrastructure. *Int. J. Smart Grid Clean Energy* **2014**, *3*, 417–424. [CrossRef]
144. Scoffield, D.; Smart, J.; Pennington, T.; Jones, C.; Lave, M.; Medam, A.; Mitra, B. Strategies to Maintain Voltage on Long, Lightly Loaded Feeders with Widespread Residential Level 2 Plug-in Electric Vehicle Charging. In Proceedings of the IEEE Transportation Electrification Conference & Expo 2021, Chicago, IL, USA, 23–25 June 2021.
145. Jones, C.B.; Lave, M.; Vining, W.; Garcia, B.M. Uncontrolled Electric Vehicle Charging Impacts on Distribution Electric Power Systems with Primarily Residential, Commercial or Industrial Loads. *Energies* **2021**, *14*, 1688. [CrossRef]
146. Mousavian, S.; Erol-Kantarci, M.; Wu, L.; Ortmeyer, T. A Risk-Based Optimization Model for Electric Vehicle Infrastructure Response to Cyber Attacks. *IEEE Trans. Smart Grid* **2018**, *9*, 6160–6169. [CrossRef]
147. Ahmed, S.; Dow, F.M. Electric Vehicle Technology as an Exploit for Cyber Attacks on the next Generation of Electric Power Systems. In Proceedings of the 2016 4th International Conference on Control Engineering & Information Technology (CEIT), Hammamet, Tunisia, 16–18 December 2016. [CrossRef]
148. Dvorkin, Y.; Garg, S. IoT-Enabled Distributed Cyber-Attacks on Transmission and Distribution Grids. In Proceedings of the 2017 North American Power Symposium (NAPS), Morgantown, WV, USA, 17–19 September 2017. [CrossRef]
149. Pratt, R.M.; Carroll, T.E. Vehicle Charging Infrastructure Security. In Proceedings of the 2019 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 11–13 January 2019. [CrossRef]
150. Soltan, S.; Mittal, P.; Poor, H.V. BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid. In Proceedings of the 27th USENIX Security Symposium (USENIX Security 18), Baltimore, MD, USA, 15–17 August 2018; pp. 15–32.
151. Khan, O.G.M.; El-Saadany, E.; Youssef, A.; Shaaban, M. Impact of Electric Vehicles Botnets on the Power Grid. In Proceedings of the 2019 IEEE Electrical Power and Energy Conference (EPEC), Montreal, QC, Canada, 16–18 October 2019. [CrossRef]
152. Deb, S.; Tammi, K.; Kalita, K.; Mahanta, P. Impact of Electric Vehicle Charging Station Load on Distribution Network. *Energies* **2018**, *11*, 178. [CrossRef]
153. *ANSI C84.1-2016*; American National Standard for Electric Power Systems and Equipment—Voltage Ratings (60 Hertz). ANSI: Rosslyn, VA, USA, 2016.
154. Johnson, J.; Anderson, B.; Wright, B.; Graves, R.; Daley, J.; Quiroz, J.; Pratt, R.; Carroll, T.; O'Neil, L.R.; Dindlebeck, B.; et al. *Securing Electric Vehicle Charging Infrastructure—Final Report*; Sandia National Laboratory: Albuquerque, NM, USA, 2021.
155. Morrison, G. Threats and Mitigation of DDoS Cyberattacks Against the U.S. Power Grid via EV Charging. Ph.D. Thesis, Wright State University, Dayton, OH, USA, 2018.
156. Amini, S.; Pasqualetti, F.; Mohsenian-Rad, H. Dynamic Load Altering Attacks Against Power System Stability: Attack Models and Protection Schemes. *IEEE Trans. Smart Grid* **2018**, *9*, 2862–2872. [CrossRef]
157. Acharya, S.; Dvorkin, Y.; Karri, R. Public Plug-in Electric Vehicles + Grid Data: Is a New Cyberattack Vector Viable? *IEEE Trans. Smart Grid* **2020**, *11*, 5099–5113. [CrossRef]
158. Sajid, A.; Abbas, H.; Saleem, K. Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges. *IEEE Access* **2016**, *4*, 1375–1384. [CrossRef]
159. Zhou, M.; Zhang, R.; Xie, W.; Qian, W.; Zhou, A. Security and Privacy in Cloud Computing: A Survey. In Proceedings of the 2010 Sixth International Conference on Semantics, Knowledge and Grids, Beijing, China, 1–3 November 2010; pp. 105–112. [CrossRef]
160. Lombardi, F.; Di Pietro, R. Secure Virtualization for Cloud Computing. *J. Netw. Comput. Appl.* **2011**, *34*, 1113–1122. [CrossRef]

161. Bhamare, D.; Zolanvari, M.; Erbad, A.; Jain, R.; Khan, K.; Meskin, N. Cybersecurity for Industrial Control Systems: A Survey. *Comput. Secur.* **2020**, *89*, 101677. [CrossRef]
162. Maglaras, L.A.; Jiang, J. Intrusion Detection in SCADA Systems Using Machine Learning Techniques. In Proceedings of the 2014 Science and Information Conference, London, UK, 27–29 August 2014; pp. 626–631. [CrossRef]
163. Nicholson, A.; Webber, S.; Dyer, S.; Patel, T.; Janicke, H. SCADA Security in the Light of Cyber-Warfare. *Comput. Secur.* **2012**, *31*, 418–436. [CrossRef]
164. Chandia, R.; Gonzalez, J.; Kilpatrick, T.; Papa, M.; Shenoi, S. Security Strategies for SCADA Networks. *IFIP Int. Fed. Inf. Process.* **2007**, *253*, 117–131. [CrossRef]
165. Wang, W.; Lu, Z. Cyber Security in the Smart Grid: Survey and Challenges. *Comput. Netw.* **2013**, *57*, 1344–1371. [CrossRef]
166. Chen, B.; Yim, S., II; Kim, H.; Kondabathini, A.; Nuqui, R. Cybersecurity of Wide Area Monitoring, Protection, and Control Systems for HVDC Applications. *IEEE Trans. Power Syst.* **2021**, *36*, 592–602. [CrossRef]
167. Duan, N.; Yee, N.; Salazar, B.; Joo, J.Y.; Stewart, E.; Cortez, E. Cybersecurity Analysis of Distribution Grid Operation with Distributed Energy Resources via Co-Simulation. In Proceedings of the 2020 IEEE Power & Energy Society General Meeting (PESGM), Montreal, QC, Canada, 2–6 August 2020. [CrossRef]
168. Smith, C. *The Car Hacker's Handbook: A Guide for the Penetration Tester*; No Starch Press: San Francisco, CA, USA, 2016. [CrossRef]
169. Sharma, S.; Kaul, A. A Survey on Intrusion Detection Systems and Honeypot Based Proactive Security Mechanisms in VANETs and VANET Cloud. *Veh. Commun.* **2018**, *12*, 138–164. [CrossRef]
170. ElaadNL. *Security Architecture for Electric Vehicle Charging Infrastructure*, version 1.0; European Network for Cyber Security: Den Haag, The Netherlands, 2019.
171. ElaadNL. *Security Requirements for Procuring EV Charging Stations*, version 2.0; European Network for Cyber Security: Den Haag, The Netherlands, 2019.
172. ElaadNL. *Security Test Plan for EV Charging Stations*, version 1.0; European Network for Cyber Security: Den Haag, The Netherlands, 2019.
173. van Eekelen, M.; Poll, E.; Hubbers, E.; Vieira, B.; van den Broek, F. *An End-to-End Security Design for Smart EV-Charging for Enexis and ElaadNL*; ElaadNL: Arnhem, The Netherlands, 2014.
174. Chan, A.C.F.; Zhou, J. Cyber-Physical Device Authentication for the Smart Grid Electric Vehicle Ecosystem. *IEEE J. Sel. Areas Commun.* **2014**, *32*, 1509–1517. [CrossRef]
175. Vaidya, B.; Mouftah, H.T. Multimodal and Multi-Pass Authentication Mechanisms for Electric Vehicle Charging Networks. In Proceedings of the 2020 International Wireless Communications and Mobile Computing (IWCMC), Limassol, Cyprus, 15–19 June 2020; pp. 371–376. [CrossRef]
176. Zhang, X.; Van Doorn, L.; Jaeger, T.; Perez, R.; Sailer, R. Secure Coprocessor-Based Intrusion Detection. In Proceedings of the 10th Workshop on ACM SIGOPS European Workshop, Saint-Emilion, France, 1 July 2002; pp. 239–242. [CrossRef]
177. Rohde, K. Grid Modernization Laboratory Consortium: Diagnostic Security Modules for Electric Vehicle-to-Building Integration (163). In Proceedings of the DOE Peer Review, Arlington, VA, USA, 21 June 2018.
178. *VDE-AR-E 2802-100-1*; Handling of Certificates for Electric Vehicles, Charging Infrastructure and Backend Systems within the Framework of ISO 15118. VDE: Frankfurt am Main, Germany, 2019.
179. *Hubject Plug&Charge Certificate Policy for the Hubject ISO 15118 V2G PKI*; Hubject GmbH: Berlin, Germany, 2019.
180. Brooke, L. SAE Kicks off Project to Develop Cyber-Secure EV Charging. Available online: https://www.sae.org/news/2020/09/sae-pki-secure-ev-charging-project (accessed on 6 October 2021).
181. SAE International to Launch Industry-Driven SAE EV Charging Public Key Infrastructure Project. Available online: https://www.sae.org/news/press-room/2020/05/sae-international-to-launch-industry-driven-sae-ev-charging-public-key-infrastructure-project (accessed on 6 October 2021).
182. SAE International Hires World-Class Contractor Team for EV Charging Public Key Infrastructure Cooperative Research Project. Available online: https://www.sae.org/news/press-room/2021/02/sae-international-hires-world-class-contractor-team-for-ev-charging-public-key-infrastructure-cooperative-research-project (accessed on 6 October 2021).
183. Fuchs, A.; Krauss, C.; Lahr, N.; Petri, R. *Security Module for the Electric Vehicle Charging System Proposal for a Protection Profile*; Fraunhofer SIT: Darmstadt, Germany, 2019.
184. Fuchs, A.; Kern, D.; Krauß, C.; Zhdanova, M. TrustEV: Trustworthy Electric Vehicle Charging and Billing. In Proceedings of the the 35th Annual ACM Symposium on Applied Computing, Brno, Czech, 30 March–3 April 2020.
185. Mültin, M. The Case for ISO 15118 and OCPP 2.0: Preventative Solutions to Hacking Charging Infrastructure. Available online: https://www.switch-ev.com/news-and-events/iso15118-mitigates-hacking-charging-infrastructure (accessed on 29 October 2021).
186. The Smart Grid Interoperability Panel-Smart Grid Cybersecurity Committee. *NISTIR 7628 Revision 1: Guidelines for Smart Grid Cybersecurity, Volume 1-Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements*; NIST: Gaithersburg, MD, USA, 2014.
187. Van Aubel, P.; Poll, E.; Rijneveld, J. Non-Repudiation and End-to-End Security for Electric-Vehicle Charging. In Proceedings of the 2019 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe), Bucharest, Romania, 29 September–2 October 2019. [CrossRef]

188. Vaidya, B.; Mouftah, H.T. Deployment of Secure EV Charging System Using Open Charge Point Protocol. In Proceedings of the 2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC), Limassol, Cyprus, 25–29 June 2018; pp. 922–927. [CrossRef]
189. Zhou, Z.; Wang, B.; Dong, M.; Ota, K. Secure and Efficient Vehicle-to-Grid Energy Trading in Cyber Physical Systems: Integration of Blockchain and Edge Computing. *IEEE Trans. Syst. Man, Cybern. Syst.* **2020**, *50*, 43–57. [CrossRef]
190. Morosan, A.G.; Pop, F. OCPP Security—Neural Network for Detecting Malicious Traffic. In Proceedings of the International Conference on Research in Adaptive and Convergent Systems, Krakow, Poland, 20–23 September 2017; pp. 190–195. [CrossRef]
191. Gottumukkala, R.; Merchant, R.; Tauzin, A.; Leon, K.; Roche, A.; Darby, P. Cyber-Physical System Security of Vehicle Charging Stations. In Proceedings of the 2019 IEEE Green Technologies Conference(GreenTech), Lafayette, LA, USA, 3–6 April 2019. [CrossRef]
192. Chhaya, S.; Ghatikar, R. Cybersecurity Platform and Certification Framework Development for EXtreme Fast Charging (XFC) Infrastructure Ecosystem DoE Vehicle Technologies Office Annual Merit Review Presentation, ELT206. In Proceedings of the DOE Vehicle Technologies Office Annual Merit Review, Washington, DC, USA, 24 June 2021.
193. Yang, Z.; Yu, S.; Lou, W.; Liu, C. P2: Privacy-Preserving Communication and Precise Reward Architecture for V2G Networks in Smart Grid. *IEEE Trans. Smart Grid* **2011**, *2*, 697–706. [CrossRef]
194. Liu, H.; Ning, H.; Zhang, Y.; Xiong, Q.; Yang, L.T. Role-Dependent Privacy Preservation for Secure V2g Networks in the Smart Grid. *IEEE Trans. Inf. Forensics Secur.* **2014**, *9*, 208–220. [CrossRef]
195. He, M.; Zhang, K.; Shen, X.S. PMQC: A Privacy-Preserving Multi-Quality Charging Scheme in V2G Network. In Proceedings of the 2014 IEEE Global Communications Conference, Austin, TX, USA, 8–12 December 2014; pp. 675–680. [CrossRef]
196. Chen, L.; Zhou, J.; Chen, Y.; Cao, Z.; Dong, X.; Choo, K.K.R. PADP: Efficient Privacy-Preserving Data Aggregation and Dynamic Pricing for Vehicle-to-Grid Networks. *IEEE Internet Things J.* **2021**, *8*, 7863–7873. [CrossRef]