Electric Vehicle Charger Cybersecurity Vulnerabilities

Subjects: Transportation

Contributor: Jay Johnson, Timothy Berg

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 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.

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

1. Introduction

Potential electric vehicle supply equipment (EVSE) vulnerabilities have been identified through risk and threat modeling efforts, e.g., [1][2][3][4][5][6][7]. 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. The following sections present a survey of EVSE vulnerabilities to better understand the threat landscape for electric vehicle (EV) charging, separated by the four interfaces. Chronological summaries of these vulnerabilities are presented for each of the interfaces in **Table 1**, **Table 2**, **Table 3** and **Table 4**.

2. 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 [8] traffic, using a software defined radio (SDR) [9]. Köhler et al. subsequently showed that charging sessions could be wirelessly aborted by disrupting the PLC communications in their *Brokenwire* attack demonstrations [10]. 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 [11]. 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) [12]. 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 [13]. 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 [14].

The ISO 15118 protocol has garnered extensive security and threat analyses [3][15][16][17]. 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 [15]. Bao et al. had similar concerns of session hijacking; charging repudiation; and machine-in-the-middle (MITM), denial-of-service (DoS), and masquerading attacks [16]. The CCS Plug-and-Charge (PnC) PKI approach and credential management that were defined in ISO 15118-2 [18] 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 [3][17]. 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 [19].

3. 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 [20]. 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 [21]. There have also been warnings about credit card skimmers on EVSE equipment [22].

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 [23]. Many EVSE web service vulnerabilities have also been disclosed; these will be covered in the next section.

4. 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. The vulnerabilities associated with internet communications are presented in this section and can be divided 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.

4.1. 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 [24]. 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 [24]. In the INL assessment, they found unauthorized access to configuration files, and data were provided via insecure wireless web servers [23]. 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 [4].

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 [25][26][27][28]. 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 [28].

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 [29]. 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 [30].

4.2. 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 [31]. 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 [23]. 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 [24]. 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 [32][33].

Hille and Allhoff showed that several vulnerable services running on an EVSE could be accessed from the mobile network interface [34]. 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.

4.3. 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 [23]. 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) [35]. 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 [24].

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 [36]. 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 [21]. 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 [20][21][37]. Rubio et al. further noted the risk of MITM attacks on OCPP [38]. 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 [39].

Supply chain vulnerabilities are also a risk for EV charging operations. During the Russian invasion of Ukraine in early 2022, Россети Электротранспорт (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 [40][41]. This access allowed the component vendor to change the settings in the EVSE devices remotely.

5. 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 [20]. 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 [23]. 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 [29].

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 [24][42][43]. 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 [25][26][27].

Table 1. EV-to-EVSE interface vulnerabilities.

Researchers	Year	Vulnerability Description	Coupler	Citation
Höfer et al.	**2013**	**Credential theft and privacy risks.**	**CCS**	[19]
Lee et al.	**2014**	**EV ID spoofing, power stealing, falsifying meter data, and preventing operations.**	**CCS**	[15]
INL	**2017**	**Malware potentially passed between EVs and EVSE.**	**CHAdeMO**	[11]
Boa et al.	**2018**	**Session hijacking, charging repudiation, MITM, DoS, and masquerading attacks.**	**CCS**	[16]
Baker & Martinovic	**2019**	**Eavesdrop on CCS charging sessions with radiated side-channel.**	**CCS**	[9]
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**	[13]
Rohde	**2019**	**DCFC charging disruptions when EVSE HMI or EV is compromised and falsifies battery SOC.**	**CHAdeMO**	[44]
Dudek	**2021**	**Injected a Log4Shell payload in a CCS HPGP charging session.**	**CCS**	[14]
Köhler et al.	**2022**	**“Brokenwire” wireless/RF attack terminates CCS charging session(s) using an antenna and Software Defined Radio.**	**CCS**	[10]

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**	[21]
Dalheimer	**2017**	**RFID card cloning to falsify billing account.**	**RFID**	[20]
INL	**2018**	**Poorly secured smart phone apps used to manage customer charging sessions.**	**iOS and Android apps**	[23]
Wright & Street	**2019**	**Credit card skimmers on EVSE.**	**Card swipes**	[22]

Table 3. EVSE internet interface vulnerabilities.

Researchers	Year	Vulnerability Description	Interface	Citation
Shezef	2013	Open configuration web server running on EVSE.	EVSE web server	[4]
Friedland	2016	Network traversal with OCPP.	EVSE/cloud	[21]
Dalheimer	2017	Interception of RFID, credit card, or other near-field-communication (NFC) data.	EVSE/cloud	[20]
Alcaraz et al.	2017	OCPP MITM vulnerabilities.	EVSE/cloud	[36]
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	[23]
Kaspersky Lab	2018	Buffer overflow in web server Common Gateway Interface.	EVSE web server	[29]
Castro	2018	View or exfiltrate software information, statuses, and critical setup information.	Internet	[33]
Hille & Allhoff	2018	Vulnerable services running on an EVSE that could be accessible from the mobile network interface.	Internet/HTTPS port	[34]
Rubio et al.	2018	OCPP MITM vulnerabilities.	EVSE/Cloud	[38]
Pen Test Partners	2021	Unauthenticated APIs, insecure direct object API references, account hijacking, insecure firmware update mechanisms, exposed OCPI endpoint.	Cloud, EVSE web servers	[24]
Nasr et al.	2021	Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), Server-Side Request Forgery (SSRF), and information exposure.	EVSE web server	[26][28]
Varriale, Crawford, & Jaynes.	2021	EVSE chargers on public internet with unnecessary/outdated services, weak credentials, or missing login timeout functions.	Open ports & services	[31]

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	[20]
INL	2018	Weak hashing, insecure bootloaders, firmware modification, JTAG interfaces allowed direct control of the processor, etc.	Various	[23]
Kaspersky Lab	2018	Factory reset using special blinking pattern.	Photodiode	[29]
Pen Test Partners	2021	Extraction of credentials and other data from EVSE.	Memory	[24]
Schneider Electric	2021	Hard-coded credentials, improper cryptographic signatures verification, insecure password hashing, etc.	Operating system	[26][28]

References

1. 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.
2. Acharya, S.; Dvorkin, Y.; Pandzic, H.; Karri, R. Cybersecurity of Smart Electric Vehicle Charging: A Power Grid Perspective. IEEE Access 2020, 8, 214434–214453.
3. Fries, S.; Falk, R. Securely Connecting Electric Vehicles to the Smart Grid. Int. J. Adv. Internet Technol. 2013, 6, 57–67.
4. 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.
5. Van Keulen, J. Smart Charging: A Privacy and Security Analysis, Radboud Universiteit. Bachelor's Thesis, Radboud Universiteit, Nijmegen, The Netherlands, 2014.
6. ElaadNL. EV Charging Systems Security Threats; European Network for Cyber Security: Den Haag, The Netherlands, 2016.

7. 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.
8. 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.
9. 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.
10. Köhler, S.; Baker, R.; Strohmeier, M.; Martinovic, I. Brokenwire: Wireless Disruption of CCS Electric Vehicle Charging. arXiv 2022, arXiv:2202.02104.
11. Rohde, K. Electric Vehicle Cyber Research. In Proceedings of the DOE FEMP Energy Exchange, Tampa, FL, USA, 16 August 2017.
12. Rohde, K. A Distributed Auto Charger Attack On The Grid. In Proceedings of the S4, Miami, FL, USA, 9 April 2019.
13. 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.
14. 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).
15. 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.
16. 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.
17. 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.
18. Klapwijk, P.; Driessen-Mutters, L. Exploring the Public Key Infrastructure for ISO 15118 in the EV Charging Ecosystem; ElaadNL: Arnhem, The Netherlands, 2018.
19. 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.
20. 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.
21. Friedland, A. Security and Privacy in the Current E-Mobility Charging Infrastructure. In Proceedings of the DeepSec, Vienna, Austria, 31 July 2016.
22. 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).
23. 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.
24. 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).
25. 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).
26. 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).
27. 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).
28. 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.

29. 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).
30. 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).
31. 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.
32. 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).
33. CirCarLife SCADA 4.3.0. Credential Disclosure—Hardware Webapps Exploit. Available online: https://www.exploit-db.com/exploits/45384 (accessed on 29 September 2021).
34. 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.
35. Open Charge Point Interface. Available online: https://evroaming.org/ (accessed on 29 September 2021).
36. Alcaraz, C.; Lopez, J.; Wolthusen, S. OCPP Protocol: Security Threats and Challenges. IEEE Trans. Smart Grid 2017, 8, 2452–2459.
37. 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).
38. 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.
39. 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).
40. 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).
41. 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).
42. 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).
43. 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).
44. 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.