MitM Cyber Risk Analysis in OCPP enabled EV Charging Stations

Safa Hamdare*, David J.Brown*, Omprakash Kaiwartya*, Yue Cao†, Manish Jugran‡

*Department of Computer Science, Nottingham Trent University, Nottingham, NG11 8NS, UK
† School of Cyber Science and Engineering, Wuhan University, Wuhan, 430072, China
‡JMVL Limited, Jenkins Avenue,Bricket Wood,, St Albans,London, AL2 3SB UK

***Abstract*—The increasing adoption of Electric Vehicle Charging Stations (EVCS) necessitates robust security measures, particularly in the communication protocols used between Charging Point (CP) and EVCS Server (CS). This paper focuses on the vulnerabilities associated with the Open Charge Point Protocol (OCPP), a widely used protocol for EVCS communication. Specifically, we analyze the risks of Man-in-the-Middle (MitM)attack, which exploit weaknesses in OCPP's client and server communication. We implemented a MitM attack on OCPP 1.6, discovering that although it uses TLS 1.2 for encryption, this version is not secure. In the intercepted packets, the information about the cipher suites used by TLS 1.2, session id , server address, application protocols is in plaintext, making the system vulnerable. Our findings underscore the need for enhanced security measures. First and foremost, preventing MitM attacks is crucial. Additionally, if communication is intercepted, using the latest version of TLS and encrypting cipher suite information can further strengthen security. Our analysis is supported by experimental results demonstrating the feasibility of such attacks and their potential consequences.**

***Index Terms*—EVCS, EV charging, Cyber security, Session Hijacking,MITM, OCPP**

I. Introduction

The adoption of Electric Vehicles (EVs) and EVCS has grown rapidly due to their environmental benefits, including reduced greenhouse gas emissions and decreased reliance on fossil fuels [1]. EVs also offer economic advantages, such as lower operating costs and less maintenance compared to traditional internal combustion engine vehicles [2]. EVCS play a critical role in supporting the widespread use of EVs by providing the necessary infrastructure for charging, thereby enabling longer travel distances and enhancing the convenience for EV owners [3].

Despite these benefits, EVCS are vulnerable to various security risks, particularly the communication protocol used to manage interactions between CP and CS [4]. The OCPP is a widely adopted communication standard, designed to ensure interoperability between different manufacturers of charging stations and back-end systems [5]. However, the current versions of OCPP, including OCPP 1.6 and the newer OCPP 2.0.1, have been found to have significant security flaws that can be exploited by malicious actors [6]. These vulnerabilities include weak authentication mechanisms and insufficient data integrity checks, which can lead to unauthorized access and manipulation of the communication channel [7].

OCPP's primary versions, 1.6 and 2.0.1, facilitate communication using either SOAP (Simple Object Access Protocol) or JSON (JavaScript Object Notation) [5]. Despite improvements in version 2.0.1, OCPP 1.6 remains widely used and is particularly susceptible to security threats. OCPP operates by transmitting data bidirectionally through HTTPs or WebSockets, utilizing SOAP or JSON, respectively. Regardless of the transmission format, data is encrypted using TLS 1.2. However, TLS 1.2 has its own vulnerabilities which can be exploited by attackers [8]. Researchers have identified several vulnerabilities in OCPP 1.6, including the potential for Man-in-the-Middle (MitM) attack, which can compromise the security and reliability of EVCS operations [7], [9], [10]. These attacks exploit the protocol's inadequate handling of data transmitted over WebSocket connections. In cases where encrypted data is intercepted, attackers face significant challenges in deciphering the information, but the interception itself still poses risks such as potential disruptions in service [11].

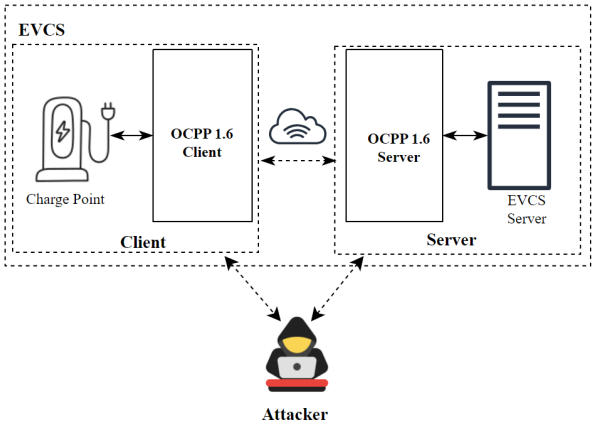

Fig. 1. MitM attack in EVCS using OCPP 1.6

The consequences of MitM attacks on OCPP-based systems are severe. Attackers can intercept and manipulate the data exchanged between the CP and CS, leading to fraudulent charging sessions, denial of service, and even broader impacts on the power grid's stability [11]. Such attacks not only threaten the confidentiality, integrity, and availability of the charging services but also pose significant financial and reputations risks to the stakeholders involved, including EV owners, charging station operators, and energy providers [6], [12]. In light of these security challenges, this paper analyzes the risks associated with MitM in EVCS using the OCPP 1.6 protocol as shown in (Fig.1), to demonstrate the potential communication vulnerabilities that exist between OCPP 1.6 Client and OCPP 1.6 server. Here OCPP 1.6 is utilized to send data through web sockets utilizing JSON. Our findings underscore the necessity for enhanced security measures, including prevention of MitM and robust encryption protocols, to safeguard against these threats and ensure the secure operation of EVCS.

The key contribution of this paper is as follws:

- Analyzed the MitM risks associated with intercepting OCPP 1.6 client-server communication.
- Successfully implemented a MitM attack on OCPP 1.6, highlighting vulnerabilities in client-server communication.
- Identified that OCPP 1.6 uses TLS 1.2 for message encryption, which is vulnerable and requires updating to a more secure TLS version for improved security.

The remainder of this paper is organized as follows: In Section II, a literature review on cyber security issues in OCPP is presented. Section III analyzes the risk of MitM attacks on OCPP 1.6. Section IV presents performance evaluation, including the experimental setup and result analysis. Finally, Section VI concludes the paper with future research directions.

II. Literature Review

The EV charging ecosystem comprises various cyber and physical components, each with its own vulnerabilities. Previous research demonstrated the exploitation of EV charging applications as attack vectors against the power grid [13]. Other studies have highlighted vulnerabilities that could be exploited to manipulate EV charging and affect the power grid [14]. Recent reports indicate that EV charging stations have been actively targeted and exploited. During the Russia-Ukraine conflict, attackers used a manufacturer backdoor to display anti-war messages on Russian EV charging stations and carry out Denial of Service (DoS) attacks [15]. In the United Kingdom, third-party applications on EV charging stations were exploited to display inappropriate images and conduct DoS attacks [16]. Moreover, a security researcher managed to breach an Electrify America EV charging station using TeamViewer, gaining remote control and access [17].

Due to the openness of the OCPP, various studies have explored building on the protocol to enhance EV charging solutions. However, significant security concerns, especially regarding OCPP 1.6, have also been extensively examined. Conti, M. et al. [18] found additional vulnerabilities in the communication between EVs and charging stations. Nasr, T. et al. [19] discussed several critical and high-severity vulnerabilities in existing EV charging management systems, which could lead to remote cyber-attacks. Vaidya and Mouftah [20] introduced SecCharge, a management system aimed at supporting the deployment of charging infrastructure in smart cities. This work also details numerous security issues present in OCPP 1.6 and outlines several security requirements to improve the protocol's security. SaiFlow identified weak authentication policies in OCPP, indicating that connections between CPs and CSs could be disrupted by falsifying additional connections to the CS [21]. Friedland examined potential issues when an attacker gains network access to OCPP 1.6 [22].

Alcaraz et al. [23] investigated security vulnerabilities in OCPP 1.6 that could potentially destabilize the power network. They identified several threats targeting OCPP charge points, including unauthorized access to private messages, data insertion and modification, and data deletion, which could result in denial-of-service attacks. The authors also discussed attacks on the communication channel, such as service and resource interference, and energy theft through credential fraud and pricing model manipulation.Rubio et al. [24] focused on security threats in OCPP 1.6, particularly Man-in-the-Middle (MITM) attacks. They highlighted the consequences of successful MITM attacks, such as compromising user privacy by exposing private data and causing system instability or financial loss through data manipulation. To mitigate MITM attacks, they proposed using the OCPP DataTransfer method to exchange secret data between a charge point and a central system, and provided a JavaScript implementation. Both Alcaraz et al. and Rubio et al. have explored MITM vulnerabilities in OCPP, suggesting that these vulnerabilities could enable fraudulent charging or disrupt power system operations on a large scale [23], [24]. Morosan and Pop [25] proposed a neural network approach for classifying OCPP traffic (i.e., request/response pairs) into malicious and benign categories, enhancing threat detection within the OCPP ecosystem.

These studies collectively enhance our understanding of the cybersecurity landscape of EVCS and underscore the need for robust security measures to protect against identified threats.

III. Analysis of MitM on OCPP 1.6

A. OCPP Attack Model

This paper aims to protect EVCS from MitM attacks targeting the OCPP 1.6. In these attacks, a potential attacker intercepts and possibly alters the communication between the CP and the CS without either party's knowledge. The attacker does this by tapping into the communication link between the CP and the CS, which may use wireless technology. Regardless, OCPP relies on bidirectional data transmission over this link, using HTTPs or Websockets with either SOAP or JSON formats. In our experiment, we have utilized OCPP 1.6 using Websockets with JSON. However, it is crucial to note that, in OCPP version 1.6, the information that is sent between client and server, or vice versa, is currently transmitted in encrypted form using TLS 1.2. The type of encryption used ensures

that even the ”change cipher spec” message is encrypted. This basic level of encryption provided by OCPP 1.6 protects the data from being intercepted, modified, or disrupted by attackers during transmission. However, if a MitM attack is successfully executed, the attacker can intercept the encrypted messages. While these messages are encrypted, sophisticated attacks could potentially decrypt them. Therefore, it is essential to implement measures to prevent MitM attacks in the first place.

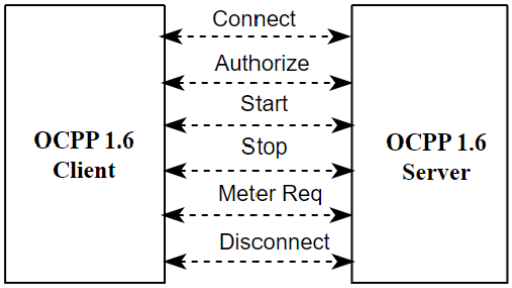

Fig. 2. OCPP Client and Server Communication in EVCS

To illustrate the information that we aim to protect, we must first examine the communication between the OCPP Client (Charge Point) and the OCPP Server (EVCS Charge Server) in an EVCS as defined by the OCPP specification [26]. The communication between the client and server involves various types of messagesas shown in (Fig. 2), to manage the charging process and ensure proper functioning.

Initially, the connection process is initiated by the CP to establish communication with the CS. This begins with a Boot Notification, where the CP sends a message to the CS detailing the CP's status, vendor, model, firmware version, and readiness to operate. The CS responds with a confirmation to accept or reject the connection based on the provided information. Before any charging session can commence, the user must be authorized. The CP sends an Authorize Request to the CS, including the user's identification information, such as user ID. The CS processes this request and responds with an Authorize Response indicating whether the user is permitted to start a charging session. Upon authorization, the Start Transaction process begins. The CP sends a Start Transaction Request to the CS, detailing the user's identifier, the charging point, and the session start timestamp. The CS acknowledges this request with a Start Transaction Response, providing a unique transaction ID to track the session.

To end the charging session, a Stop Transaction Request is sent by the CP to the CS, including the transaction ID, final meter reading, and session end timestamp. The CS confirms the transaction's end with a Stop Transaction Response. During the charging session, the CP periodically sends Meter Value Requests to the CS, reporting the energy consumed with the current meter reading and timestamp. The CS processes and stores this information for future reference or billing. Finally, to close the communication link, a Disconnect Notification is sent by the CP to the CS, indicating the intention to terminate the connection. The CS acknowledges this notification and safely closes the communication session. Understanding these messages is crucial for ensuring their security, as each involves the transmission of potentially sensitive data that must be protected from interception, alteration, and disruption.

B. MitM Attack Analysis on OCPP

In a MitM attack, an attacker intercepts and possibly alters the communication between the CP and the CS. Below, we analyze the data transferred in each message and discuss how an attacker could maliciously use this information if intercepted.

- **Connect (Boot Notification)**
  As shown below, the actual data transformed from CP to CS in Connect request.
  Vulnerable Data: Vendor, model, firmware version, current status of the CP.
  Malicious Use: An attacker could gather detailed information about the hardware and software used by the CP, which can be used for targeted attacks. By understanding the specifics, the attacker might exploit known vulnerabilities in the firmware or hardware.

```
"chargePointVendor":"AVT-Company",
"chargePointModel":"AVT-Express",
"chargePointSerialNum":"avt.001.13.1",
"chargeBoxSerialNum":"avt.001.13.1.01",
"firmwareVersion":"0.9.87",
"iccid": "",
"imsi": "",
"meterType": "AVT NQC-ACDC",
"meterSerialNumber": "avt.001.13.1.01"
```

- **Connect(Boot Notification Response)**
  Vulnerable Data: Confirmation of CP's connection status.
  Malicious Use: If an attacker intercepts and blocks this message, the CP might not be able to establish a connection with the CS, rendering the charging station non-functional. Alternatively, the attacker could send a false response, misleading the CP about its connection status.

```
"status": "Accepted",
"interval": 100,
"currentTime":"2023-09-10T10:36:18.475Z"
```

- **Authorize Request**
  Vulnerable Data: User identification information (user ID).
  Malicious Use: An attacker could capture the user's identification details and use them to impersonate the user, potentially gaining unauthorized access to charging services or user accounts.

```
"idTag":"TAG001"
```

- **Authorize Response**
  Vulnerable Data: Authorization status.
  Malicious Use: Intercepting this message allows an attacker to alter the authorization status. They could deny service to legitimate users by sending a false rejection or allow unauthorized users by sending a false acceptance.

```
"status":"Accepted"
```

- **Start Transaction Request**
  Vulnerable Data: User identifier, charging point ID, timestamp, transaction details.
  Malicious Use: By capturing this information, an attacker could start unauthorized charging sessions. They might also manipulate transaction details, such as altering timestamps or the amount of energy to be delivered, leading to incorrect billing or fraudulent use of services.

```
"connectorId":1,
"idTag":"TAG001",
"timestamp":"2023-09-10T10:38:57.882Z",
"meterStart":0,
"reservationId":16943302990312306
```

- **Start Transaction Response**
  Vulnerable Data: Unique transaction ID, acknowledgment.
  Malicious Use: An attacker could intercept and modify this message to provide a different transaction ID, causing confusion in tracking the session. This might also be used to interrupt or hijack ongoing transactions.

```
"transactionId": 1,
"idTagInfo":{
"status": "Accepted"}
```

- **Meter Value Request**
  Vulnerable Data: Current meter reading, timestamp.
  Malicious Use: An attacker could alter meter readings, causing inaccurate billing or energy tracking. They might also flood the CS with false meter readings, potentially disrupting the system's ability to manage energy usage.

```
"connectorId": 1,
"transactionId": 1,
"meterValue": [{
"timestamp": "2023-09-10T10:38:58.896Z",
"sampledValue":[ {
"value": "0.0049"}
]}]
```

- **Meter Value Response**
  Vulnerable Data: Acknowledgment of meter value.
  Malicious Use: By blocking or altering this message, an attacker could disrupt the communication flow, causing the CP to resend meter values unnecessarily, which could lead to network congestion or data inconsistencies.

```
"status":"Accepted"
```

- **Stop Transaction Request**
  Vulnerable Data: Transaction ID, final meter reading, timestamp.
  Malicious Use: An attacker could manipulate this message to prematurely stop a transaction or alter the final meter reading, resulting in incorrect billing. They could also block this message to prevent the session from ending, causing prolonged charging without proper authorization.

```
"transactionId": 1,
"idTag": "TAG001",
"timestamp":"2023-09-10T10:42:55.021Z",
"meterStop": 1
```

- **Stop Transaction Response**
  Vulnerable Data: Acknowledgment of transaction termination.
  Malicious Use: By intercepting and altering this message, an attacker could make the CP believe the transaction has ended when it has not, or vice versa. This could lead to incorrect logging of sessions and potential disputes between users and operators.

```
"idTagInfo": {
"status": "Accepted"}
```

- **Disconnect Notification**
  Vulnerable Data: Notification of intent to disconnect.
  Malicious Use: An attacker could block or alter this message to keep the CP connected longer than necessary or prematurely disconnect it. This could be used to deny service to legitimate users or disrupt the normal operation of the charging station.

```
"idTagInfo": {
"status": "Disconnect"}
```

- **Disconnect Response**
  Vulnerable Data: Acknowledgment of disconnection.
  Malicious Use: By intercepting and altering this message, an attacker could disrupt the proper disconnection process, potentially causing errors in the system's operation or leading to data loss.

```
"status": "Accepted"
```

To understand the potential impact of a MitM attack on the communication between the CP and CS, we analyzed the different types of messages exchanged. Each message type is assessed for its vulnerability to various attack vectors, such

as interception, modification, impersonation, and denial of service. The following (Table.1) summarizes these vulnerabilities.

TABLE I
OCPP MESSAGES AND THEIR VULNERABILITY TO ATTACK VECTORS

OCPP Message	Interception	Modification	Impersonation	Denial of Service
Boot Notification	✓	✓	✓	✓
Boot Notification Response	✓	✓	✗	✓
Authorize Request	✓	✓	✓	✗
Authorize Response	✓	✓	✗	✓
Start Transaction Request	✓	✓	✓	✗
Start Transaction Response	✓	✓	✗	✓
Meter Value Request	✓	✓	✗	✗
Meter Value Response	✓	✓	✗	✓
Stop Transaction Request	✓	✓	✗	✓
Stop Transaction Response	✓	✓	✗	✓
Disconnect Notification	✓	✓	✗	✓
Disconnect Response	✓	✓	✗	✓

IV. PERFORMANCE EVALUATION

This section provides a description of the experimental setup used to implement the MitM attack on the OCPP 1.6 communication protocol used in EVCS. Additionally, it includes an analysis of the traffic intercepted during the MitM attack in the result analysis section.

A. Experimental Setup

For this proof-of-concept, an Ubuntu VM and a Kali Linux VM are used. The Ubuntu VM hosts the ChargeBox simulator, including the OCPP server and OCPP client (OCPP charger). The Kali Linux VM conducts the MitM attack, utilizing its pre-installed penetration testing tools. First, network discovery is performed to identify the IP addresses of the Ubuntu VM and the target device (OCPP client) using nmap on Kali Linux with the following command:

```
nmap -sn 172.24.32.0/24
```

After identifying the IP,the default gateway is located. Thus Mitm is conducted using ARP spoofing command as follows:

```
sudo arpspoof -i eth0 -t UbuntuIP gatewayIP
sudo arpspoof -i eth0 -t gatewayIP UbuntuIP
```

In this above command UbuntuIP used is (172.24.46.82) and gatewayIP used is (172.24.32.1). To facilitate packet forwarding between the Ubuntu VM and the gateway, IP forwarding is enabled in kali machine using the below command as follows:

```
echo 1|sudo tee /proc/sys/net/ipv4/ipforward
```

This command will help to forward the communication of packets to kali machine. Then finally traffic between the OCPP client and server is captured using tcpdump. After capturing the necessary traffic, IP forwarding is disabled. This setup allows for the successful performance of a MitM attack on OCPP 1.6 communication, with the captured pcap file ready for analysis in the result analysis section.

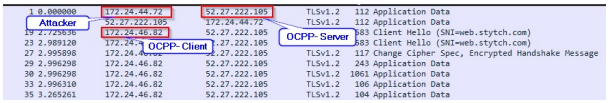

Fig. 3. Network traffic capture using tcpdump

After performing the MitM attack and capturing the network traffic using tcpdump as shown in (Fig. 3), it was observed that the traffic displayed includes communication between the OCPP client and server. Importantly, due to the MitM attack, the attacker's IP address is interjected into this communication flow. This presence indicates that the attacker successfully intercepted between the OCPP client and server, demonstrating the vulnerability of the communication to such attacks.

B. Result Analysis

While analyzing the network traffic between the OCPP client and server, it was observed that TLS 1.2 is utilized to encrypt their communication. This ensures that most of the data exchanged remains confidential and integral during transmission. Although the communication packets such as the Client Hello and Server Hello, contains critical information such as session IDs and cipher suite. (Fig.4) shows the Client Hello message, where the OCPP client initiates communication with the server. This message typically includes details like the chosen cipher suites, supported TLS versions, and a session ID if a session is being resumed.

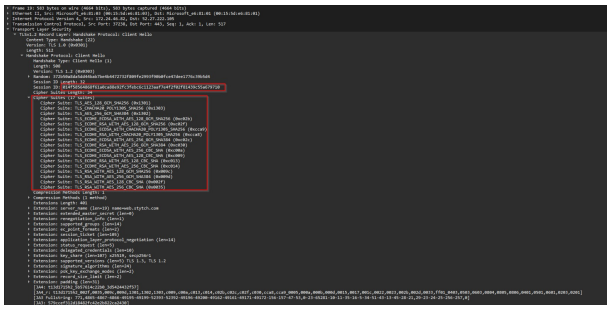

Fig. 4. Client Hello message analysis

(Fig.5) depicts the Server Hello message, where the server responds to the client's hello. This message confirms the selected cipher suite from the client's list and includes its own session ID and additional security parameters.

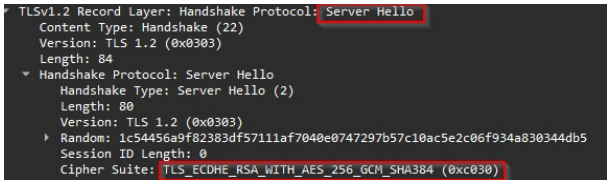

Fig. 5. Server Hello message analysis

These messages are integral parts of the TLS handshake process, establishing a secure connection between the OCPP client and server. The presence of session IDs and cipher suite information in these messages highlights key aspects of the security configuration used for encryption and authentication during communication.Session IDs in TLS are used to resume previous sessions, which can potentially expose session-related information if intercepted. An attacker intercepting a session ID could use it to hijack or impersonate the session.The cipher suite specifies the encryption algorithms and cryptographic parameters used to secure the communication. If intercepted, an attacker could analyze the cipher suite to identify potential vulnerabilities or weaknesses. This could lead to decryption of intercepted data if the cipher suite used is compromised. Thus, interception of session IDs and cipher suite details during the TLS handshake exposes the communication to various risks, including session hijacking, decryption of intercepted data, and potential compromise of the entire communication channel. Also, protocols used at the application layer are visible, as depicted in (Fig.6). Attackers can exploit vulnerabilities in these protocols.

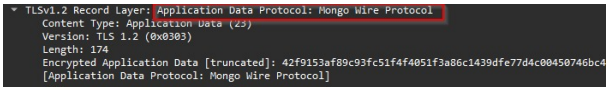

Fig. 6. Application data protocol analysis

Additionally,OCPP client and server communication is encrypted using TLS 1.2. However, TLS 1.2, while widely used, is known to have vulnerabilities that can compromise its security [8]. TLS 1.2 lacks support for modern cryptographic algorithms and security enhancements found in later TLS versions, such as TLS 1.3 [8]. These vulnerabilities make TLS 1.2 potentially susceptible to interception, decryption, and manipulation of encrypted data by skilled attackers. As a result, relying solely on TLS 1.2 for securing sensitive communications, such as those in OCPP 1.6 for EVCS, poses risks to data confidentiality and overall system integrity.

To mitigate these risks and enhance security, it is imperative for OCPP 1.6 implementations to upgrade to the latest TLS version available. The latest TLS versions will address known vulnerabilities, introduce stronger encryption algorithms, and provide better resistance against MitM attack. Also measures can be taken at network level to safegaurd network from MitM attack using VPN and Endpoint detection and response Tools. These proactive approach ensures that OCPP 1.6 systems benefit from improved security measures, safeguarding against potential exploits and ensuring secure and reliable operation in modern cybersecurity landscapes.

V. Conclusion

The study highlights significant vulnerabilities in the OCPP1.6, particularly concerning its susceptibility to MitM attacks. Despite using TLS 1.2 for encryption, which has known vulnerabilities, the protocol leaves critical data like session ID, cipher suite and application level protocol information exposed to interception. This exposes EVCS to risks such as data manipulation and service disruptions. Moving forward, adopting newer, more secure versions of TLS and implementing robust encryption practices are essential to mitigate these risks and ensure the secure operation of EVCS infrastructure. In the future, conducting further assessments of vulnerabilities in OCPP 1.6 and implementing corresponding mitigations will be essential to enhance the security of EVCS, thereby ensuring their resilience in the evolving landscape of electric vehicle technologies.

References

[1] Change, C.C., 2019. Net Zero The UK's contribution to stopping global warming.

[2] Liu, W., Placke, T. and Chau, K.T., 2022. Overview of batteries and battery management for electric vehicles. Energy Reports, 8, pp.4058-4084.

[3] Patil, P., 2020. The Future of Electric Vehicles: A Comprehensive Review of Technological Advancements, Market Trends, and Environmental Impacts. Journal of Artificial Intelligence and Machine Learning in Management, 4(1), pp.56-68.

[4] Hamdare, S., Kaiwartya, O., Aljaidi, M., Jugran, M., Cao, Y., Kumar, S., Mahmud, M., Brown, D. and Lloret, J., 2023. Cybersecurity risk analysis of electric vehicles charging stations. Sensors, 23(15), p.6716.

[5] Alliance, O.C., 2016. Open charge point protocol 1.6, 2015.

[6] Garofalaki, Z., Kosmanos, D., Moschoyiannis, S., Kallergis, D. and Douligeris, C., 2022. Electric vehicle charging: A survey on the security issues and challenges of the open charge point protocol (OCPP). IEEE Communications Surveys & Tutorials, 24(3), pp.1504-1533.

[7] Rubio, J.E., Alcaraz, C. and Lopez, J., 2018, February. Addressing security in OCPP: Protection against man-in-the-middle attacks. In 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS) (pp. 1-5). IEEE.

[8] de Carne de Carnavalet, X. and van Oorschot, P.C., 2023. A Survey and Analysis of TLS Interception Mechanisms and Motivations: Exploring how end-to-end TLS is made "end-to-me" for web traffic. ACM Computing Surveys, 55(13s), pp.1-40.

[9] Elmo, D., Fragkos, G., Johnson, J., Rohde, K., Salinas, S. and Zhang, J., 2023, November. Disrupting EV Charging Sessions and Gaining Remote Code Execution with DoS, MITM, and Code Injection Exploits using OCPP 1.6. In 2023 Resilience Week (RWS) (pp. 1-8). IEEE.

[10] Alcaraz, C., Lopez, J. and Wolthusen, S., 2017. OCPP protocol: Security threats and challenges. IEEE Transactions on Smart Grid, 8(5), pp.2452-2459.

[11] Rubio, J.E., Alcaraz, C. and Lopez, J., 2017. Selecting privacy solutions to prioritise control in smart metering systems. In Critical Information Infrastructures Security: 11th International Conference, CRITIS 2016, Paris, France, October 10–12, 2016, Revised Selected Papers 11 (pp. 176-188). Springer International Publishing.

[12] Johnson, J., Berg, T., Anderson, B. and Wright, B., 2022. Review of electric vehicle charger cybersecurity vulnerabilities, potential impacts, and defenses. Energies, 15(11), p.3931.

[13] Sarieddine, K., Sayed, M.A., Torabi, S., Atallah, R. and Assi, C., 2023. Investigating the security of ev charging mobile applications as an attack surface. ACM Transactions on Cyber-Physical Systems, 7(4), pp.1-28.

[14] Sayed, M.A., Atallah, R., Assi, C. and Debbabi, M., 2022. Electric vehicle attack impact on power grid operation. International Journal of Electrical Power & Energy Systems, 137, p.107784.

[15] Chris Jewers For Mailonline. 2022. Russian motorways electric vehicle chargers are hacked to display message supporting Ukraine. [Online]. Available at: https://shorturl.at/irvAX (Accessed: 12 May 2024).

[16] BBC News,2022.Isle of Wight: Council's Electric Vehicle Chargers hacked to show porn site.[Online]. Available at: https://www.bbc.com/news/uk-england-hampshire-61006816 (Accessed: 14 May 2024).

[17] Akuchie, M. (2023) 'Hacked Electrify America charger exposes major cybersecurity risk'. ScreenRant, January. Available at: https://screenrant.com/electrify-america-hacked-charger-cybersecurity-risk/ (Accessed: 23 May 2024).

[18] Conti, M., Donadel, D., Poovendran, R. and Turrin, F., 2022, September. Evexchange: A relay attack on electric vehicle charging system. In European Symposium on Research in Computer Security (pp. 488-508). Cham: Springer International Publishing.

[19] Nasr, T., Torabi, S., Bou-Harb, E., Fachkha, C. and Assi, C., 2023. ChargePrint: A Framework for Internet-Scale Discovery and Security Analysis of EV Charging Management Systems. In NDSS.

[20] Vaidya, B. and Mouftah, H.T., 2018, June. Deployment of secure EV charging system using open charge point protocol. In 2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC) (pp. 922-927). IEEE.

[21] Saposnik, L.R. and Porat, D., 2023. Hijacking ev charge points to cause DOS.Available at: https://www.saiflow.com/hijacking-chargers-identifier-to-cause-dos/ (Accessed: 24 May 2024).

[22] Friedland, A., 2016. Security and privacy in the current e-mobility charging infrastructure. Proceedings of the DeepSec, Vienna, Austria, 31.

[23] Alcaraz, C., Lopez, J. and Wolthusen, S., 2017. OCPP protocol: Security threats and challenges. IEEE Transactions on Smart Grid, 8(5), pp.2452-2459.

[24] Rubio, J.E., Alcaraz, C. and Lopez, J., 2018, February. Addressing security in OCPP: Protection against man-in-the-middle attacks. In 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS) (pp. 1-5). IEEE.

[25] Morosan, A.G. and Pop, F., 2017, September. OCPP security-neural network for detecting malicious traffic. In Proceedings of the International Conference on Research in Adaptive and Convergent Systems (pp. 190-195).

[26] Victormunoz, 2023. OCPP-1.6-Chargebox-Simulator: A simple chargepoint simulator, working with OCPP 1.6. Available at: https://github.com/victormunoz/OCPP-1.6-Chargebox-Simulator [Accessed 3 August 2023].