MitM Attack to Electric Vehicle AC Chargers

Javier Jarauta Gastelu, Roberto Gesteira-Miñarro, Javier Matanza, Rafael Palacios, and Gregorio López

***Abstract*—This article explores a Man-in-the-Middle (MitM) attack targeting alternating-current charging points for electric vehicles (EVs), demonstrating the ability to covertly control the vehicle's charging process without detection by either the charging station or the vehicle. The attack was conducted successfully in both controlled laboratory environments and real-world settings, exposing vulnerabilities in the communication protocols between the charging station and the vehicle. By intercepting and manipulating the communication, an attacker can adjust the charging rate, reducing, increasing, or halting the charging process altogether. This not only affects individual vehicles but could have a broader impact on the electrical grid, especially as the use of high-power EV chargers continues to grow. With the rapid increase in EV adoption worldwide, the potential for synchronized attacks on multiple charging points presents a significant risk to grid stability, from local affections to higher widespread impacts. This research then underscores the need for stronger cybersecurity measures to protect the charging infrastructure and prevent large-scale disruptions to energy systems.**

***Index Terms*—alternating-current (AC) charging, cybersecurity, electric vehicles (EVs), Man-in-the-Middle (MitM).**

I. Introduction

THE COORDINATED and simultaneous attacks on the electricity supply or demand through Internet of Things (IoT) devices have been identified, by electric grid operators and distributors, as a harder risk to control than other more traditional attacks such as advanced persistent threats (APTs) or phishing [1]. Consequently, such attacks have attracted the interest of the research community, and their impact on the power grid has been analyzed, primarily, through a series of articles published in *USENIX Security* [2], [3], [4]. In the first article, inspired by the DYN attack at the end of 2016, the term Manipulation of Demand via IoT (MaDIoT) attack is defined, and using different simulations, it is demonstrated that demand attacks can cause local blackouts or, in some cases, widespread blackouts. In the second article, the authors test and verify with more complex simulations that the probability of successfully executing these attacks is not as high as previously thought, due to the existence of protections in the electricity grid that prevent these types of widespread blackouts. However, in the final article of the series, it is demonstrated that a malicious attacker with enough and privileged knowledge of the grid, for example, taking into consideration the local grid topology and geographic distribution, may have more success in performing a grid attack with serious consequences. However, it is highly unlikely that an attacker has all of this information readily available without a significant amount of time and effort.

The three articles presented above focus on evaluating the impact of this kind of attacks in the electrical grid, assuming that they can compromise as many high-power devices as needed and wherever they are needed. In this article, however, we focus on investigating if it is possible to compromise and remotely control one example of such high-power devices, in particular, electric vehicle (EV) charging points.

EV chargers provide the means to charge EVs, from a slow charge of a few kW to more than 500 kW. Due to the significant increase in EV sales in recent years, in markets such as the European Union, China, and the United States, with a 35 % year-on-year increase globally for 2023 [5], the number of EV Charging Stations is increasing significantly in order to support that surge in sales.

For example, in the European Union, according to some studies using open-source data, the amount of publicly available EV chargers is, as of the end of 2023, of around 750 000 chargers [6]. That includes both slow alternating-current (AC) chargers and fast direct-current (DC) chargers in varying proportions, with the later amounting for 15 % of the total number of chargers [7]. Furthermore, in terms of total capacity, the current maximum available charging capacity is of around 28.7 GW concurrently [6].

In the United States, just like Europe, the number of publicly available chargers is increasing, with an estimated number of 192 000 ports installed by August 2024 [8]. That amount is set to expand significantly in the next few years, as decarbonization objectives come into effect from 2030 [8].

Considering the increase in EV Charging Stations, there is clear evidence that these devices, if compromised massively, may pose some risks to the grid in general, especially considering the amount of installed power that these can provide. As a matter of fact, based on a World Economic Forum report [9], only approximately 150k of 20 kW charging units, 75k of 40 kW charging units, and 37.5k of 80 kW charging units would be required to generate a 3GW imbalance which would put against the rope the entire continental European Synchronized Power System [10]. Of course, a smaller amount would only be needed for local or regional blackouts.

Received 14 June 2025; accepted 29 June 2025. Date of publication 23 July 2025; date of current version 25 September 2025. This work was supported by the European Union's Horizon Europe Energy Research and Innovation programme under Grant 101075665. *(Corresponding author: Javier Jarauta Gastelu.)*

Javier Jarauta Gastelu, Roberto Gestiera-Miñarro, Javier Matanza, and Gregorio López are with the Institute for Research in Technology, ICAI Engineering School, Universidad Pontificia Comillas, 28015 Madrid, Spain (e-mail: jjarauta@alu.comillas.edu; rgesteira@comillas.edu; javier.matanza@iit.comillas.edu; gllopez@comillas.edu).

Rafael Palacios is with the Institute for Research in Technology, ICAI Engineering School, Universidad Pontificia Comillas, 28015 Madrid, Spain, and also with Cybersecurity at MIT Sloan-CAMS, Massachusetts Institute of Technology, Cambridge, MA 0213 USA (e-mail: rafael.palacios@iit.comillas.edu).

Digital Object Identifier 10.1109/JIOT.2025.3589219

Thus, in this article, we address the following research question: Is it possible to control maliciously the charging rate of an EV while in the charging process? In order to answer this question, we first analyze how the EV charging works and we adapt STRIDE threat model to investigate vulnerabilities in this context in a systematic way. Then, we focus on AC charging and demonstrate that it is possible to perform a Man-in-the-Middle (MitM) attack that allows controlling the vehicle's charging process without detection by the charging point or the vehicle. Finally, we discuss possible countermeasures to this attack as well as future research lines.

II. Background

There are two main mechanisms for charging EVs: 1) AC charging and 2) DC charging. Beyond the type of electricity used, chargers can also be classified according to factors such as charging speed (i.e., the maximum power at which the vehicle can be charged), type of plug connectors, and other criteria. For charging speed, the maximum power may depend on several factors, including the charging equipment, the vehicle's capabilities, and environmental conditions, among others.

To first understand the charging process and the steps involved in executing a MitM attack, it is helpful to grasp the basics of the AC charging protocol.

A. Classification of Charging Powers

The classification by maximum charging power varies in both denomination and power categories among different charging point operators and manufacturers, with some consensus only on slow charging. This allows for the following tentative classification: [11].

1) *[Slow Charging] [1.3–44 kW]:* AC charging points, available in garages, urban public roads, etc. Long charging times of multiple hours.
2) *[Semi-Very/Fast/Ultra/Super-Fast Charging] [>50 kW]:* These are only DC charging points with the highest power available, currently up to about 500 kW. Their charging times range from 10–60 min.
3) *[Mega-Watt Charging System] [< 3000 kW]:* This is the latest standard destined for commercial vehicle charging, such as trucks and buses. It is still under development and in deployment in limited pilots.

B. Standards

Within the charging process, there are a series of protocols and standards that integrate the entire charging process of EVs. Below are the main protocols and standards necessary for executing the charging process. Additionally, Fig. 1 shows the role of each protocol in the charging process.

IEC 62196 defines the physical elements and regulations of plugs, connectors, ports, cables. *ISO 61851* defines the electrical requirements of vehicles and charging stations. It includes basic signaling of the system, such as pulse width modulation (PWM) signals and charging states. *ISO 15118* defines the most advanced communication protocol between the EV and the grid, including Vehicle-to-Grid (V2G) functionalities. It also comprises the IP communication mechanism and Plug&Charge. *OCPP/OICP* are the *de facto* open-source standard protocols for communication between charging stations and charging station managers/providers.

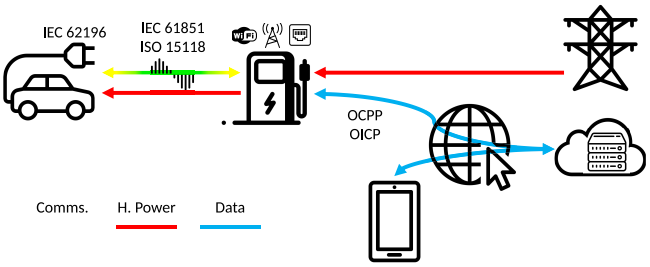


Fig. 1. Charging system and protocols.

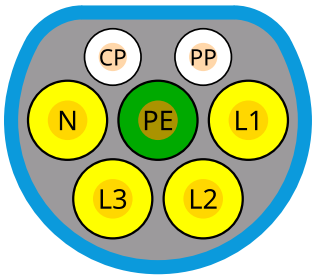


Fig. 2. Type 2 connector. Source: [12].

C. AC Charging

AC charging allows for one- or three-phase charging up to 44 kW for a vehicle equipped with a sufficiently powerful onboard charger. This type of charging constitutes the majority of supply points in the European market and is the most widespread among small users, as its installation only depends on the presence of minimal power in the electrical grid [6]. The advantage of this type of charging is that the vehicle itself has the charger or converter between AC (grid) and DC (battery).

1) Connectors: For AC charging in the European market, the connector called Type 2 or Mennekes is used, as defined in the IEC 62196 standard. It contains seven conductors, as shown in Fig. 2.

In this case, the conductors are N (Neutral), L1, L2, and L3 (Lines), protective Earth (PE) proximity pilot (PP) that indicates to the charging station that a vehicle is connected, and, control pilot (CP) which is the conductor through which bidirectional encoded information is transmitted.

2) Signaling: For communication between the vehicle and the charging station, the standard indicates the use of PWM signals on the CP line to indicate different states and power levels. This PWM will be the signal on which higher-level protocols will base their more complex information transmission, in the case of DC charging [13].

With the PWM signal, there is bidirectional communication from both the charging station and the vehicle. In this scheme, the charging station indicates the maximum available power and the state of the charging point, including failure scenarios.

TABLE I
DUTY CYCLE/CURRENT

Duty Cycle	Current/Information
<3,00 %	Charging not allowed
3,00 - 7,00 %	Use ISO 15118
7,00 - 8,00 %	Charging not allowed
10,00 %	6 A
26,67 %	16 A
53,33 %	32 A
96,00 %	80 A

TABLE II
CHARGING STATUS AND VOLTAGES

States	PWM Voltage	Resistance between CP/PE
Vehicle disconnected	$+12$ V	$\infty\ \Omega$
Vehicle ready	$+9/-12$ V	2740 Ω
Charging	$+6/-12$ V	882 Ω
Charging - Ventilation required	$+3/-12$ V	246 Ω
Off	0 V	
Error	-12 V	

The vehicle then communicates the current charging status and any other failures modes in itself.

The information about the available power of the charging point is encoded using the PWM signal's duty cycle. Additionally, in case of a stop, an non-compliant duty cycle, such as 0 %, is sent on the PWM. This duty cycle is defined for values between 6...50 A using this formula [13]

$$\text{Duty\_Cycle} = \left(\frac{\text{Current}}{0.6}\right). \tag{1}$$

And for values between 51...80 A

$$\text{Duty\_Cycle} = \left(\frac{\text{Current}}{2.5} + 64\right). \tag{2}$$

In addition, there are certain ranges of values with different meanings. Table I presents a limited relationship of values for the PWM signal [14].

For car communication, the voltage of the PWM signal is used to indicate the current charging status. As shown in Section II-C3, the PWM signal provided by the charging point always presents values between ±12 V, and the vehicle modifies the maximum upper value of the PWM signal by introducing resistors between the CP and PE lines to indicate the current charging status. The different states are shown in Table II [13].

3) Circuitry: For both elements to establish basic communication, it is necessary to correctly define the communication elements between both systems. However, due to the simplicity of the systems, the circuitry is based on the measurement of control lines, resistors, diodes, and a limited number of active elements. A schematic of the connection between the vehicle elements and the charging point, using an independent cable, is shown in Fig. 3 [14].

4) Charging Process: The process of charging an EV in AC follows these steps.

1) *Connecting the Vehicle to the Charging Point:* The connection between both elements is made using an independent cable or one permanently connected to the charging point. The PE (Earth) pins will first connect for safety reasons, and the charging point will detect the presence of the vehicle/cable as it maintains a voltage of 5 V on the PP line. The presence of the vehicle is detected by a 5 V signal and the maximum charge power allowed by the cable is measured by additional resistors in the cable which vary between 1500 Ω and 100 Ω or known with integrated cables [13].
2) *Starting the Charging Process:* The charging point starts with a PWM signal of ±12 V indicating the maximum charging power in the duty cycle, signaling that it is ready. Once the signal is detected, the vehicle indicates its readiness through a 2740 Ω resistor.
3) *Charging:* Having received a response from the vehicle, the charging point closes the relays/contacts to supply energy to the vehicle. When it detects a positive current, it indicates through a 1200 Ω resistor that it is charging correctly.
4) *Disconnection/Interruption:* To disconnect, the vehicle will interrupt the charge and disconnect the voltage on the presence line, indicating the disconnect from the charging point. In the case of the charging point, if it needs to interrupt the charge without failure, it will simply indicate a PWM signal with a 0 % duty cycle.

D. DC Charging

Although not the subject of this research, for DC charging, the underlying protocol uses the same basic communication as AC charging to establish the connection between the charging point and the vehicle. Additionally, it uses a modified connector, called CCS 2 (Combined Charging System), which has the same structure as Type 2 but with two additional pins that allow for DC charging with a direct connection to the vehicle's battery.

Given that the protocol for DC charging uses a power line communication (PLC) signal on the same CP line, using upper-level TCP/IP communication, it is necessary for the underlying PWM signal to be present on that line for successful charging to happen. Additionally, in any situation, a disconnection of the PWM signal results in a stop of the DC charging [15].

III. METHODOLOGY

Before analyzing device vulnerabilities, a clear methodology is needed to examine the charging ecosystem's attack surfaces, including devices, communication channels, and key components.

To achieve this, a STRIDE-based threat model was chosen for its modularity and completeness, building on previous work [16], [17]. STRIDE represents six threats, such as spoofing, tampering, repudiation, information disclosure, denial-of-service, and elevation-of-privilege [18].

The purpose of refining and adopting this improved STRIDE-based methodology is to establish a unified framework for analyzing IoT devices, including high-power and grid-connected elements. Building on previous work by our team [17], this enhanced methodology aims to provide a

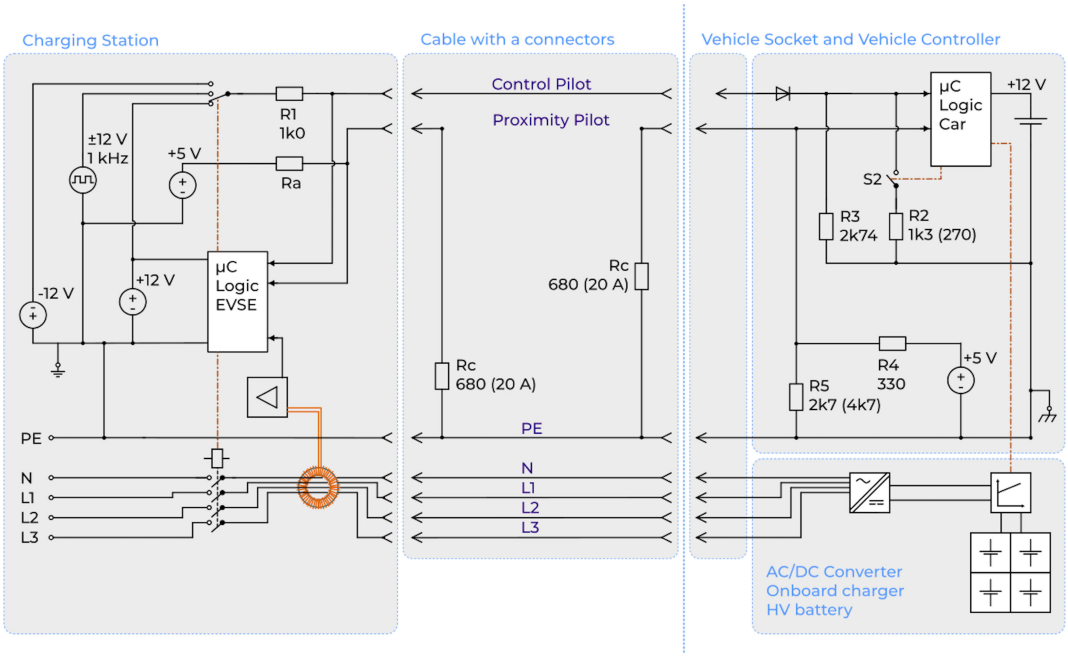


Fig. 3. Connection circuitry between the vehicle and the charging station. Source: [14].

comprehensive view of potential attacks across an entire system, even if this research focuses on a specific scenario. The use of this methodology is also focused on providing researchers a framework used for future work, and encourage its application in future research to enhance consistency and completeness in vulnerability assessments.

To ensure the methodology's effectiveness, it was adapted to meet the unique demands of cyber–physical systems and high-power IoT devices. Since STRIDE was originally designed for secure code development, additional considerations were introduced to address integrated systems [19]. The resulting methodology incorporates STRIDE's core principles with added adaptations for IoT systems [17].

1) *System Definition and Decomposition:* This step includes a high-level representation of all components that participate in the charging process. In our case, the components are shown in Fig. 1. These should be classified in the following categories with the aim of elaborating a data flow diagram (DFD).
   a) *External entities:* Represent elements external to the process, like data providers, etc. Represented in the DFD as rectangles.
   b) *Data flows:* Showcase the transfer of data between entities. Represented by arrows.
   c) *Processes:* These are either actions or data processing that happens as part of the system. They are represented by circles, when complex, that circle is doubled.
   d) *Data Stores:* Data storage and processing nodes. Represented by two parallel horizontal lines.
   e) *Trust Boundary:* This is the boundary where the system can be assumed to be safe and free form external influence, that is the safe/nonsafe entities. Represented by a dotted line.

TABLE III
RELATIONSHIP BETWEEN STRIDE AND EACH ENTITY

Type of entity	S	T	R	I	D	E
External Entity	X		X			
Data Flow		X		X	X	
Data Store		X	*	X	X	
Process	X	X	X	X	X	X

2) *Generic DFD Creation and Analysis:* Using the components identified in the first stage, a generic DFD for the system is created. In this case, the components should remain general rather than manufacturer-specific to allow for flexibility in the specific analysis. In this stage, the main attack vectors may be analyzed for the global components.
3) *Specific Implementation Analysis:* This is the stage where the specific components of a manufacturer/provider implementation are analyzed. In this case, a more specific DFD can be generated according to the actual components used in the system.
4) *Component Vulnerability Analysis:* Knowing the structure of the system and its individual components, a vulnerability analysis of each one should be performed, including OSINT techniques and CVE searches.
5) *Use of STRIDE Tools to Complete the Vulnerability/Attack Surface Search:* In this case, the STRIDE methodology takes the main role into decomposing and analyzing the different attack vectors. Using both DFDs previously created, we can use STRIDE's tables and trees to analyze each of the components individually, depending on their type, as shown in Table III [19]. Once the possible attacks for each entity are defined, it is then possible to use the threat trees that are explained in the methodology to evaluate possible specific attacks for each entity, as shown in Fig. 5 [19].

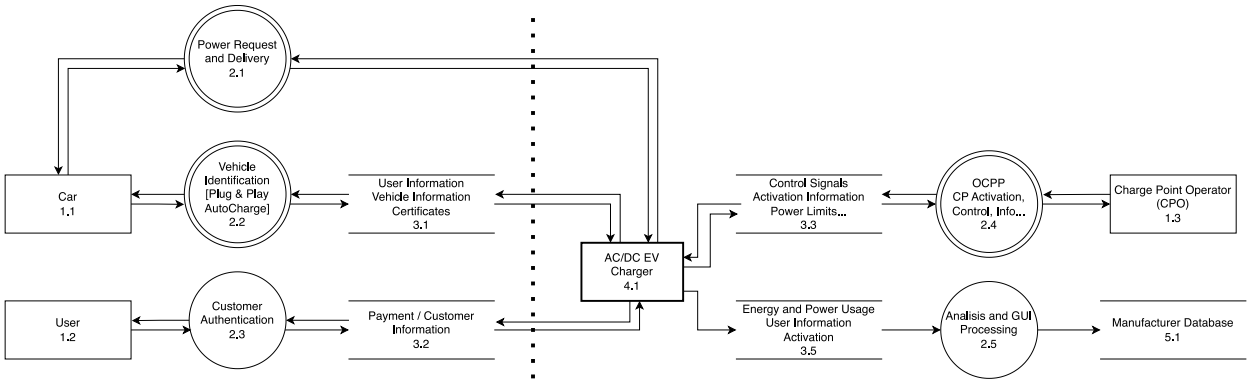


Fig. 4. DFD representing the AC/DC charging process.

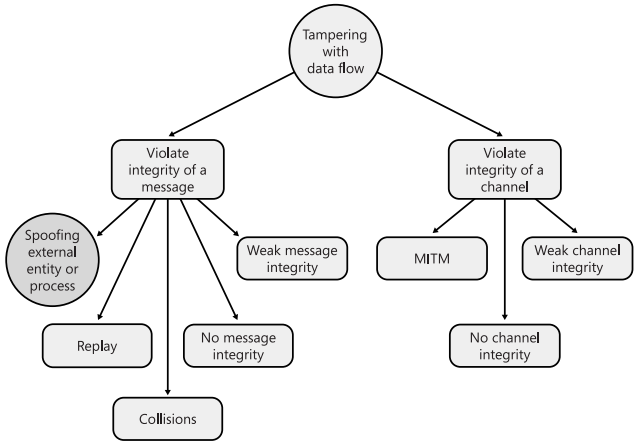


Fig. 5. Threat tree for the alteration of a data flow. Source: [19].

TABLE IV
EV CHARGER THREATS TABLE

Element type	Name	Number	Threats
External Entities	Car	1.1	S,T,R
	User	1.2	S,R
	Charge Point Operator	1.3	S,T,R,I,D,E
	Manufacturer	5.1	S,R,I
	EV charger	4.1	S,T,R,D,E
Processes	**Power Request and Delivery**	**2.1**	**S,T,R,I,D,E**
	Vehicle Identification	2.2	S,T,R,I,D,E
	Customer Auth.	2.3	S,T,R,I,D,E
	Charge Point Control [OCPP...]	2.4	S,T,R,I,D,E
	Data Analysis and GUI	2.5	S,T,R,I,D,E
Data Stores	AC/DC Charger	4.1	T,R,*,D
	Charge Point Operator	1.3	T,R,I,D
	Manufacturer Database	5.1	T,I,D
Data Flows	**Car Communication**	**(1.1↔4.1)**	**S,T,R,I,D**
	Customer Auth.		
	Automatic	(1.1↔3.1)	S,T,I,D,E
		(3.1↔4.1)	T,I,D
	Manual	(1.2↔3.2)	S,T,I,D,E
		(3.2↔4.1)	T,I,D
	Charge Point Control		
	User	(1.2↔4.1)	S,T,I,D
	CPO	(1.3↔3.1)	S,T,I,D
		(3.3↔4.1)	T,I,D
	Data Reporting		
	CPO	(4.1↔1.3)	S,T,I,D
	Manufacturer	(4.1→3.5)	S,T,I,D
		(3.5→5.1)	T,I,D

In this project, and following the steps mentioned above in the STRIDE methodology, we first created a DFD, as shown in Fig. 4. This DFD represents a generic overview of the EV charging process. A description of each element is included in the Appendix.

After creating the DFD, an analysis was then performed on the different component analysis, using STRIDE as a base, but taking into account the specifics for an EV charging system. That led to Table IV, which, is part of the previous research [17]. It is worth noting that STRIDE provides basic attacks for each element type, but those, in most cases have to be adjusted in the case of cyber–physical systems.

Having performed the initial analysis for the EV Charging ecosystem, and keeping in mind that the aim is to develop and demonstrate a generic attack that is manufacturer-independent, it is then necessary to analyze the potential attack vectors and risks of the system.

1) *Attack on the Vehicle Components Like BMS, Charge Port Computer, CAN Bus:* These attacks are specific, as each vehicle manufacturer has their own safeguards and internal structure. and cannot be scaled easily.
2) *Attack on Generic Vehicle Interfaces:* Unlike attacks on component attacks, OBD port attacks can be scaled easily and be manufacturer independent, however there is ample successful attacks previously performed [20].
3) *Attack on the Plug&Charge Protocol (ISO 15118):* In order to facilitate further attacks within the ISO 15118 protocol during the charging phase, it is first essential to compromise the encryption and communication channels between the EV and the charging station. To achieve this, the initial step involves executing an AC charging attack, which serves as a prerequisite for subsequent exploitations.
4) *Attack on the EV Charger:* Although attacking individual EV chargers presents a semi-scalable approach it also introduces significant risks. These include harm to the researcher and the inadvertent disruption of legitimate charging infrastructure. Moreover, access to charging stations for testing is costly and not readily available.
5) *Attack on the Monitoring/Manufacturer Control Plane:* This approach constitutes a logical attack targeting the control infrastructure and the open charge point protocol

(OCPP). While such attacks can be effective, it is important to note that OCPP vulnerabilities have been extensively studied in existing literature.

Based on the DFD (Fig. 4) and discarding the previous possible attacks, the generated Threat Table (Table IV) and the threat tree for tampering with a data flow (Fig. 5), a MitM attack was selected as a potential threat to Process 2.1 and Data Flow (1.1↔4.1) (Car Communication), which represents the power request and delivery stage between the vehicle and the charging station. This specific attack vector was selected due to its high feasibility for real-world deployment, minimal equipment requirements, and its ability to illustrate broader system-level vulnerabilities without needing access to proprietary components or infrastructure.

The threat tree in Fig. 5 illustrates several possible methods for tampering with a data flow. In this context, tampering involves altering the integrity of the communication between the EV and the charging station. Two main branches emerge from the root of this threat tree: 1) violating the integrity of a message and 2) violating the integrity of a communication channel. This matches the previous assessment performed on each of the components.

In our scenario, the MitM attack is categorized within the threat trees under the branch of violating the integrity of a channel. This involves intercepting and modifying the data transmitted between the vehicle and the charging station without being detected. To execute this attack, the communication channel, in this case, the charging cable, is compromised by inserting malicious hardware or software that can manipulate the data flow.

By compromising the channel integrity, an attacker can perform actions such as altering the power request data, manipulating the power delivery parameters, or injecting false information to disrupt or control the charging process. It showcases a potential vulnerability in the communication between the vehicle and the charging station.

Building on that assessment, the research then narrowed its focus to a specific charging technology. In this study, the decision was made to focus on AC charging for EVs. Several factors influenced this choice, including the relative ease of obtaining AC charging equipment for testing, the reduced risk to researchers due to the lower charging power and voltage levels, and the flexibility to modify a charging cable. The European standard (Type 2) of the global charging protocol allows users to supply their own cables, which do not need to be permanently attached to the charging point. This makes it possible to create and deploy a malicious cable without needing to alter the vehicle or the charging station. Consequently, both the vehicle and the charging point remain completely unaware of any malicious actions. By following this approach, the vehicle does not detect any unusual commands from the modified charging point, while the charging point only observes seemingly anomalous fluctuations in the vehicle's charging power. These advantages, along with the greater complexity of the DC charging protocol, which relies on packet communication, led to the decision to conduct initial tests exclusively on AC chargers.

IV. Man-in-the-Middle Attack

In order to carry out the attack on the AC EV charging system, tests and research were conducted systematically, beginning with the simulation of a complete charging system in the laboratory, including both the charging point and the vehicle. After obtaining satisfactory results and performing the necessary checks, a malicious cable was developed, that could be easily deployed in field tests to verify signaling and the possibility of performing a demand attack on an EV during the charging process.

The search for an accurate simulation of the protocol guided the tests and circuitry conducted. The goal was to avoid detection by both the vehicle and the charging station, while improving the portability and scalability of the attack components.

A. Laboratory Testing

In laboratory tests, the objective is to verify the components, circuitry, and feasibility of successfully performing the MitM attack on the simulated elements. To perform the simulation correctly, the following components were developed.

1) Charging Point Simulator: Using an Arduino UNO as the logic controller, a charging point simulator was created, capable of adjusting the charging power according to preset parameters. It includes simulation of the behavior of different charging states through a state machine and adjustment of the duty cycles of the PWM signal. Additionally, it can perform all line voltage measurements through an adapter circuit, allowing it to react to vehicle errors and states. The system shown in Fig. 6 was developed, by adapting the information in Fig. 3.

2) Vehicle Simulator: To simulate the vehicle's charging states, a small circuit operated manually by switches (Fig. 7) was developed, which could indicate the vehicle's state to the simulated charging point for detection. All this is shown through LED indicators in the charging point simulator.

3) Creation of the Malicious System: Using another Arduino UNO and circuitry, a malicious system was developed by combining both circuits described above and controlling the manual switches with relays, as shown in Fig. 8.

This system is capable of intercepting the signal sent by the genuine charging point, by deciphering the duty cycle to obtain the available power and state and modifying this signal to indicate a different available power or even a lack of power to the vehicle. It can also read the control line sent to the vehicle, determine the states it communicates, and forward those states to the charger within a period of less than 200 ms, simulating vehicle behavior.

Using this process, the malicious system can modify the power the vehicle perceives as available and create periodic fluctuations or even stop the charging completely, all without altering either of the process elements. The system's logic includes three basic elements that allow its operation.

1) *Measurement System:* The measurement system performs two main functions: a) measuring the states of both lines and b) measuring the duty cycle of the PWM signal. To determine the state sent by the vehicle, this system measures the maximum line voltage after passing

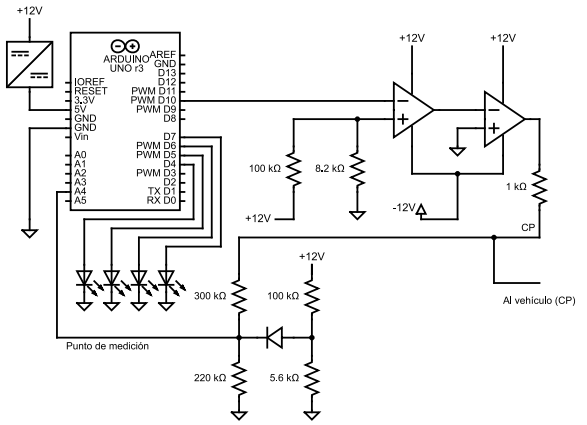


Fig. 6. Charging station simulator.

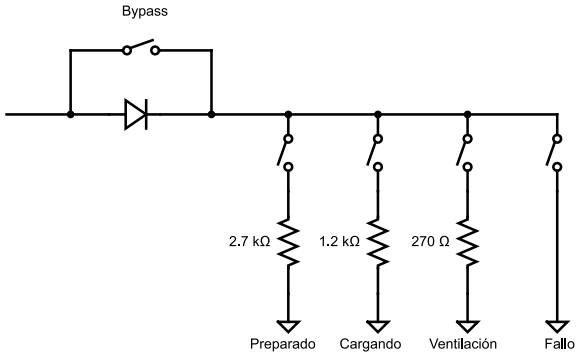


Fig. 7. Vehicle simulator.

through a voltage converter and determines the vehicle's state. It then transmits this information to the charging point using upstream relays. To determine the duty cycle that indicates the maximum power to be transmitted to the car, this system includes signal filtering logic to avoid distortions and internal resistances altering the value, and it assigns the maximum line power according to (1) or (2) that the charging point can provide.

2) *State Machine:* The state machine transmits information from the vehicle to the charging point and alters its internal value based on measurements from both pilots. It is responsible for modifying output values, monitoring both signal cables, and ensuring that despite the attack, the system remains within normal parameters. In this implementation, there are two parallel state machines. The goal is for any change in one to be instantly reflected in the other.

3) *Attack System:* This system is responsible for receiving malicious commands and executing the power fluctuation cycle within a modifiable interval of seconds. Through this mechanism, a malicious user can alter the vehicle's demand and charge based on a pattern.

4) Integration of Components in Simulator: All the above systems were integrated into a simulator to demonstrate their correct functioning by sensing the CP control lines and measuring states and maximum powers. Using two Arduinos to control a good charging point and another to control the malicious system, and a manual vehicle simulator. With this simulation system, necessary adjustments were made in the measurement systems and state machine to ensure the fastest possible information transmission for security reasons.

5) Creation of the Malicious Cable: Once all components were integrated, it was necessary to modify the cable used for EV charging. The modification does not involve altering any of the power cables (L1, L2, L3, N); it only requires intercepting the CP cable using terminal blocks and obtaining the reference voltage for all measurement components by making a small perforation in the PE insulator. This minimizes the risk to both the attacker and the charging point user, as the CP pilot signals are low voltage and the cable modification is minimally visible.

This system is integrated into a small, easily portable PCB, with its final appearance similar to that of a mobile/emergency charger provided by EV manufacturers for charging in domestic (schuko - CEE 7/3 Type F) or industrial (Cetac - IEC 60309) sockets.

B. Field Testing

Once the laboratory tests were completed, field tests were carried out with unaltered charging points and vehicles in a production environment. To conduct the field tests, the following were used: the malicious cable, malicious logic, measuring systems (oscilloscope, clamp meter, multimeter), and power supply.

1) Eavesdropping: The first approach to performing the attack is to verify that the real system operates as specified [13]. This step was necessary to include any specific implementation by the charging point manufacturer or any required peculiarity in the attack; however, no significant adjustments were needed.

Initially, the PWM signal on the cable was analyzed without intercepting the CP line. This ensured that no additional distortion was introduced by modifying the charging cable, both toward the charging point and the vehicle segment. This analysis involves first verifying the charge levels. When disconnected, a continuous voltage of $+12$ V, once the cable is detected, a PWM signal ± 12 V, and upon starting the charge, between $+9$ V/-12 V. The fault state was not tested to avoid causing any line damage [13].

Additionally, it was verified that the duty cycle for the expected current values was adequate. For 6 A current (3.6 kW), the duty cycle was around 10 %, and similarly, $\sim$50 % for 32 A current per phase (22 kW). In this case, the distortion in the line, whether due to noise introduced by the cable or its modification, is insignificant for the distances of an EV charging cable, and the current measurement received by the system was within the expected values according to the specification.

2) Attack: Once the cable signal checks were completed without any malicious modifications (*eavesdropping*), the attack was carried out in the real test environment.

The demand attack consists of periodically modifying the charging power from the maximum available at the charging point to the minimum admissible by the protocol (6 A). This

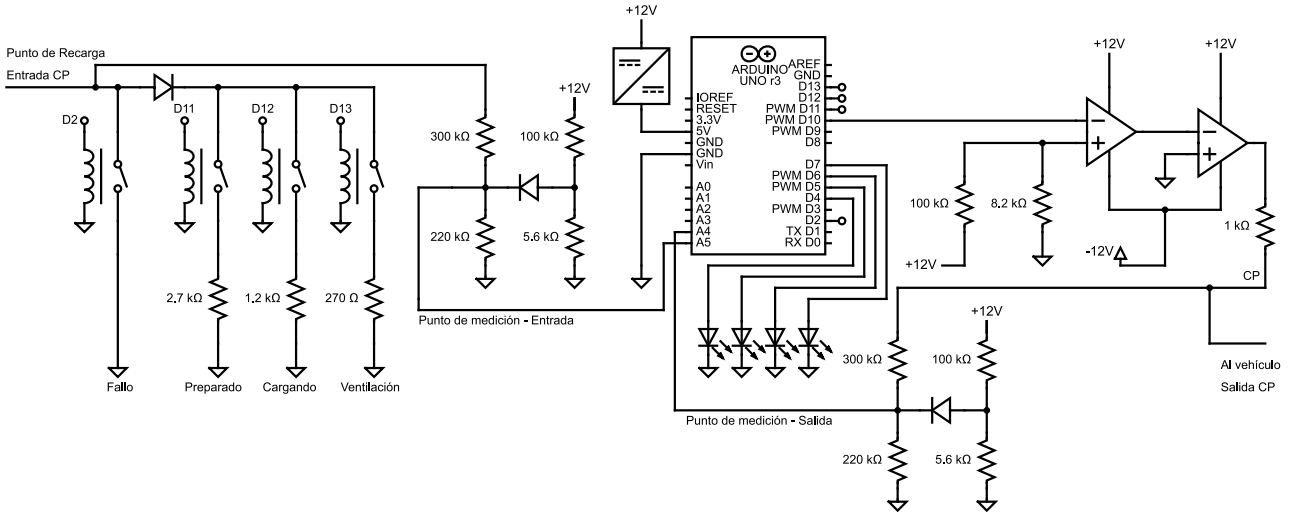


Fig. 8. Malicious system simulator.

cycle would repeat at intervals ranging from a few seconds to long periods.

The goal of this attack is to verify that it is indeed possible to modify the active charge of an EV without requiring reconnection or stopping, thus allowing demand attacks on high-power elements. Additionally, the advantage of this attack is not only to interrupt the charge, as it is easily detectable if the vehicle or charging point interrupts the charge, but to periodically fluctuate the power. This fluctuation is much harder to detect, as it could be attributed to semi-anomalous behavior by one of the process elements. For example, the vehicle might modify the charging power based on its needs, such as battery charge status, charging schedules, etc. Additionally, the charging point might be modifying the power due to line limitations, charging through photovoltaic systems, or shared power between different points, among others.

The malicious device was then inserted, intercepting the control line of the cable. Once inserted, a battery of tests was conducted to verify its correct operation, keeping the measuring elements both on the conductors and the lines to verify similar/equal behavior.

The tests began with a 3-s change cycle. This three-second cycle, tested in laboratory tests, worked as expected. However, problems were encountered as the vehicle being tested did not instantly increase the power when at low charging power. However, for safety reasons, it did instantly reduce the power when instructed by the charging station. To mitigate this minor inconvenience, subsequent tests were conducted with a 30-s interval between power changes. With this modification, the attack behavior in all elements is as follows.

1) *Normal Charging State:* The vehicle is charging at the maximum desired power (11 kW). The PWM signal in both CP segments has a duty cycle of approximately 50 %, indicating a maximum charge of 22 kW and the voltage on both sides of the PWM signal is set between $+9/-12$ V, indicating an active charging state. At this point, the system does not act, and neither element is aware of its existence. This is shown in Fig. 9.
2) *Power Reduction:* The attack begins at this point. The vehicle receives a malicious signal through CP indicating that the maximum charging power is 3.6 kW (10 % duty cycle), while the charging point continues to emit maximum power (Fig. 10). The vehicle, upon receiving this signal, instantly reduces the power to avoid faults in the charging point and begins charging at 3.6 kW. In this case, for the charging point, the only observation is that the vehicle has reduced the measured charging power in the lines, but has not altered any states. For the vehicle, it has received a direct power reduction signal but continues charging.
3) *Power Increase:* In this case, once the power is reduced, the attacker again sends a signal to the vehicle indicating that the charging point has maximum power available again, or any power between the minimum and maximum available. Upon receiving this signal, the vehicle begins to gradually increase the charging power, taking about 12 s (this behavior depends on each vehicle's make and model). For the vehicle, there has simply been a power increase without a change in the charging state. For the charging point, the measured power will begin to rise. When the vehicle is sent a power level higher than the charging point can provide, two situations may occur.
   a) The vehicle detects that the charging point does not provide more power without reaching the maximum and considers it defective. However, there will be no fault in the charging point or vehicle, at most a message indicating reduced charging power. This occurs if the charging point can physically limit the charging power.
   b) If the charging point cannot limit the power, it will interrupt the charging for safety reasons. This happens when the vehicle requests more power than is available and exceeds the limits.
4) *Charging Halt:* It is possible to halt the charging in various ways. The most suitable would be to indicate to the vehicle that there is no power. In this case, the

Fig. 9. Normal charging state.

Fig. 10. Reduced charging state.

vehicle would stop the process, and at the same time, the charging point would be indicated that the vehicle is not charging by removing the resistance in the line. Automatically, the charging point opens the voltage line contacts, and everything stops. There is also the option to completely disconnect the signal or even provoke the fault signal.

5) *Charging Restart:* The charging restart depends on the implementation by the charging point manufacturer and whether it is public (paid) or private. In a public point, the interruption might require a reauthentication process, making it impossible. In a private point, the restart is possible depending on how the stop is performed. In the tests, no restart was performed.

Once the above cases were verified, the field tests were concluded, demonstrating how it is possible to alter the AC charging process of an EV, allowing demand attacks on the charging infrastructure without detection.

V. Discussion

The security of EV charging systems has garnered significant attention due to the critical role these systems play in the broader adoption of EVs. When considering the widespread policies of electrifying the current vehicle fleet in Europe, parts of Asia and North America, research shows that security, while not the cornerstone of every manufacturer, has taken some importance due to the complex EV charging ecosystem. This is because it requires significantly more electronic/logical systems than traditional Internal Combustion Engine vehicles [21], [22].

Ample research has been performed on attacks targeting the entire EV charging ecosystem. This includes OCPP attacks to the communication of the chargers [23], [24], general attacks using techniques such as rogue access points to both the supply equipment and the vehicle [25], attacks on the user data [26] and physical attacks on the equipment and vehicles [27]. However, there is a lack of attacks that do not require modifying both components of the charging process, i.e., attacks that are completely independent of the equipment and applicable in almost any situation.

Furthermore, several methodologies have been developed to detect these types of attacks, with traditional and novel techniques, such as AI and fuzzy logic, or anomalous behavior analysis from the EV [28], [29], [30].

In this article, we presented a methodology demonstrating the potential implications of MitM attacks on the charging process. We performed a MitM attack without modifying any components or being detected, showcasing how relatively easy it is to execute. This attack demonstration can thus be used in order to train and test the possible behavioral and mitigation systems presented in several other articles.

VI. Conclusion

After conducting both laboratory and field tests, it has been demonstrated that with simple electronics it is possible to control EV AC charging. This article does not aim to explain how these attacks could be performed at scale, but to highlight that security in EV AC chargers needs to be improved.

The attack demonstrates the necessity of incorporating mutual authentication as part of the AC charging protocol. Furthermore, considering that the attack can be executed without the knowledge of either party involved in the charging process (vehicle and charger), it is conceivable that one of these two might maliciously interfere with the charging. Given the existence of a higher protocol with authentication and certificate verification, it would be advisable to promote the adoption of this protocol for AC charging as well.

Due to the previously mentioned limitations and dangers, such as the risk from high voltage and power of these chargers, DC charging was not considered for this attack. However, with sufficient safety measures and by creating an overlay plug (as there are no dedicated cables for DC charging), similar to credit card skimmers, it might be possible to replicate the presented attack on DC chargers.

VII. Future Work

For developing the attack on DC, it is noteworthy that the basic communication system uses the same structure as AC chargers, as seen from the CCS connector structure in Fig. 11. It continues to use PWM signals for connection and

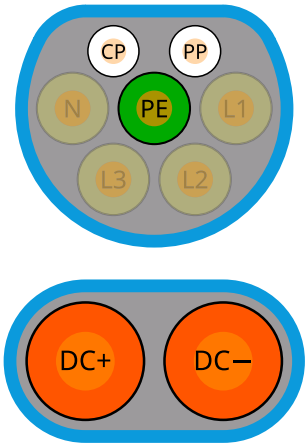


Fig. 11. CCS 2 connector. Source: [31].

state indication, and therefore the basic circuitry could be reused. However, this charging mode uses a higher protocol for communication (ISO 15118) [15] based on TCP/IP. For its activation, the duty cycle of the lower protocol is set at approximately 5 %, after which the higher protocol begins to operate, adhering to the different communication layers with respect to the OSI model.

1) *Physical:* HomePlug Green PHY—PLC Modem—[1.8 MHz $\leftrightarrow$ 30 MHz].
2) *Data Link:* signal level attenuation characterization (SLAC)—[−75 dBm/Hz].
3) *Network:* IPv6—Neighbor Broadcast Protocol + ICMPv6.
4) *Transport:* TCP + TLS (Optional), UDP.
5) *Session:* Vehicle to grid transfer protocol (V2GTP).
6) *Presentation:* W3C EXI 1.0 encoding/decoding.
7) *Application:* Charge packet communication, which includes actual charging communication and relevant information for the charge process (authorization, charging parameters, etc.).

The advantage of this protocol is that, in its latest implementation, it uses certificates issued by an authority for the communication between the vehicle and the charger. However, this security relies solely on the use of *Plug&Charge*, which is not implemented by all manufacturers nor activated by all charging operators.

Therefore, despite using certificates for communication and TLS, these are self-signed so they can also be susceptible to MitM attacks. Future research could investigate the communication security between the charger and the vehicle in DC and the existing mutual authentication mechanisms.

APPENDIX

DFD ELEMENTS

Relation of the elements that form part of the DFD for an EV Charging system.

1) *External Entities:*
   a) *Car (1.1):* The EV being charged.
   b) *User (1.2):* The user or owner of the EV.
   c) *Charge Point Operator (CPO) (1.3):* Entity responsible for operating and managing the charging infrastructure.
2) *Processes:*
   a) *Power Request and Delivery (2.1):* Handles the request and delivery of power to the vehicle.
   b) *Vehicle Identification [Plug & Play / AutoCharge] (2.2):* Manages vehicle identification, ensuring compatibility and authorization for charging.
   c) *Customer Authentication (2.3):* Authenticates the user for the charging process.
   d) *OCPP CP Activation, Control, Info$\cdots$ (2.4):* Handles the OCPP for charge point activation, control, and information exchange.
   e) *Analysis and GUI Processing (2.5):* Performs data analysis and processes information the user (GUI).
3) *Data Stores:*
   a) *User Information, Vehicle Information, and Certificates (3.1):* Stores user and vehicle identification data, along with security certificates.
   b) *Payment/Customer Information (3.2):* Stores payment details and customer-specific information.
   c) *Control Signals, Activation Information, and Power Limits (3.3):* Stores control signals and power-related data, including activation information and power limits.
   d) *Energy and Power Usage, User Information, and Activation (3.5):* Maintains records of energy and power usage, as well as user and activation details.
   e) *Manufacturer Database (5.1):* Contains manufacturer-specific data necessary for charging operations and analysis.
4) *Data Flows:*
   a) Flows between entities, processes, and data stores, such as the flow of *User Information, Vehicle Information, and Certificates* from the *User* to the *AC/DC EV Charger* via *Customer Authentication*.
   b) Flows from the *AC/DC EV Charger (4.1)* to various data stores, such as *Control Signals, Activation Information, and Power Limits (3.3)*, and to external entities like the *CPO*.
5) *Main Components:*
   a) *AC/DC EV Charger (4.1):* Represents the physical charging unit that connects the EV to the power grid. In our case, the main component.

ACKNOWLEDGMENT

The opinions expressed are those of the author(s) only and should not be considered as representative of the European Commission's official position.

REFERENCES

[1] L. Anderson, D. Dobrygowski, and S. Rajachudamani, (World Econ. Forum, Cologny, Switzerland). *Cyber Resilience in the Electricity Ecosystem: Principles and Guidance for Boards*, Jan. 2019. [Online]. Available: https://www3.weforum.org/docs/WEF_Cyber_Resilience_in_the_Electricity_Ecosystem.pdf

[2] S. Soltan, P. Mittal, and H. V. Poor, "BlackIoT: IoT botnet of high wattage devices can disrupt the power grid," in *Proc. 27th USENIX Secur. Symp. (USENIX Secur.)*, 2018, pp. 15–32. [Online]. Available: https://www.usenix.org/conference/usenixsecurity18/presentation/soltan

[3] B. Huang, A. A. Cardenas, and R. Baldick, "Not everything is dark and gloomy: Power grid protections against IoT demand attacks," in *Proc. 28th USENIX Secur. Symp. (USENIX Secur.)*, 2019, pp. 1115–1132. [Online]. Available: https://www.usenix.org/conference/usenixsecurity19/presentation/huang

[4] T. Shekari, A. A. Cardenas, and R. Beyah, "MaDIoT 2.0: Modern high-wattage IoT botnet attacks and defenses," in *Proc. 31st USENIX Secur. Symp. (USENIX Secur.)*, 2022, pp. 3539–3556. [Online]. Available: https://www.usenix.org/conference/usenixsecurity22/presentation/shekari

[5] (IEA, Paris, France). *Global EV Outlook 2024*. Apr. 2024. [Online]. Available: https://iea.blob.core.windows.net/assets/a9e3544b-0b12-4e15-b407-65f5c8ce1b5f/GlobalEVOutlook2024.pdf

[6] (GridX, Walnut Creek, CA, USA). *Gridx Charging Report 2024*. (2024). [Online]. Available: https://gridx-public.s3.eu-central-1.amazonaws.com/gridX_Charging_Report_2024.pdf

[7] "New Study on accelerating EU electric vehicle charging infrastructure roll-out: European alternative fuels observatory." May 2024. [Online]. Available: https://alternative-fuels-observatory.ec.europa.eu/general-information/news/new-study-accelerating-eu-electric-vehicle-charging-infrastructure-roll

[8] (Fed. Highway Adm., Washington, DC, USA). *INVESTING IN AMERICA: Number of Publicly Available Electric Vehicle Chargers Has Doubled Since Start of Biden-Harris Administration*, Accessed: Sep. 11, 2024. [Online]. Available: https://highways.dot.gov/newsroom/investing-america-number-publicly-available-electric-vehicle-chargers-has-doubled-start

[9] (World Econ. Forum, Cologny, Switzerland, Boston Consult. Group, Boston, MA, USA). *Cyber Resilience in the Electricity Ecosystem: Principles and Guidance for Boards*. Jan. 2019. [Online]. Available: https://www3.weforum.org/docs/WEF_Cyber_Resilience_in_the_Electricity_Ecosystem.pdf

[10] "Frequency stability evaluation criteria for the synchronous zone of continental Europe: European network of transmission system operators for electricity." Mar. 2016. [Online]. Available: https://docstore.entsoe.eu/Documents/SOC

[11] (Iberdrola, Bilbao, Spain). Accessed: Apr. 26, 2024. *Puntos de recarga para coches eléctricos*. [Online]. Available: https://www.iberdrola.es/smart-mobility/puntos-de-recarga

[12] Mliu92. "IEC 62196-2 type 2 (plug)." 2021. [Online]. Available: https://commons.wikimedia.org/wiki/File:IEC_62196-2_Type_2_(plug).svg

[13] *Electric Vehicle Conductive Charging System*, IEC Standard 61851-1, 2023.

[14] M. Hubinský. "EVSE—Charging of electric vehicles." Sep. 2023, Accessed: Mar. 28, 2024. [Online]. Available: https://www.elso.sk/en/blog/technologies/evse-charging-of-electric-vehicles

[15] *Road Vehicles—Vehicle to Grid Communication Interface*, ISO Standard 15118-1, 2019.

[16] C. Cilleruelo, J. Junquera-Sánchez, L. De-Marcos, N. Logghe, and J.-J. Martínez-Herráiz, "Security and privacy issues of data-over-sound technologies used in IoT healthcare devices," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, 2021, pp. 1–6.

[17] J. A. Font, J. J. Gastelu, R. Gesteira, R. Palacios, and G. López, "Threat models for vulnerability analysis of IoT devices for manipulation of demand attacks," in *Proc. JNIC Cybersecur. Conf. (JNIC)*, 2023, pp. 1–8.

[18] S. Hernan, S. Lambert, T. Ostwald, and A. Shostack, (Microsoft, Redmond, WA, USA). *Uncover Security Design Flaws Using the STRIDE Approach*. Jul. 2019, Accessed: Mar. 28, 2024. [Online]. Available: https://learn.microsoft.com/en-us/archive/msdn-magazine/2006/november/uncover-security-design-flaws-using-the-stride-approach

[19] M. Howard and S. Lipner, *The Security Development Lifecycle*. Redmond, WA, USA: Microsoft Press, 2006.

[20] I. Gutiérrez, G. López, R. G. Miñarro, and R. Palacios, "Plataforma de demostración para ataques extremo a extremo de dispositivos con interfaz OBD-II," in *Proc. IX Jornadas Nacionales de Investigación en Ciberseguridad (JNIC)*, Sevilla, Spain, 2024, pp. 474–476. [Online]. Available: https://idus.us.es/items/9f1bbab8-670b-47f3-8b3e-7986279

[21] A. Khalid, A. Sundararajan, A. Hernandez, and A. I. Sarwat, "FACTS approach to address cybersecurity issues in electric vehicle battery systems," in *Proc. IEEE Technol. Eng. Manag. Conf. (TEMSCON)*, 2019, pp. 1–6.

[22] Z. Garofalaki, D. Kosmanos, S. Moschoyiannis, D. Kallergis, and C. Douligeris, "Electric vehicle charging: A survey on the security issues and challenges of the open charge point protocol (OCPP)," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 3, pp. 1504–1533, 3rd Quart., 2022.

[23] J. E. Rubio, C. Alcaraz, and J. Lopez, "Addressing security in OCPP: Protection against man-in-the-middle attacks," in *Proc. 9th IFIP Int. Conf. New Technol., Mobility Security (NTMS)*, 2018, pp. 1–5.

[24] D. Elmo, G. Fragkos, J. Johnson, K. Rohde, S. Salinas, and J. Zhang, "Disrupting EV charging sessions and gaining remote code execution with DoS, MITM, and code injection exploits using OCPP 1.6," in *Proc. Resil. Week (RWS)*, 2023, pp. 1–8.

[25] K. C. Patel and A. Patel, "Rogue access point: The WLAN threat," in *Proc. Int. Conf. Comput., Commun., Intell. Syst. (ICCCIS)*, 2022, pp. 943–950.

[26] S. I. Jeong and D.-H. Choi, "Electric vehicle user data-induced cyber attack on electric vehicle charging station," *IEEE Access*, vol. 10, pp. 55856–55867, 2022.

[27] B. Yang, L. Guo, and J. Ye, "Physics-based attack detection for traction motor drives in electric vehicles using random forest," in *Proc. IEEE Appl. Power Electron. Conf. Expo. (APEC)*, 2021, pp. 849–854

[28] R. P. Parameswarath, N. V. Abhishek, and B. Sikdar, "PREVENT: A mechanism for preventing message tampering attacks in electric vehicle networks," in *Proc. IEEE 97th Veh. Technol. Conf. (VTC)*, 2023, pp. 1–5.

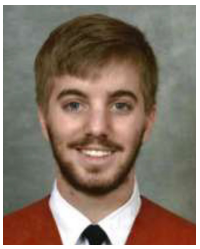
[29] M. Girdhar, J. Hong, H. Lee, and T.-J. Song, "Hidden Markov models-based anomaly correlations for the cyber-physical security of EV charging stations," *IEEE Trans. Smart Grid*, vol. 13, no. 5, pp. 3903–3914, Sep. 2022.

[30] S. K. Sonker, V. K. Raina, B. B. Sagar, and R. C. Bansal, "A cyber physical security for electrical vehicles using deep learning," in *Proc. Int. Conf. Autom. Comput. (AUTOCOM)*, 2024, pp. 519–523.

[31] Mliu92. "IEC 62196 type 2 (M, DC, CCS combo 2)." 2021. [Online]. Available: https://commons.wikimedia.org/wiki/File:IEC_62196_Type_2_(M,_DC,_CCS_Combo_2).svg

Javier Jarauta Gastelu received the B.S. and M.S. degrees in telecommunications engineering from Comillas Pontifical University (ICAI School of Engineering), Madrid, Spain, in 2022 and 2024, respectively, and the M.S. degree in cybersecurity from Comillas Pontifical University and Illinois Institute of Technology, Chicago, IL, USA, in 2024.

He contributed to research on cybersecurity of electric vehicle charging systems and high-power IoT devices as part of the European Commission Horizon Europe eFort Project with the Institute for Research in Technology. He is currently a Cybersecurity and an AI Consultant, focusing on the development of AI-powered static application security testing tools. His research interests include cybersecurity in critical infrastructure, reverse engineering, and AI applications in security.



Roberto Gesteira-Miñarro received the B.S. degree in telecommunications engineering and the M.S. degree in telecommunications engineering and cybersecurity from Comillas Pontifical University (ICAI School of Engineering), Madrid, Spain, in 2020 and 2022, respectively. He is currently pursuing the B.S. degree in mathematics and the Ph.D. degree in vehicle cybersecurity with Universidad Nacional de Educación a Distancia, Madrid.

He developed his master thesis with the Institute for Research in Technology regarding vehicle cybersecurity.

Dr. Gesteira-Miñarro received the Extraordinary Award from ICAI in 2020 and the Best Final Degree Project Award from COITT/AEGITT in 2021. He achieved Two Honorific Mentions, Two Bronze Medals, and One Silver Medal at the International Mathematics Competition. He also enjoys learning hacking and exploitation techniques in CTF platforms.

Javier Matanza (Domingo) received the M.Sc. degree in telecommunications engineering from the Universidad Politécnica de Valencia, Valencia, Spain, in 2008, and the Ph.D. degree in telecommunications engineering from Universidad Pontificia Comillas, Madrid, Spain, in 2013.

He is currently an Assistant Professor with the Department of Electronics, Automation, and Communications with the ICAI School of Engineering, Universidad Pontificia Comillas, and a Researcher with the Institute for Research in Technology, Madrid. He has co-authored the book *Smart Grid Telecommunications* (Wiley-IEEE Press, 2021) and has contributed to numerous peer-reviewed journals and conferences. His research interests include power line communications, signal processing, communication network simulation, co-simulation, demand response, medical monitoring communications, and smart grid technologies.

Rafael Palacios was born in Madrid, Spain, in 1966. He received the B.S. and M.S. degrees in mechanical engineering from the ICAI School of Engineering, Comillas Pontifical University, Madrid, in 1990, and the Ph.D. degree from Comillas Pontifical University, in 1998.

He joined the ICAI School of Engineering, as an Assistant Professor, and the Institute for Research in Technology, as a Researcher, in 1998. He obtained Tenure, in 2004, and became a Full Professor, in 2020. He has been the Head of the Programs in Telecommunications Engineering and Computer Science since 2012. He also helped to create the master's program in cybersecurity and was the coordinator from 2019 to 2021. He is a Frequent Visiting Professor with the Massachusetts Institute of Technology (MIT), Cambridge, MA, USA, where he carried out research with the Sloan School of Management from 2001 to 2002 and from 2024 to 2025, the Department of Aeronautics and Astronautics from 2009 to 2010, and the MIT Energy Initiative from 2017 to 2018. His areas of research include advanced data analytics and artificial intelligence applied to a wide array of fields, including anomaly detection, image processing and GIS, cybersecurity and privacy, telemedicine, and aviation safety.

Gregorio López received the Ph.D. in telecommunications engineering from Universidad Carlos III de Madrid, Madrid, Spain, in 2014.

He is currently an Associate Professor with the ICAI School of Engineering, Comillas Pontifical University, Madrid, where he also serves as the Coordinator of the Cybersecurity M.S., and as a Senior Researcher with the Institute for Research in Technology. He gathers wide experience in close-to-market research gained through his participation in more than 10 national and European research projects. As a result of his research activity, he holds a European Patent and has published more than 50 papers in top-tier conferences and journals, receiving more than 1500 citations. His current research interests revolve around cybersecurity in IoT/OT, AI for cybersecurity and cybersecurity in AI, human and technological factors in cybersecurity, and children and adolescents online, having been the coordinator of the European H2020 project RAYUELA (empoweRing and educAting YoUng pEople for the Internet by pLAying), which addresses this latter topic.