Physical-Layer Signal Injection Attacks on EV Charging Ports: Bypassing Authentication via Electrical-Level Exploits

Hetian Shi[1], Yi He[1], Shangru Song[1], Jianwei Zhuge[1], Jian Mao[2]

[1]Tsinghua University, Beijing, China

[2]Beihang University, Beijing, China

Email: shiht18@tsinghua.org.cn, clangllvm@126.com,

ssr22@mails.tsinghua.edu.cn, zhugejw@tsinghua.edu.cn, maojian@buaa.edu.cn

Abstract

The proliferation of electric vehicles in recent years has significantly expanded the charging infrastructure while introducing new security risks to both vehicles and chargers. In this paper, we investigate the security of major charging protocols such as SAE J1772, CCS, IEC 61851, GB/T 20234, and NACS, uncovering new physical signal spoofing attacks in their authentication mechanisms. By inserting a compact malicious device into the charger connector, attackers can inject fraudulent signals to sabotage the charging process, leading to denial of service, vehicle-induced charger lockout, and damage to the chargers or the vehicle's charge management system. To demonstrate the feasibility of our attacks, we propose PORTulator, a proof-of-concept (PoC) attack hardware, including a charger gun plugin device for injecting physical signals and a wireless controller for remote manipulation. By evaluating PORTulator on multiple real-world chargers, we identify 7 charging standards used by 20 charger piles that are vulnerable to our attacks. The root cause is that chargers use simple physical signals for authentication and control, making them easily spoofed by attackers. To address this issue, we propose enhancing authentication circuits by integrating non-resistive memory components and utilizing dynamic high-frequency Pulse Width Modulation (PWM) signals to counter such physical signal spoofing attacks.

Index Terms

Charging piles, Charging ports, Spoofing signal, Hardware Reverse Engineering

I. INTRODUCTION

The widespread adoption of EVs represents a transformative shift towards sustainable transportation, addressing environmental concerns and reducing dependence on fossil fuels. Meanwhile, new security issues [9], [13], [17] are emerging within the EV charging infrastructure. Unfortunately, as more EV chargers are deployed in cities, they become increasingly attractive targets for cyberattacks. Moreover, the complexity and diverse range of charging standards open the door to numerous vulnerabilities that could threaten both user safety and the stability of critical charging infrastructures [30].

Existing works [7], [18], [22] mostly focus on remote attacks. For instance, the Brokenwire attack [18] can disrupt the Combined Charging System (CCS) charging process by performing remote electromagnetic interference on the charger's programmable logic controller (PLC) to terminate the charging session. While Nasr et al. [22] and Vailoces et al. [28] both analyze vulnerabilities in the backend of electric vehicle supply equipment (EVSE) systems, including charge management platforms and network-level authentication, little attention has been paid to the physical-layer signaling protocols and port-level logic at the EV charger interface.

In this work, we investigate local attacks on charger piles and identify new common physical attack vectors that can exploit the weaknesses in the authentication process of several major charging standards. We demonstrate practicable physical signal injection attacks on various real-world charger pipes. By planting a small concealed hardware plugin onto the charging guns, attackers can inject control signals into the various ports of the guns. Specifically, by manipulating different ports with specific physical signals, attackers can launch: (1) Denial-of-service (DoS) attacks disrupting charging via Charging Confirmation (CC) / Control Pilot (CP) port manipulation; (2) Deadlock attacks spoofing impedance on the CC port, which can lockout the charging gun; and (3) PWM/CAN Bus signal injection attacks that can damage the EV battery, overloading the charging system, or inject malicious CAN Bus message to further exploiting the inner systems of vehicles. We prototype an attack hardware called PORTulator, which can be seamlessly integrated into the charger guns' ports and perform physical signal injection attacks. Unlike [6], which only showed a simple demo of authentication issues, our work is the first to fully study and exploit state forgery problems in several EV charging protocols. We show that attackers can tamper with the physical authentication process and then send fake CAN messages to the vehicle, which can bypass battery safety protections and cause overcharging.

We evaluate PORTulator on several real-world chargers and identify that 7 charging standards used by 20 charger piles are vulnerable to our attacks. Finally, we propose defensive strategies to mitigate these vulnerabilities, offering solutions that enhance the cybersecurity of EVSE systems. By integrating non-resistive memory components and utilizing dynamic high-frequency Pulse Width Modulation (PWM) power in existing charging authentication processes, the impedance is changed from fixed values to changeable values that are infeasible to be forged by attackers. Experiment results show that our solution can effectively counter the physical signals of spoofed attacks.

Here are the contributions of our work:

- We first identify critical vulnerabilities in the authentication mechanisms of various EV charging standards, allowing attackers to execute a charging process DoS attack, lock the charging port, manipulate discharge power, and potentially gain unauthorized access to internal systems such as the CAN Bus, posing significant security risks.
- We develop PORTulator, an attack suite that integrates a microcontroller unit (MCU), flexible printed circuit (FPC), and wireless communication, enabling covert connection to different charging standards and remote manipulation of vehicle charging port states for various attacks.
- We test PORTulator against multiple mainstream charging gun standards, demonstrating its practical effectiveness in real-world scenarios and providing three comprehensive case studies to highlight significant threats to vehicle charging safety.
- To address these vulnerabilities, we propose a defensive mechanism and validate it with real-world prototypes. Experimental results show that it can effectively prevent physical signal injection attacks.

Roadmap. This paper is organized as follows: § II presents the fundamental concepts of the EV charging process, establishing the technical groundwork for understanding vulnerabilities in the system. § III explores the weak authentication vulnerabilities associated with the CC & CP ports in EV Charging system. In § IV, we introduce PORTulator, a novel device that can be discreetly installed on different standards of charging guns, enabling various real-world attack scenarios. § V provides an in-depth demonstration of three practical attacks to validate the effectiveness of PORTulator. § VII reviews relevant research on signal spoofing and its impact on charging port security. In § VI, we propose two defense mechanisms against CC port

impedance manipulation and PWM signal spoofing. § VIII discusses the ethical considerations, limitations of PORTulator, and potential directions for future research. Finally, § IX summarizes the key findings regarding weak authentication vulnerabilities in EV charging systems.

II. Preliminaries

The advent of electric vehicles (EVs) as a sustainable alternative to traditional fossil fuel-powered automobiles has necessitated the development of a robust and efficient charging infrastructure. This infrastructure is supported by various charging port technologies and authentication protocols designed to facilitate EVs' safe and effective charging. The diversity in charging standards, including GB/T 20234(predominantly used in China), IEC EU (International Electrotechnical Commission) standards for European compatibility, SAE J1772 (common in the United States and other countries), NACS (North American Charging Standard) and the Combined Charging System (CCS) catering to both AC and DC charging, reflects the global effort to enhance EV accessibility and utility. Each standard specifies physical guns and electrical specifications, ensuring compatibility and safety across vehicles and charging piles.

A. *Security Risks in EV Charging System*

The EV charging process involves several key steps, beginning with the removal of the charging gun, which activates a wireless sensor and triggers the vehicle's charging port lid to open, as discussed in § II-C.

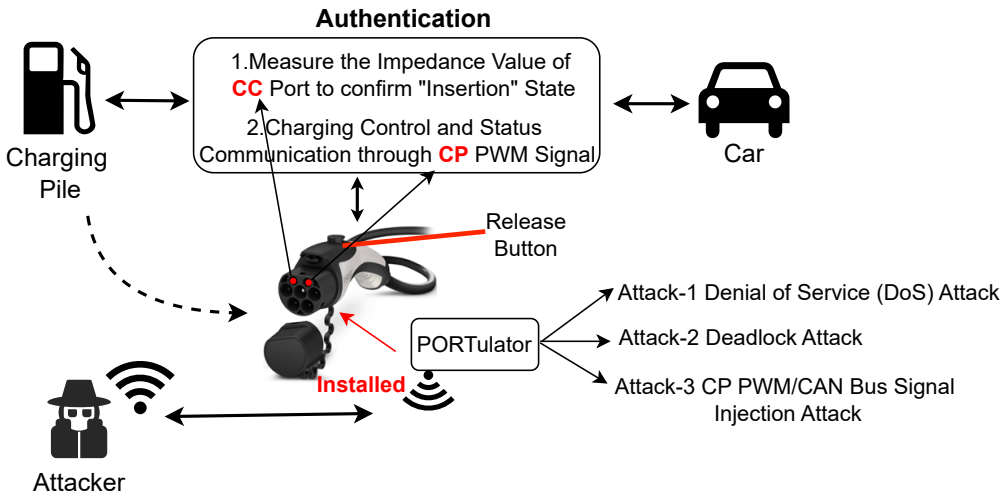


Fig. 1: Overview of PORTulator Attack Vectors on EV Charging Infrastructure

Once the charging gun is connected to the vehicle's charging port, a series of communications is initiated between the vehicle and the charging pile. The vehicle checks the **Charging Confirmation (CC)** port, **Proximity Pilot (PP)** port, or in the case of fast charging, the CC1 and CC2 ports, to verify the connection status of the charging gun. Once these ports detect a valid connection (i.e., the ports are no longer in an "open" state), the vehicle's charging port engages a locking mechanism that secures the charging gun in place. This lock, an electromechanical device, ensures that the charging gun remains firmly attached during the charging process. The details of this locking mechanism are further discussed in § II-D.

Furthermore, the vehicle transmits essential information, such as the Vehicle Identification Number (VIN) and frame number, to the charging pile through the Control Pilot (CP) port. This communication is particularly common with certain manufacturers. More critically, the CP port facilitates the exchange of the vehicle's status, required charging power, and current specifications to regulate the charging process.

Throughout the charging process, the vehicle and charging pile maintain continuous communication via the charging cable to ensure the charging process runs smoothly. Once the battery reaches full charge, the vehicle notifies the charging pile via the CP port to end the session. In public charging stations, after payment is processed, the user can disconnect the charging gun by pressing the release button on the gun, which deactivates the locking mechanism and allows the gun to be safely removed, as shown in Figure 1. The user then returns the charging gun to the pile and is free to leave.

B. Weaknesses in Chargers' Authentication Process

The authentication process begins when the charging gun is inserted into the vehicle's charging port. Typically, the user presses and releases a button on the gun, which not only physically engages the lock but also triggers a signal change in the internal circuit. Specifically, this action alters the signal on the CC line, signaling that the gun has been properly inserted into the vehicle's port. As shown in Figure 2 and Table I, all charging standards share a similar connection confirmation step during the authentication process.

However, this mechanism introduces a critical weakness. By spoofing the expected resistance on the CC line (highlighted in red), an attacker can trigger a "deadlock" condition: the EV mechanically locks the charging gun before any digital authentication occurs. Once locked,

further interaction is blocked, halting the process and creating a denial-of-service state. This flaw is present across standards, exposing a shared point of failure in physical-layer authentication.

Before electrical power is transferred, the system verifies the connection to ensure safety. A voltage detection point in the CC port circuit continuously monitors real-time changes to confirm the proper connection. Once the correct signal value is detected, the system advances to the next step: identification and the handshake protocol.

(a) GB/T AC GB/T 20234.2 (b) GB/T DC GB/T 20234.3 (c) NACS (d) SAE J1772

(e) CCS I (f) IEC 62196 (g) CCS II

Fig. 2: Charging Gun Standards (Signals from the ports, highlighted in red circles, confirm the proper connection between the EV and the charging pile.)

Identification and handshake between the charging pile and the vehicle are facilitated by the CP port, through which data packets are exchanged. These packets verify the identities of both the car and the charging pile, ensuring compatibility and preventing any electrical mistakes. During the process, the vehicle communicates its electrical requirements, which are cross-checked with the charging pile's capabilities. This prevents mismatches that could lead to unsafe conditions. In cases where the vehicle is part of a charging network or requires user authentication, the process may involve further communication with a central charging management system. This

ensures that the vehicle or user has the proper authorization to access the charging service. In some instances, this may include confirming payment authorization before charging begins.

Once authentication and authorization are complete, the vehicle transmits its specific charging needs to the pile, and the charging session begins. Continuous monitoring by both the vehicle and the pile ensures that electricity is delivered safely and efficiently, with adjustments made dynamically based on the vehicle's requirements and the charging pile's capabilities. At the end of the charging session, a final communication between the vehicle and the charging pile safely terminates the process. The charging port's locks are then disengaged, allowing the user to safely remove the charging gun.

C. Control Signals in Charging Pile

Wireless Signal for Opening the Charging Port Lid. Modern EVs often support wireless unlocking of the charging port lid to improve usability. This is commonly triggered when the user presses a button on the charging gun, which transmits a fixed wireless "open lid" signal to a receiver near the charging port.

As shown in Figure 3, we captured this signal from a NACS-standard charging gun using a HackRF One and GQRX. Each trigger emits ten identical packets, each containing a 26-bit sync word followed by three payloads, delimited by 3-bit guards. The last bit in the final packet is always '0', indicating transmission end.

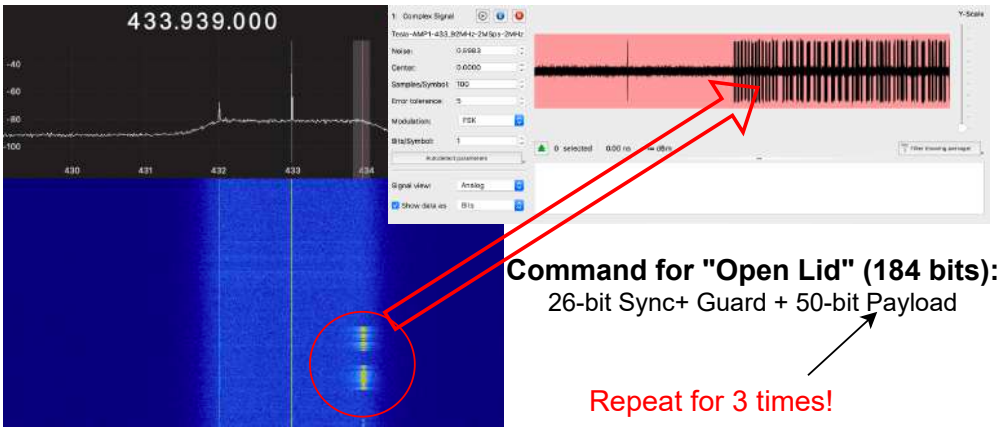


Fig. 3: Wireless Signal for "Open Lid"

Using Universal Radio Hacker (URH), we replayed this signal on multiple EV models, including Tesla Model S/Y and Volkswagen ID.4. In every case, the charging port lid opened

without needing any authentication. Notably, GB/T-compliant Tesla Superchargers in China use the exact same signal format.

This uniformity reveals a critical flaw: the wireless "open lid" command is a fixed, unauthenticated signal reused across platforms. As a result, an attacker with low-cost equipment can remotely gain physical access to the charging port, enabling further attacks on the vehicle's internal interface.

PWM Signal for Controlling Charging Current. A 1 kHz Pulse Width Modulated (PWM) signal is transmitted through the CP line to coordinate charging power. The duty cycle of this signal is defined as $DutyCycle = \frac{TimeON}{TotalPeriod} X 100\%$. It determines the proportion of time the signal remains high during each cycle and directly reflects the available current capacity [25]. For example, a 50% duty cycle typically indicates an available current of 32 A at 220–250 V AC, corresponding to approximately 7–8 kW of charging power.

The vehicle interprets both the duty cycle and the peak voltage level of the CP signal to determine the operational state, such as *standby*, *charging*, *ventilation required*, or *error* [1], [2], [4]. Further details on the authentication and signal interpretation process are discussed in Section III-B.

D. Safety Measures for EV Charging

Ensuring charging safety is essential for both EVs and chargers due to the high operating voltages. To address this issue, vendors have implemented several safety measures, including emergency switches, electromechanical locks, and temperature sensors. In this section, we focus on two key safety features found in modern charging systems: **electromechanical locks** and **temperature sensors**, both of which work together to ensure safe and uninterrupted charging.

Electromechanical Locks for Preventing Electrical Hazards. Electromechanical locks are a fundamental safety measure implemented across various charging standards, including GB/T, IEC, SAE J1772, NACS, and CCS [3], [10], [27], [33]. These locks provide a physical layer of security by preventing the charging gun from being accidentally disconnected during the charging process. This is especially important given that the voltage used in EV charging systems far exceeds the typical safety threshold for humans and animals, which is around 36V.

Once the charging gun is connected and the vehicle detects the correct CC port voltage, the lock engages, ensuring that the charging gun remains securely in place throughout the session. This prevents accidental disconnections and potential exposure to high voltage. In addition to

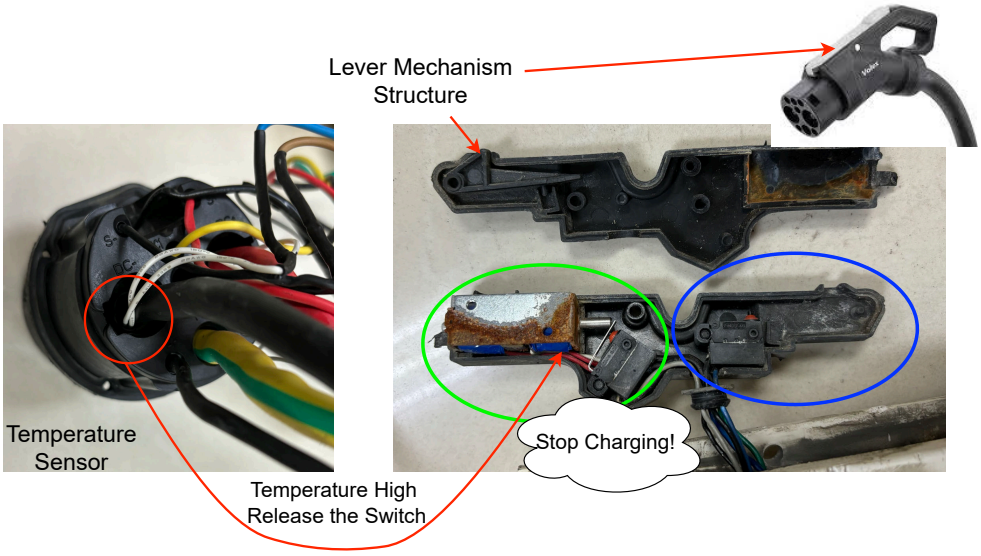


Fig. 4: Automatic Triggering of High-Temperature Protection Switch

safeguarding users from electrical hazards, the lock ensures continuous power transfer, which is essential for both safety and efficient charging.

As shown in Figure 4, the travel switch in the blue circle monitors the connection status of the charging gun. When the ”Unlock” button is pressed, the lever mechanism moves from a pressed to a raised state, causing the impedance between the CC1 and PE ports to drop to $0\ \Omega$, signaling to the vehicle that the charging gun is ready to be removed. This ensures that the system correctly disengages the electronic lock and ends the charging session safely.

Temperature Sensors for High-Temperature Protection. In addition to electromechanical locks, temperature sensors play another vital role in ensuring the safe operation of EV charging systems. According to standards such as IEC 62196 and GB/T 20234.3 for DC fast charging, the internal temperature of the charging system must not exceed 90°C. Overheating can lead to significant safety risks, including damage to both the vehicle battery and the charging equipment, making temperature monitoring a key safety feature.

As shown in Figure 4, temperature sensors (highlighted in red) are strategically placed inside the charging gun to continuously monitor heat levels. If the temperature exceeds the safety threshold, these sensors trigger an automatic response. The thermal protection mechanism (marked in green) activates the motor, causing the left travel switch to close. This sends a stop signal to the charging pile, halting the charging process to prevent further overheating.

III. Overview

A. Motivation

The global adoption of EVs has accelerated the deployment of diverse charging infrastructures. Meanwhile, this rapid expansion introduces new security risks, especially in the physical and signaling layers of EV–charger communication [18]. Recent research has identified a weak authentication vulnerability in the GB/T 20234.2 standard [6], which enables adversaries to manipulate resistance values in the charging confirmation (CC) port, thus inducing unauthorized state transitions or even deadlocks between vehicles and charging piles.

However, the potential impact of such attacks remains unclear, especially given the diversity of charging standards. A critical question arises: Can malicious signals be injected across all charging standards, and if so, what are the broader consequences? Beyond simply disrupting charging, could such attacks target an EV's charging management system or even inject malicious commands into the EV's internal data bus? To address these concerns, we conduct an empirical study to investigate whether more devices with diverse charging standards are vulnerable to physical signal injection attacks and explore whether these attacks could result in more severe consequences.

B. Weak Authentication Vulnerabilities in Charging Port

Authentication mechanisms in EV charging protocols are designed to prevent unauthorized access to vehicle charging functions. However, our investigation reveals that several widely adopted standards rely on weak signal level authentication [5], where charging state transitions are determined by analog parameters such as port impedance or PWM duty cycles, without any cryptographic validation. This architectural assumption leaves room for adversaries to spoof authentication signals and gain unauthorized control over the charging process. Figure 5 illustrates a typical falsified signal attack that exploits this weakness.

To explore this vulnerability, we begin by reverse engineering the internal signal circuits of several representative charging guns. In an initial study of a GB/T AC charging gun, we use a multimeter to probe the impedance of the CC line and identify an unexpectedly simple configuration consisting of only two resistors and a mechanical travel switch. Although this demonstrates the feasibility of spoofing CC signals by manipulating resistor values, we also note the risk of signal coupling between ports. To better understand the design, we disassemble the

gun and confirm that the authentication logic relied purely on passive resistance and mechanical actuation, with no built-in tamper detection.

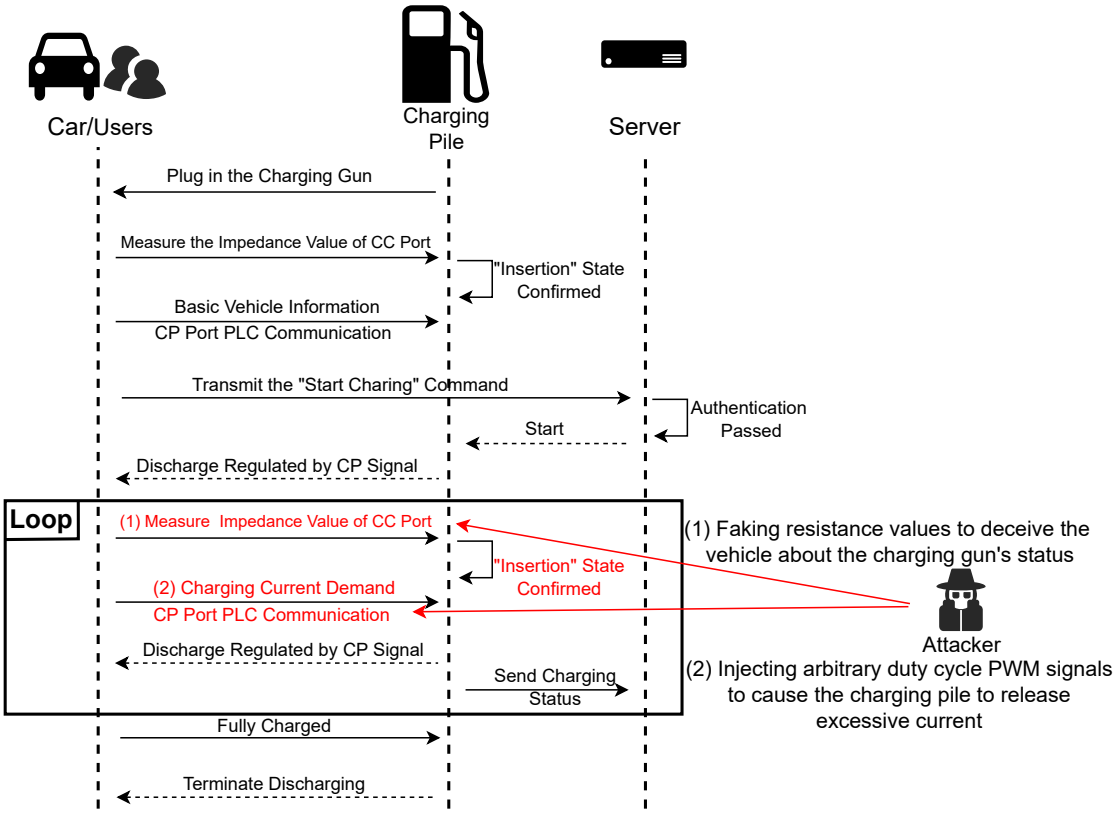
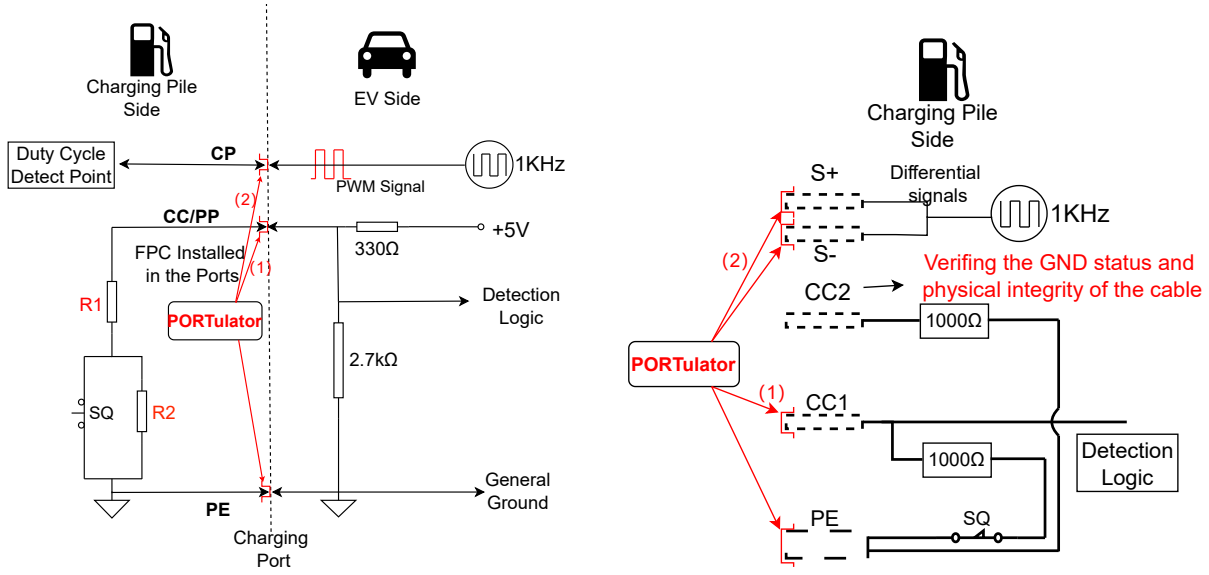


Fig. 5: Falsified Signal Attack Exploiting Weak Authentication in Charging Protocols

Since many commercial charging guns employ anti-tamper designs that hinder physical disassembly, we developed PORTulator, a non-invasive port analysis tool capable of automatically identifying internal electrical characteristics. By interfacing with multiple charging gun ports, PORTulator can assess port isolation, impedance values, and the presence of memory components such as capacitors or inductors, without opening the casing. This allows us to extract authentication logic from devices across multiple standards in a repeatable and scalable manner.

Figure 6 shows the typical internal signal circuits for slow and fast charging guns, which were mapped using our automated method. These diagrams reveal that signal-based authentication remains consistent across protocols: electrical states are inferred through analog conditions, rather than protocol-level cryptographic handshakes.

Building on this insight, we designed a signal spoofing attack targeting these weak authentication mechanisms. The attack involves mimicking the electrical signatures that represent various



(a) Slow Charging Gun Authentication Circuit

(b) Fast Charging Gun Authentication Circuit

Fig. 6: Comparison of Slow and Fast Charging Gun Authentication Circuits

charging states. For example, as summarized in Table I, changing the resistance value on the CC line can simulate events such as plug insertion, button press, or user confirmation. By replicating these states, an attacker can deceive the charging pile into initiating or continuing a charging session without authorization.

To construct these spoofed signals, we first used PORTulator to capture reference waveforms and parameter ranges during normal charging sessions. This included measuring resistance transitions, PWM frequencies, and voltage thresholds under different operational states. Based on this data, we generated counterfeit signals using a programmable MCU that emulates the behavior of a legitimate EV-side interface. These signals are then injected into the CC or CP ports at specific phases of the charging handshake to trigger unauthorized transitions.

Since the charging pile relies solely on analog signal conditions for authentication, it is unable to distinguish between genuine and spoofed interactions. As a result, the attacker can initiate, manipulate, or deadlock the charging process, even without any access to cryptographic credentials or prior pairing with the vehicle.

C. Threat Model

We consider a realistic adversary targeting public EV charging infrastructure, which is widely deployed in semi-supervised environments such as parking lots, apartment complexes, and service

stations. These locations often lack strict physical supervision, allowing attackers **short-term access** to charging equipment. This model reflects real-world scenarios observed in similar physical-layer attacks, such as ATM skimming [8], [24] and RFID spoofing [19], where covert hardware can be deployed without attracting attention.

The attacker is assumed to have brief physical access to a charging gun, either during their own charging session. Leveraging this opportunity, the attacker discreetly installs a modified version of PORTulator, which embeds signal injection hardware into the head or sheath of the charging gun. The device remains dormant until remotely triggered via wireless communication.

Once a victim connects their vehicle to the compromised charging gun, the attacker activates the device to inject falsified CC or CP signals. These spoofed signals exploit weak authentication mechanisms to induce denial-of-service conditions, lock the charging port, or manipulate current flow. In standards such as GB/T 20234.3 and NACS, the attack may further escalate to in-vehicle CAN Bus injection via exposed communication lines.

This threat model does not assume firmware modification or charger disassembly. Instead, it demonstrates that brief, opportunistic access-combined with a camouflaged device, can enable powerful attacks in realistic public settings.

IV. PORTULATOR DESIGN

To verify if the chargers are vulnerable to physical signal injection attacks, we propose PORTulator, a customize hardware platform based on the RP2040 Microcontroller Unit (MCU) [23], designed to uncover and exploit signal-level vulnerabilities in EV charging infrastructures. This device enables remote and precise manipulation of physical-layer communication between electric vehicles and charging piles, supporting real-world spoofing and injection attacks.

A. Hardware Design

The core of PORTulator is a compact, modular spoofing device—PORTulator —built to physically interface with the CC and CP lines of standard EV charging guns. As shown in Figure 7, the system is powered by an RP2040 MCU, chosen for its real-time control capabilities, low-latency GPIO access, and flexible ADC/DAC integration.

The PCB is designed to interface directly with both analog signaling pins (CC/CP) and digital monitoring subsystems. A programmable potentiometer (AD5160 module) is included to emulate impedance-based logic states on the CC line, while a PWM-capable GPIO output

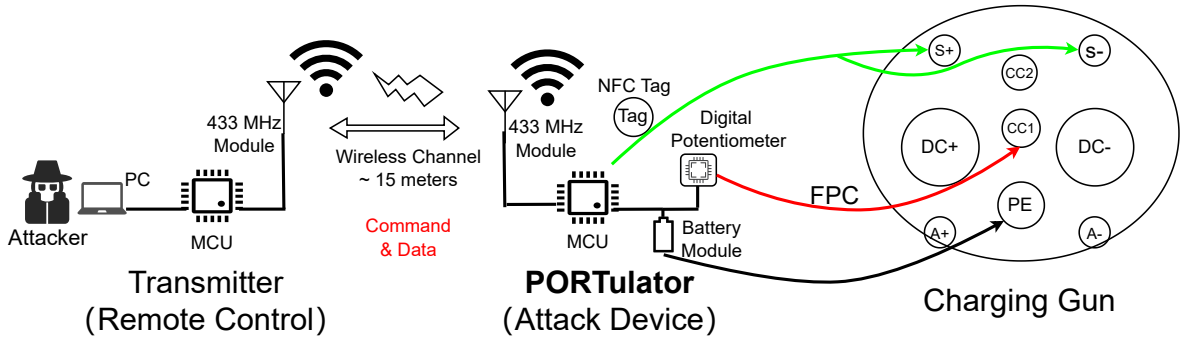


Fig. 7: Design of PORTulator for Resistor Spoofing & Signal Injection

pin synthesizes the CP signal to reflect various charging states. To allow for remote-controlled behavior, the hardware integrates a 433ṀHz wireless receiver (GC433-TC007) that accepts over-the-air commands from an Arduino-based controller. This setup enables dynamic payload delivery, such as adjusting resistance values or toggling CP duty cycles, effectively changing the perceived EV state in real-time.

The physical device is encapsulated in a modified charging gun shell. Specifically, a thin custom cable is routed through the charging gun to the CC pin, internally connected to a pre-configured resistor, and routed through an insulating sleeve to avoid interfering with normal charging pile operations. A small metal ring is used to stabilize the CC contact position. This modification is minimally intrusive, does not affect standard charging under normal conditions, and is nearly invisible from the outside, making the attack device covert and practical for deployment in semi-public scenarios. In addition, the compact design enables rapid installation: the entire module can be integrated into a fake adapter or portable testing tool and clipped onto the target charging gun in under 90 seconds, minimizing the attacker's exposure time on-site.

Figure 8 shows the physical construction of the prototype. All components used are off-the-shelf and reproducible: the microcontroller board (RP2040), AD5160 potentiometer, GC433 wireless module, and the modified charging gun enclosure. PORTulator's hardware setup and open-sourced code is provided at: https://github.com/Vehicle-Security.

B. Signal Interpretation & Injection Principles

The design of PORTulator is grounded in the signal-level understanding of EV charging protocols, particularly the logic interpretation on CC and CP lines. As illustrated in Figure 9,

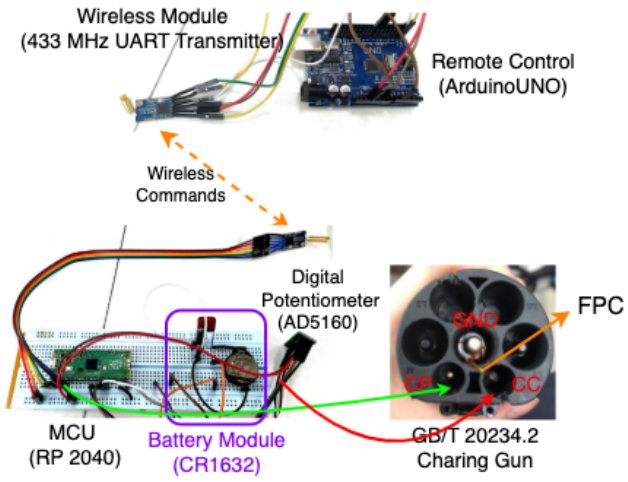
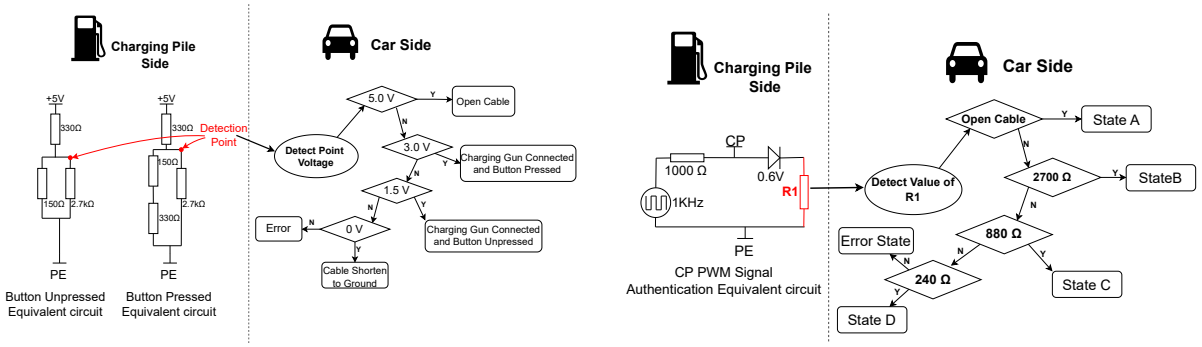


Fig. 8: Physical Prototype of the PORTulator Attack Device

our system mimics legitimate interactions by matching impedance and PWM behaviors expected during the communication phase.



(a) Impedance-Based Logic for CC Port Status

(b) PWM Signal-Based Logic for CP Port Status

Fig. 9: Parameter Values and Logical State Determinations at the CC Port (a) and CP Port (b) of EV Charging Gun

- **Impedance-Based Logic for CC Port Status.** The CC pin voltage is determined by a resistive voltage divider formed between the EV's internal pull-down resistor and a fixed resistor inside the charging gun, often connected through a travel switch linked to the physical button. As shown in Figure 9a, the EV measures the voltage between the detection point (CC port) and GND to infer the connection state: 5 V indicates an open cable, 3 V means the charging gun is connected and the button is pressed, 1.5 V indicates connected but unpressed, and 0 V signals a fault or short condition.

- **PWM Signal-Based Logic for CP Port Status.** The CP line enables the charger to determine the vehicle's connection and charging states based on the equivalent resistance R_1 presented between the transistor and ground, as shown in Figure 9b. In the default unconnected state (State A), no resistor is applied, and the charger interprets this as "cable not connected." Upon physical connection (State B), the vehicle applies a $2.74k\Omega$ pull-down resistor to indicate the presence of the EV without charging intent. When the vehicle is ready to charge (State C), it adds a $1.3k\Omega$ resistor in parallel, forming an equivalent resistance of approximately 880Ω. This resistance signals to the charger that charging is authorized. Only in State C does the vehicle actively respond by modulating the CP line with a 1k̇Hz PWM signal. The duty cycle of this signal encodes the maximum allowable charging current (e.g., 50% for 32A, 85% for 51A). Additionally, certain implementations apply a 240Ω equivalent resistance to indicate DC charging with forced ventilation requirements. Any deviation from the expected resistance values, such as short or undefined configurations, results in a fault condition (State D). Overall, the EV communicates its charging state not by direct signaling, but by dynamically altering the resistance on the CP line.

To ensure compatibility across various charging standards, we systematically reproduced the expected impedance values used to signal connection states. As shown in Table I, PORTulator precisely emulates these reference resistances, with minimal deviation, to maximize spoofing success across a range of charging standards. This calibration enhances cross-standard reliability and enables consistent behavior in both AC and DC charging scenarios.

Standard	**Unpressed Status (Expected Impedance)**	**Real Impedance (Deviation Ω)**	**Pressed Status (Expected Impedance)**	**Real Impedance (Deviation Ω)**
SAE J1772	480 Ω	487 (+1.5%)	150 Ω	145 (-3.3%)
CCS I	480 Ω	487 (+1.5%)	150 Ω	145 (-3.3%)
IEC 61851	1030 Ω	1027 (-0.3%)	760 Ω	768 (+1.1%)
CCS II	1030 Ω	1027 (-0.3%)	760 Ω	768 (+1.1%)
NACS	460 Ω	466 (+1.3%)	400 Ω	390 (-2.5%)
GB/T 20234.2	220 Ω	210 (-4.5%)	3520 Ω	3511 (-0.3%)
GB/T 20234.3	0 Ω	0 (0%)	1000 Ω	1003 (+0.3%)

TABLE I: Comparison of Expected and Spoofed Impedance Values Across Different Charging Standards

C. Adaptive Control & Attack Interface

The adaptive control and attack interface of PORTulator is designed to facilitate real-time manipulation of spoofed signals during an ongoing attack. This interface integrates both low-level hardware control and a high-level user interface to enable precise and efficient execution of various spoofing scenarios.

At the hardware level, the MCU is responsible for processing incoming commands and adjusting signal outputs accordingly. These commands, typically sent in the form of HEX codes over a 433MHz wireless link, instruct the MCU to modify key signal parameters such as resistance on the CC line or duty cycle on the CP line. For instance, issuing a command to set the CC line resistance to a specific value allows the device to mimic the "charging plug inserted" or "charging authorized" states, effectively manipulating the EV-side logic as perceived by the charging pile. In addition to active control, the system supports real-time monitoring of the charging pile's behavior during the attack. Embedded sensors measure key electrical parameters such as voltage and current, while communication feedback channels track the pile's response to spoofed signals.

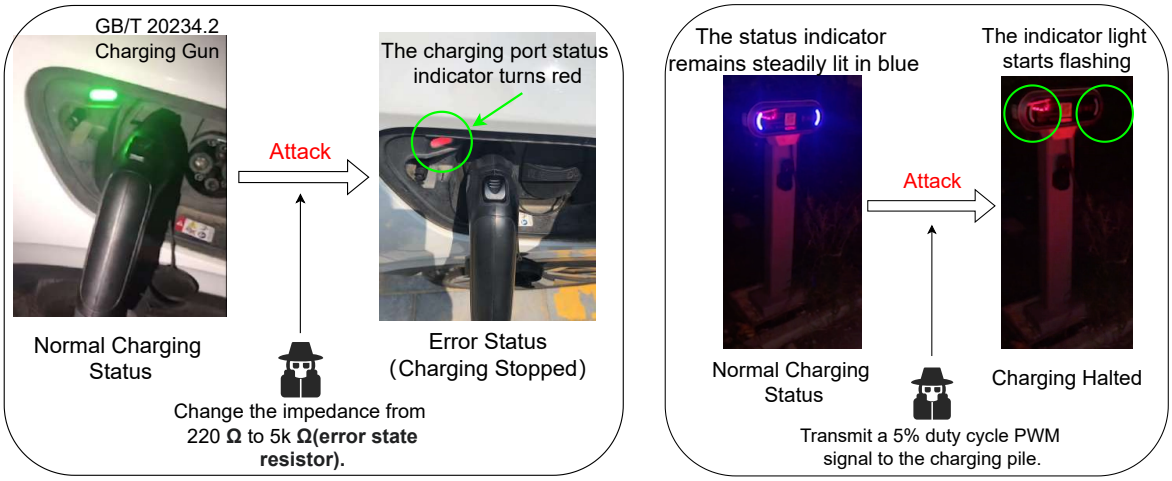
V. Evaluation

In this section, we evaluate the effectiveness of PORTulator across three key physical-layer attack scenarios: (1) inducing Denial-of-Service (DoS) conditions by manipulating the CC and CP lines, (2) spoofing resistor values to deadlock the charging gun in ransom-style attacks, and (3) injecting malicious PWM signals to manipulate charging behavior. We further explore the potential for higher-layer CAN Bus injection via the charging interface.

Specifically, PORTulator successfully executed all three attacks across seven EV models and six major charging standards in Table II, including GB/T 20234.2, GB/T 20234.3, CCS I, CCS II, NACS, and IEC 62196. These results highlight systemic weaknesses in EV charging infrastructures and underscore the need for stronger signal validation mechanisms across physical and communication layers. Detailed information can be accessed at https://github.com/Vehicle-Security.

A. Case I: DoS Attack

EVs continuously monitor the physical state of the charging gun during charging to ensure safe operation under high-voltage and high-current conditions. Disruptions in the connection, such as improper insertion or unexpected impedance changes, are treated as critical events and



(a) DoS on CC to Disrupt Charging Process

(b) DoS on CP to Control Charging State

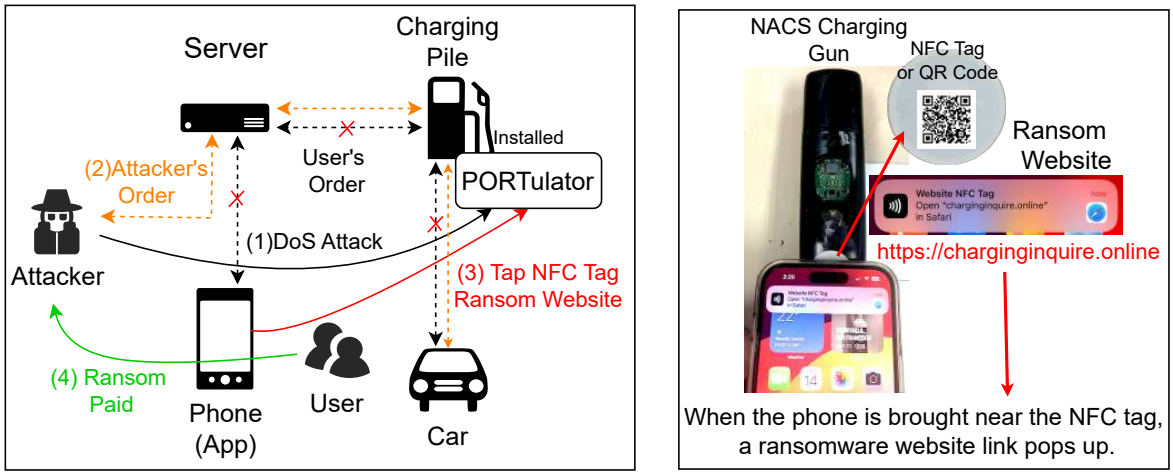
Fig. 10: DoS Attacks on CC and CP Lines in EV Charging Systems

will immediately halt the charging process. As shown in Figure 10a, our attack leverages this safety mechanism by exploiting the capabilities of PORTulator, as detailed in § IV. Specifically, attackers can remotely alter the CC line impedance to abnormal values, for instance, reducing it to 0 Ω or increasing it to simulate a disconnected state. This results in the charging pile immediately terminating the session. We validated this behavior on multiple vehicles, including the Volkswagen ID.4 and Tesla Model S. By pre-installing PORTulator on public charging piles, an attacker could remotely issue commands across various charging standards to launch broad DoS attacks.

Moreover, the CP line can also be targeted. As shown in Figure 10b, injecting a low-duty-cycle PWM signal, such as 5%, can mislead the charging pile into interpreting the session as inactive communication or fault, further halting power delivery. This method offers another vector for reliably disrupting active charging sessions without requiring direct physical interaction.

B. Case II: Deadlock Attack via CC Port Impedance Manipulation for Ransomware Exploitation

We further explore a novel form of ransomware attack that manipulates CC line impedance to trap the charging gun in a locked state, thereby immobilizing the EV and coercing users into making payments to regain control. Crucially, this attack does not rely on internet connectivity, distinguishing it from conventional ransomware campaigns [6].



(a) Deadlock Attack Applied to Ransom Attack

(b) NFC Triggered Ransom Website Pop-up

Fig. 11: Deadlock Attack and NFC-Triggered Ransom Scenario

As illustrated in Figure 11a, the attack unfolds in four stages: (1)**DoS Attack**: The user initiates a legitimate charging session by connecting to a gun embedded with PORTulator. The attacker then remotely triggers a DoS condition (as outlined in § V-A), halting the process by injecting abnormal signals on the CC or CP line. (2)**Forged Charging Order Replay**: Following disruption, the attacker replays captured CP signals from a previously observed session, initiating a new charging order that appears valid but is under attacker control (see § V-C). (3)**Ransom Prompt via NFC or QR Code**: When the user returns and attempts to stop the session or remove the charging gun, they find the interface unresponsive. Simultaneously, an NFC tag embedded in the charging gun, along with an optional QR code displayed on a sticker, triggers a prompt on the user's smartphone, as shown in Figure 11b. This prompt opens a spoofed support webpage, such as "https://charginginquire.online", carefully designed to resemble a legitimate vendor site. Devices lacking NFC support can instead scan the QR code, which contains the same redirection metadata referencing NFC. (4)**Payment Demand**: The spoofed website informs the user that their charging session and thus their vehicle is locked. Instructions are provided to make a cryptocurrency or an anonymous payment to resume normal operation. This step effectively turns the charging infrastructure into a physical lever for extortion.

We successfully demonstrated this attack on a Volkswagen ID.4 using public charging piles operated by TELD and Starcharge in China. The exploit highlights a deeply concerning capability: attackers can gain remote control over EVs' charging states, using infrastructure-side

spoofing and interface deadlocks to extract payments from unsuspecting users. This underscores the urgent need for more robust authentication mechanisms, secure session management, and out-of-band validation to prevent such attacks. Detailed information and demo videos can be accessed at https://github.com/Vehicle-Security.

C. Case III: CAN Bus Signal Injection Attack

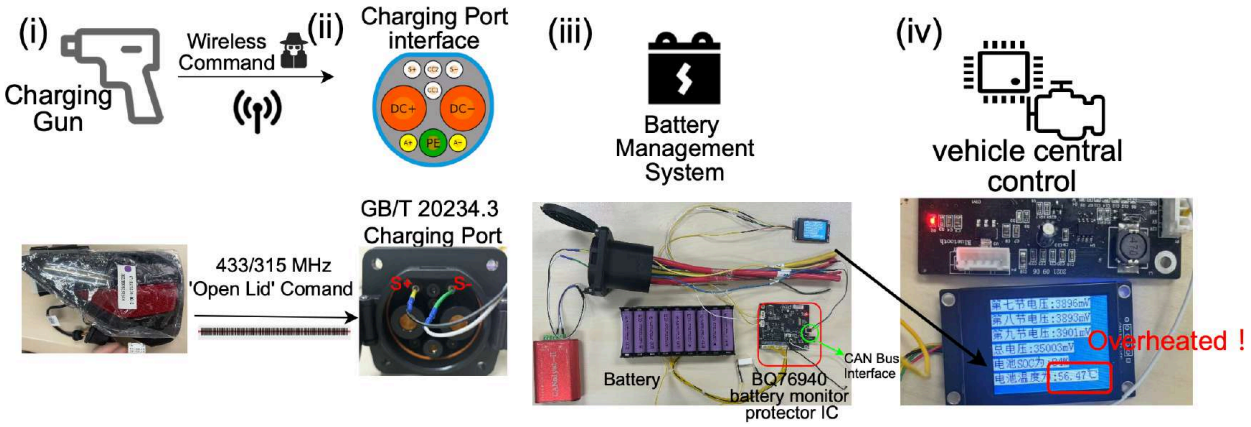


Fig. 12: CAN Bus Signal Injection Attack Overview

We explore how CAN bus injection can cause functional compromise of battery management systems (BMS). As shown in Figure 12, the attack begins with the replay of the wireless signal used to open the EV charging port, thereby enabling physical access to the S+/S– communication lines defined in the GB/T 20234.3 standard. These lines are commonly connected to CAN bus-based charging controllers in vehicles such as Denza, BYD, XPeng, and Arcfox.

To simulate a realistic vulnerability, we built a prototype BMS using the TI BQ76940 battery monitor IC and an STM32F103 MCU, both widely adopted in commercial EVs. The BMS is designed to disconnect charging MOSFETs when the battery temperature exceeds 40 $^{\circ}C$. However, we discovered a stack buffer overflow vulnerability triggered by a specific multi-stage CAN message sequence.

Our proof-of-concept payload bypasses this protection by overwriting control register values, resulting in the MOSFET remaining active even under overheating conditions. In our testbed, this led to continued charging until the battery temperature reached 56.47 $^{\circ}C$, significantly exceeding the defined thermal threshold. This results in forced charging even under unsafe thermal conditions, with our testbed reaching a battery temperature of 56.47 $^{\circ}C$ in the red box.

This demonstrates a critical safety violation caused by code-level flaws reachable via external CAN access.

Although this experiment is conducted in a simulated environment, its architecture reflects real-world systems. For instance, Tesla's Model S uses a Chargeport ECU that communicates via CAN with internal energy control modules, and lacks strict isolation between the charger-side and internal buses. Our findings suggest that in the absence of proper message authentication or bus isolation, similar injection-based attacks may compromise safety-critical subsystems across various EV platforms. This case study illustrates that CAN bus injection attacks can lead to persistent and dangerous failures, not just momentary service denial, thus exposing a deeper layer of risk within the EV charging ecosystem.

D. Attack Efficacy

We evaluated the efficacy of the proposed attacks across a range of EV models and charging port standards. Table II summarizes our findings in a controlled test environment, demonstrating the real-world feasibility of the attacks conducted using PORTulator.

DoS Attacks. The DoS attack proved to be universally applicable across all tested vehicle models and charging standards. By manipulating the CC or CP port impedance, PORTulator consistently triggered the termination of the charging process.

CP PWM Signal Injection. This attack was similarly effective across all configurations, enabling unauthorized control over charging state transitions. In some cases, we observed the ability to start or interrupt charging by replaying or injecting low-duty-cycle PWM signals.

Deadlock Attacks. Unlike the above two, the deadlock attack showed dependency on the physical locking mechanism of the charging interface. Specifically, Tesla Model 3 and Li Auto L7 vehicles equipped with CCS II ports did not exhibit a lock-based constraint and were therefore not susceptible to this attack vector. Other models with electronic locking mechanisms experienced successful deadlock scenarios.

CAN Bus Injection. Finally, the feasibility of CAN bus message injection was contingent on the standard and vehicle design. Only NACS and GB/T 20234.3-based implementations exposed interfaces through which CAN frames could be observed or injected via the charging interface. In contrast, vehicles relying on CCS or SAE J1772 lacked accessible interfaces for direct CAN interaction, preventing this type of exploitation.

Car Models	Charging Ports Standard	DoS Attack	Deadlock Attack	CP PWM Injection Attack	Potential CAN BUS Injection Attack
Tesla Model S	NACS	✔	✔	✔	✔
	SAE J1772	✔	✔	✔	✘
	CCS I	✔	✔	✔	✘
	GB/T 20234.2	✔	✔	✔	✘
	GB/T 20234.3	✔	✔	✔	✔
Tesla Model 3	GB/T 20234.2	✔	✔	✔	✘
	GB/T 20234.3	✔	✔	✔	✘
	IEC 62196	✔	✔	✔	✘
	CCS II	✔	✘	✔	✘
Tesla Model Y	NACS	✔	✔	✔	✔
	IEC 62196	✔	✔	✔	✘
	CCS II	✔	✔	✔	✘
Volkswagen ID.4	GB/T 20234.2	✔	✔	✔	✘
	GB/T 20234.3	✔	✔	✔	✔
ROEWE RX5	GB/T 20234.2	✔	✔	✔	✘
	GB/T 20234.3	✔	✔	✔	✘
ARCFOX αS	GB/T 20234.2	✔	✔	✔	✘
	GB/T 20234.3	✔	✔	✔	✘
Li Auto L7	IEC 62196	✔	✔	✔	✘
	CCS II	✔	✘	✔	✘

TABLE II: Effectiveness of Attacks Across Car Models and Charging Standards

Overall, the results confirm that while some attacks are universally effective, others rely on specific hardware designs or protocol implementations. These findings highlight the urgent need to reassess the security assumptions in current EV charging architectures.

VI. Countermeasures

To address vulnerabilities arising from weak authentication in EV charging systems, we propose a more robust, twofold countermeasure that enhances traditional impedance-based methods. Traditionally, EV charging authentication employs a fixed voltage source and a resistor-divider for impedance validation. As shown in Figure 6, this approach is limited in resisting sophisticated spoofing attacks.

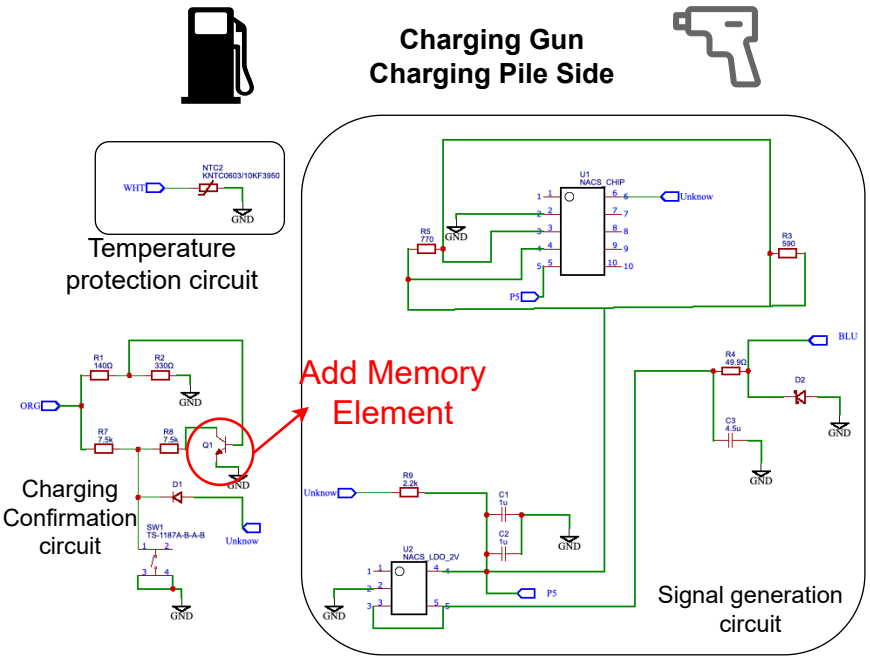


Fig. 13: Solution-I: Memory Elements on Charging Gun Side

Our solution introduces a **dual-check process** combining the legacy fixed voltage approach with a dynamic signal source. The addition of a variable power source enables comparative analysis of both static and dynamic signal responses, enhancing anomaly detection during authentication.

Security is further reinforced through memory-capable components integrated into the circuit (highlighted in red in Figure 13), replacing traditional resistors with transistors and capacitors. This is inspired by Tesla's CC circuit design [5], [27]. The added complexity alters signal behavior under varying frequencies, thwarting spoofing attempts with fixed resistors.

This design ensures that signals observed through a basic resistor-divider differ significantly from those under dynamic excitation, as shown in Figure 14. Frequency-sensitive components cause impedance shifts: $Z_{\text{transistor}} = j2\pi fL$ and $Z_{\text{capacitor}} = \frac{1}{j2\pi fC}$. A variable signal source modulates these properties, making attacker replication exceedingly difficult.

By introducing signal variability and component complexity, our method surpasses static resistance checks by adding unpredictability to the validation process and significantly enhancing security. To further strengthen authentication, we propose integrating a lightweight wireless energy transmission module (e.g., RF/NFC) for out-of-band signal generation. This additional channel enables active tamper detection: any deviation from the expected signal response, under

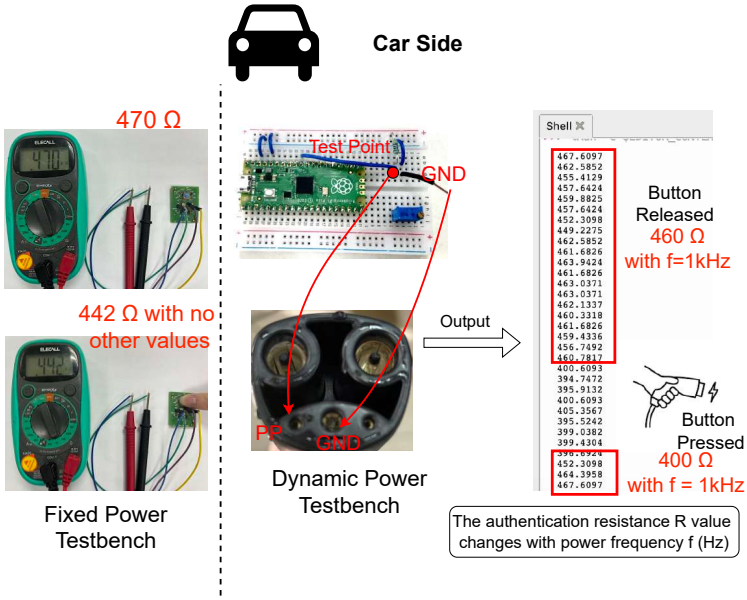


Fig. 14: Solution-II: Dynamic Power Source on EV Side

both static and dynamic conditions, can trigger alarms for manual inspection. Combined with anomaly detection in circuit signal characteristics, this integrated approach provides robust protection against spoofing attempts and reinforces the resilience of EV charging systems against sophisticated attacks.

VII. Related Works

As EVs become increasingly widespread, the security of EVSE has gained critical attention. A growing body of research has investigated vulnerabilities across the charging infrastructure, from remote attacks to physical-layer threats.

Network-based EVSE Vulnerabilities. Vailoces et al. [28] provided a broad analysis of vulnerabilities in EVSE systems, including weak backend authentication and insecure end-to-end communication. Their work outlines several attack scenarios and corresponding countermeasures, primarily at the backend server and network level. In contrast, our work presents the first in-depth analysis and exploitation of state forgery vulnerabilities in the front-end charging protocol between EV and charger, extending the attack surface to include physical and protocol-layer manipulation that can induce denial-of-service, deadlock, and in-vehicle CAN bus injection.

Johnson et al. [16] explored remote spoofing attacks on EV chargers and highlighted weaknesses in authentication flows. While their analysis remains at the simulation level, our study

moves beyond theoretical models by building hardware-based attack prototypes and conducting real-world experiments against multiple EV models.

Several studies have investigated publicly accessible EVSE infrastructure. Varriale et al. [29] and Hille et al. [12] demonstrated that many chargers are discoverable via Shodan and contain outdated firmware, weak credentials, or insecure web interfaces. While these works uncover accessible attack surfaces, our research introduces novel exploitation methods that directly interact with the CP/CC analog signaling to induce misbehavior, representing a more proactive and low-level attack vector.

Liu et al. [20] proposed blockchain-based authentication and logging systems to protect EV charging records. While effective for securing data integrity, their approach does not address the physical-layer or analog signaling vulnerabilities we exploit.

Physical Layer EVSE Attacks. Baker et al. [7] presented credential-stealing attacks via wireless eavesdropping on EV-EVSE communication. By contrast, our work bypasses credential-based assumptions entirely by injecting crafted signals to spoof legitimate EV states, requiring no prior knowledge or access credentials.

Other physical-layer efforts, such as Kohler et al.'s "Brokenwire" attack [18] demonstrated large-scale charging disruptions through RF interference. While impactful, their method targets the communication channel as a whole. In contrast, our work precisely targets control signals and impedance states to forge EV charging logic from within the protocol itself.

Kohler et al. examined systemic vulnerabilities across the EV charging infrastructure, showcasing the potential for widespread disruptions that could impact millions of vehicles simultaneously [18]. Their call for comprehensive cybersecurity solutions, incorporating both technical and regulatory frameworks, aligns with the broader industry's need for a multi-layered defense strategy. However, our research zeroes in on physical layer security, presenting new attack vectors that exploit these foundational vulnerabilities in more focused and tangible ways.

Dudek et al. [11] released an open-source V2G injector to manipulate XML-based vehicle-to-grid exchanges. Our work complements this by addressing AC/DC handshake and signaling-level weaknesses, particularly those allowing access to the in-vehicle CAN bus via public charging ports.

Practical EVSE Exploitation. The Southwest Research Institute (SwRI) [14], [15] explored the J1772 protocol and proposed a zero-trust model for charging networks. However, their limited

focus and lack of empirical validation leave key protocol-layer attack vectors unexplored. Our work addresses this gap by systematically evaluating real-world AC and DC charging standards (e.g., GB/T 20234.2/.3, NACS), revealing authentication flaws that permit attacker-controlled state transitions.

Wasumwa et al. [32] highlighted the importance of policy and adaptive defense frameworks. While their perspective is valuable for large-scale ecosystem protection, our research focuses specifically on the technical root causes that enable real-time EVSE manipulation, contributing hands-on methodologies for exploitation and defense.

Signal Injection Attacks. Recent research has uncovered emerging attack vectors leveraging signal injection. Wang et al. [31] demonstrated how inaudible power-line noise can affect EV charging control logic. Similarly, laser-based voice injection attacks [25], [26] show that unconventional signals can be used to trigger unintended behaviors. Inspired by these, our work contributes the **first practical demonstration of signal injection into the charging interface**, exploiting physical signal-level authentication flaws to control EV states directly.

VIII. Discussion

A. Ethical Considerations

All experiments in this study were conducted on EVs owned by the authors. No third-party vehicles or public users were involved, ensuring that our research caused no unintended disruption or harm. We followed ethical research guidelines throughout the entire process, including full compliance with relevant data protection laws, safety protocols, and usage consent to contribute positively to the EV security ecosystem through transparent and responsible disclosure.

To ensure that our work aligns with the broader interests of the community, we engaged with safety experts. We also verified that all test signals introduced during experimentation, such as PWM pulses and CAN frames, were confined within hardware safety thresholds and did not pose any risk of physical damage, data leakage, or irreversible changes to vehicle systems.

B. Responsible Disclosure

To ensure the ethical handling of vulnerabilities identified in EV charging systems, we completed a coordinated responsible disclosure process before publication. The initial disclosure was

conducted through the organizers of the GEEKCON competition[1], where our work was selected and showcased as a live demonstration to the security community and participating vendors.

Following this initial presentation, we formally reported the vulnerabilities to the China National Vulnerability Database (NVDB), specifically through the China Automotive Vulnerability Database (CAVD). Our submissions have been assigned four official identifiers. In addition to national database disclosures, we have also submitted four CVE requests through a recognized CNA partner, and these applications are currently under review.

The vulnerabilities were disclosed to major stakeholders across the EV ecosystem, including but not limited to Seres, Denza, Zeekr, BYD, XPeng, Arcfox, and Dongfeng Motor. Several vendors acknowledged receipt of the disclosure and expressed intent to investigate or mitigate the reported issues. A detailed timeline of the disclosure process, including vendors and impacts, is included in Appendices.

C. Implications

Our research uncovers critical weaknesses in the authentication mechanisms of publicly deployed EV charging systems, revealing the ease with which adversaries can exploit physical-layer vulnerabilities to manipulate charging states and vehicle behavior. Using our PORTulator attack suite, we demonstrated the ability to remotely interfere with charging processes and simulate discharge signals through PWM injection.

These findings highlight a broader systemic issue: the authentication protocols embedded in many EV charging infrastructures remain overly simplistic and insufficiently protected against signal-level spoofing. Given the adoption of international standards across diverse vendors, the risks identified here are not isolated to a single manufacturer but span a wide range of EV models and charging pile deployments.

The most immediate risk is the potential for vehicles to be unlawfully immobilized or mischarged at public stations, causing severe disruption to users. More concerning, however, is the long-term exposure these weaknesses create, particularly in environments where vehicles are integrated into smart transportation grids or used for Vehicle-to-Grid (V2G) interactions.

To mitigate such risks, manufacturers must adopt more robust, multi-layered authentication approaches—including physical signal verification, real-time anomaly detection, and cryptographic

[1]GEEKCON, formerly known as GeekPwn, is a premier security event in China where researchers publicly demonstrate cutting-edge vulnerabilities and novel attack surfaces.

validation. Regulators should also update certification requirements and standards to mandate stronger safeguards at both the protocol and hardware levels.

Finally, our findings point to future research directions. These include extending our threat model to private home charging systems, analyzing backward compatibility concerns for proposed countermeasures, and applying similar techniques to evaluate authentication protocols in other critical embedded systems.

D. Limitations

As with any practical security research, our work has certain limitations defined by the scope of our experiments and the constraints of real-world systems.

First, the PORTulator attack suite was designed to target widely deployed public EV charging piles, and may not apply to newer systems that adopt proprietary or advanced authentication protocols. Notably, we did not test against CHAdeMO [21] or ChaoJi, limiting coverage across all global standards.

Second, although our experiments were conducted in realistic charging environments, they were still controlled to ensure safety. Some extreme behaviors, such as disabling hardware-level protections or simulating malicious firmware inside EVs, were beyond our scope due to ethical constraints. For instance, when experimenting with CP line PWM injection, internal Battery Management System (BMS) safeguards prevented us from inducing high-current damage, demonstrating the effectiveness of built-in safety designs, but also limiting attack depth.

Lastly, we focused on protocol-level and analog signal-layer attacks. Future work could explore cross-layer attacks that integrate physical-layer spoofing with protocol fuzzing, or conduct broader empirical studies involving international vendors and private charging facilities.

IX. Conclusion

Our research reveals significant vulnerabilities in the authentication mechanisms of EV charging systems, specifically highlighting weak points in widely adopted protocols. Through the use of PORTulator, we successfully demonstrate the feasibility of remote manipulation of charging operations, showcasing attack vectors such as signal injection and manipulation of the CP and CC ports. These vulnerabilities expose public charging infrastructures to potential threats, where attackers could exploit weak authentication processes to disrupt or immobilize vehicles, posing both safety and security risks.

Our findings suggest that current authentication protocols across various charging standards—including GB/T 20234, IEC, SAE J1772, NACS, and CCS—are inadequate in defending against sophisticated spoofing attacks, particularly in systems that rely on static resistance-based authentication mechanisms. The potential for injecting malicious signals, such as CAN bus messages, further underscores the critical need to reevaluate the security of charging infrastructure as EV adoption accelerates globally. In addition to exposing vulnerabilities, we also propose countermeasures to mitigate these risks. These include enhancing authentication protocols by integrating dynamic power, memory electric elements, and multi-layer security checks.

APPENDICES

The table III lists four assigned vulnerability IDs affecting major EV vendors, along with brief impact summaries and their corresponding disclosure timelines.

Vuln. ID	Affected Vendor(s)	Impact Summary	Disclosure Timeline
NVDB-CAVD-2025478822	Seres, Denza, Zeekr, BYD, XPeng, Arcfox and Dongfeng Motor	Weak resistance-based authentication allows an attacker to simulate invalid CC states, causing the charger to reject charging (DoS attack).	Reported: 2025-03-18 Acknowledged: 2025-05-22 Fixed: pending
NVDB-CAVD-2025018034	Seres, Denza, Zeekr, BYD, XPeng,Arcfox and Dongfeng Motor	Forged CC resistance locks the charging gun, preventing removal (deadlock attack).	Reported: 2025-03-18 Acknowledged: 2025-05-22 Fixed: pending
NVDB-CAVD-2025864575	Seres, Denza, Zeekr, BYD, Arcfox	Malicious CC values trigger discharge mode, draining the EV battery.	Reported: 2025-03-18 Acknowledged: 2025-05-22 Fixed: pending
NVDB-CAVD-2025820938	Denza, BYD, XPeng Arcfox	Bypassing CC2 check enables CAN injection, allowing remote control of charging.	Reported: 2025-03-18 Acknowledged: 2025-04-10 Fixed: pending

TABLE III: Vulnerability Disclosure Summary

REFERENCES

[1] "Definition and implementation of a global ev park charge," accessed: 2023-10-05. [Online]. Available: https://www.yumpu.com/en/document/read/39489467/definition-and-implementation-of-a-global-ev-park-charge

[2] "Iec 61851-1 standard document," accessed: 2023-10-05. [Online]. Available: http://www.msi-automation.com/Download/jishujiaoliu/IEC61851-1-2010-%E6%8E%A7%E5%88%B6%E5%AF%BC%E5%BC%95%E7%94%B5%E8%B7%AF%E7%9B%B8%E5%85%B3%E5%86%85%E5%AE%B9.pdf

[3] "Physical connection of dc charging process," accessed: 2023-10-05. [Online]. Available: https://wattsaving.com/blogs/knowledge-base/physical-connection-of-dc-charging-process

[4] "Specifications iec 309-2 charging concept," accessed: 2023-10-05. [Online]. Available: https://www.yumpu.com/en/document/view/39489470/specifications-iec-309-2-charging-concept-park-charge

[5] "Reverse Engineering an EV Charger," https://news.ycombinator.com/item?id=33564088, 2023, accessed: 2023-11-10.

[6] Anonymous, "Demo: Ransom Vehicle through Charging Pile," in *Proceedings of the 2023 Inaugural Symposium on Vehicle Security and Privacy*, ser. VehicleSec '23, 2023.

[7] R. Baker and I. Martinovic, "Losing the car keys: Wireless {PHY-Layer} insecurity in {EV} charging," in *28th USENIX Security Symposium (USENIX Security 19)*, 2019, pp. 407–424.

[8] J. Ciaccio and I. Onat, "An analysis of atm and point-of-sale skimming," *Policy*, 2025.

[9] M. Conti, D. Donadel, R. Poovendran, and F. Turrin, "Evexchange: A relay attack on electric vehicle charging system," in *European Symposium on Research in Computer Security*. Springer, 2022, pp. 488–508.

[10] W. contributors. Combined charging system. [Online]. Available: https://en.wikipedia.org/wiki/Combined_Charging_System

[11] S. Dudek, J.-C. Delaunay, and V. Fargues, "V2g injector: Whispering to cars and charging units through the power-line," in *Proceedings of the SSTIC (Symposium sur la sécurité des technologies de l'information et des communications), Rennes, France*, 2019, pp. 5–7.

[12] C. Hille and M. Allhoff, "Ev charging: Mapping out the cyber security threats and solutions for grids and charging infrastructure," *UtiliNet Europe*, 2018.

[13] K. Iehira, H. Inoue, and K. Ishida, "Spoofing attack using bus-off attacks against a specific ecu of the can bus," in *2018 15th IEEE annual consumer communications & networking conference (CCNC)*. IEEE, 2018, pp. 1–4.

[14] S. R. Institute, "Electric vehicle charging cybersecurity vulnerabilities," https://www.swri.org/press-release/electric-vehicle-charging-cybersecurity-vulnerabilities, 2024, accessed: 2024-07-25.

[15] ——, "Electric vehicle cybersecurity services," https://www.swri.org/industry/automotive-software-electronics/electric-vehicle-cybersecurity-services, 2024, accessed: 2024-07-25.

[16] J. Johnson, B. Anderson, B. Wright, J. Quiroz, T. Berg, R. Graves, J. Daley, K. Phan, M. Kunz, R. Pratt *et al.*, "Cybersecurity for electric vehicle charging infrastructure," Sandia National Lab.(SNL-NM), Albuquerque, NM (United States), Tech. Rep., 2022.

[17] A. Kailus, D. Kern, and C. Krauß, "Self-sovereign identity for electric vehicle charging," in *International Conference on Applied Cryptography and Network Security*. Springer, 2024, pp. 137–162.

[18] S. Köhler, R. Baker, M. Strohmeier, and I. Martinovic, "Brokenwire: Wireless disruption of ccs electric vehicle charging," *arXiv preprint arXiv:2202.02104*, 2022.

[19] J. Li, A. Li, D. Han, Y. Zhang, T. Li, and Y. Zhang, "Rcid: Fingerprinting passive rfid tags via wideband backscatter," in *IEEE INFOCOM 2022-IEEE Conference on Computer Communications*. IEEE, 2022, pp. 700–709.

[20] C. Liu, K. K. Chai, X. Zhang, and Y. Chen, "Enhanced proof-of-benefit: A secure blockchain-enabled ev charging system," in *2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall)*. IEEE, 2019, pp. 1–6.

[21] T. Nakanishi, H. Zaitsu, T. Kikuta, S. Tsuda, H. Nii, and S. Kodama, "Chademo-conformity high-power charger connector assembly for over 100 kw-class ev charge," *SEI Tech Rev*, vol. 88, pp. 49–54, 2019.

[22] T. Nasr, S. Torabi, E. Bou-Harb, C. Fachkha, and C. Assi, "Chargeprint: A framework for internet-scale discovery and security analysis of ev charging management systems." in *NDSS*, 2023.

[23] Raspberry Pi Foundation, "RP2040 Hardware Design," https://datasheets.raspberrypi.com/rp2040/hardware-design-with-rp2040.pdf, 2024, accessed: 2024-04-27.

[24] N. Scaife, C. Peeters, and P. Traynor, "Fear the reaper: Characterization and fast detection of card skimmers," in *27th USENIX Security Symposium (USENIX Security 18)*, 2018, pp. 1–14.

[25] H. Shi, Y. He, Q. Wang, J. Zhuge, Q. Li, and X. Liu, "Laser-based command injection attacks on voice-controlled microphone arrays," *IACR Transactions on Cryptographic Hardware and Embedded Systems (CHES)*, vol. 2024, no. 2, pp. 654–676, 2024.

[26] T. Sugawara, B. Cyr, S. Rampazzi, D. Genkin, and K. Fu, "Light commands:{Laser-Based} audio injection attacks on {Voice-Controllable} systems," in *29th USENIX Security Symposium (USENIX Security 20)*, 2020, pp. 2631–2648.

[27] Tesla Inc., *Tesla Model X Owner's Manual*, 2024, accessed: 2024-04-26. [Online]. Available: http://5491145.s21d-5.faiusrd.com/61/ABUIABA9GAAg2KDH_gUoztumpwY.pdf

[28] G. Vailoces, A. Keith, A. Almehmadi, and K. El-Khatib, "Securing the electric vehicle charging infrastructure: An in-depth analysis of vulnerabilities and countermeasures," in *Proceedings of the Int'l ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications*, 2023, pp. 31–38.

[29] R. Varriale, R. Crawford, and M. Jaynes, "Risks of electric vehicle supply equipment integration within building energy management system environments: A look at remote attack surface and implications," in *National Cyber Summit (NCS) Research Track 2021*. Springer, 2022, pp. 163–173.

[30] A. Venčkauskas, M. Taparauskas, Š. Grigaliūnas, and R. Brūzgienė, "Enhancing communication security an in-vehicle wireless sensor network," *Electronics*, vol. 13, no. 6, p. 1003, 2024.

[31] Y. Wang, H. Guo, and Q. Yan, "Ghosttalk: Interactive attack on smartphone voice system through power line," *arXiv preprint arXiv:2202.02585*, 2022.

[32] S. A. Wasumwa, "Safeguarding the future: A comprehensive analysis of security measures for smart grids," *World Journal of Advanced Research and Reviews*, vol. 19, no. 1, pp. 847–871, 2023.

[33] Wikipedia contributors, "Sae j1772 — Wikipedia, the free encyclopedia," 2024, [Online; accessed 18-April-2024]. [Online]. Available: https://en.wikipedia.org/wiki/SAE_J1772