HotWire: Real-World Impersonation and Discharge Attacks on Electric Vehicle Charging Systems

Kuan Yu Chen[1], Md Hasan Shahriar[2], Wen Wei Li[1], Shi Cho Cha[1], Wenjing Lou[2]

[1]*National Taiwan University of Science and Technology*
[2]*Virginia Tech*

{p477d343, nyps70414}@gmail.com, csc@cs.ntust.edu.tw
{hshahriar, wjlou}@vt.edu

Abstract

Electric vehicle (EV) charging infrastructures continue to depend heavily on the legacy DIN 70121 protocol, which lacks cryptographic authentication and exposes critical control messages in plaintext. Although prior studies have noted conceptual weaknesses, the feasibility and impact of *practical*, end-to-end attacks against real charging ecosystems remain insufficiently understood. We present HotWire, a systematic security analysis of DIN 70121 and the first demonstration of two practical, production-grade exploits: (i) unauthorized Autocharge activation via identifier impersonation, and (ii) unauthorized energy extraction through protocol-driven battery-state manipulation. In the first attack, an adversary replays a captured EV identifier (EVCCID) to initiate fraudulent Autocharge sessions on commercial networks using a low-cost hardware toolkit. Our experiments show that attackers can repeatedly obtain full charging sessions commonly valued at $35-45 without triggering existing fraud-detection mechanisms. In the second attack, we exploit insecure battery management system (BMS) state transitions by injecting protocol-compliant voltage claims, inducing controlled forced discharge, and enabling persistent energy loss. Furthermore, we validate these attacks across production vehicles and multiple public charging networks using a physical hardware-in-the-loop testbed, revealing widespread trust in protocol state over physical verification. We release open-source auditing tools and describe responsible disclosure outcomes, which have already prompted firmware updates and additional authentication safeguards by several vendors.

1 Introduction

According to projections, the global passenger vehicle market is poised for a significant transformation, with electric vehicle sales expected to constitute 75% to 95% of all new vehicle sales by 2030 [42]. This electrification wave has spurred an unprecedented expansion of charging infrastructure, now numbering in the millions of public stations worldwide. However, these charging stations have evolved into more than amenities. They represent critical national infrastructure, essential for transportation networks, commercial logistics, and emergency response systems. Comprehensive surveys identify authentication bypass, protocol manipulation, and physical access as the primary attack vectors in EV charging ecosystems [20]. The security of EV charging networks requires addressing vulnerabilities across the entire technology stack, from physical connectors to cloud management systems [17]. As dependency on this infrastructure deepens, its security becomes paramount for public safety, economic stability, and societal trust in electrified mobility.

The evolution of EV charging communication protocols has progressed from simple, security-agnostic designs to more sophisticated standards intended to support secure and automated charging [14]. Early charging deployments predominantly relied on DIN 70121, a DC charging protocol created before cybersecurity requirements were systematically integrated into EV infrastructure. DIN provides only *basic, non-cryptographic identification mechanisms*, such as the EV Charging Controller Identifier (EVCCID) and session identifiers, which are used to label and track communication flows. While these fields enable backend systems to associate a charging session with a vehicle, they do not provide cryptographic authentication, integrity protection, or confidentiality, leaving the protocol vulnerable to spoofing, tampering, and man-in-the-middle attacks [24] [8]. To address these limitations, the industry introduced ISO 15118, which specifies a modern security architecture based on TLS, certificate-based mutual authentication, and the Plug-and-Charge (PnC) mechanism for automated and trustworthy authorization. Despite these advancements, recent large-scale measurements reveal a substantial deployment gap: *DIN 70121 remains the dominant protocol across continents, with approximately 88% of public charging stations not using TLS or the security mechanisms defined in ISO 15118* [39]. This continued reliance on an unsecured legacy protocol exposes a sizable and insufficiently examined attack surface in today's EV charging ecosystem.

In this work, we focus primarily on vulnerabilities in DIN

70121, which remains the dominant charging protocol in deployed infrastructure. While our testing platform supports ISO 15118-2 for compatibility and comparative analysis, our attack vectors specifically exploit DIN 70121's lack of cryptographic authentication. We note that our EVCCID impersonation attack does not directly compromise ISO 15118's TLS-protected Plug-and-Charge mechanism. However, many ISO 15118-capable charging stations maintain backward compatibility with DIN 70121 to support legacy EVs, leaving them vulnerable to the proposed attacks when communicating via the unencrypted protocol.

While recent research has identified vulnerabilities in EV charging protocols [19] [5], existing work addresses only isolated attack vectors. EVExchange [12] demonstrated relay attacks on ISO 15118 Plug-and-Charge but required tampering with two charging stations simultaneously and was validated only in simulated environments using MiniV2G [6]. Large-scale infrastructure discovery studies reveal inconsistent security configurations across charging networks [35], validating the systemic nature of deployment vulnerabilities. The attack scenario necessitates the presence of both a victim vehicle and an attacker vehicle charging at adjacent stations, with malicious relay devices installed in both charging columns to intercept and forward communication. DrainDead [26] independently discovered battery discharge vulnerabilities in DIN 70121, testing 13 vehicles in laboratory settings, but did not explore the Autocharge impersonation vector or validate attacks against deployed public infrastructure. BROKENWIRE [22] focused exclusively on physical-layer denial-of-service attacks using wireless electromagnetic interference, without targeting energy theft or application-layer protocol exploitation.

In this work, we present HOTWIRE, a comprehensive security analysis of DIN 70121-based charging systems through practical attacks that expose critical vulnerabilities at both the application and physical layers. Our work differs fundamentally in three dimensions. First, we demonstrate the first practical EVCCID impersonation attack against production-level public charging infrastructure, successfully stealing 1.25 kWh from a commercial charging network in an East Asian country without requiring station tampering or the presence of the victim. This validates that Autocharge systems relying solely on EVCCID authentication are vulnerable to energy theft. While our demonstration session stole 1.25 kWh, a complete charging session (60-75 kWh) could result in financial impacts of $35-45 per session in the U.S. and $62-81 in Europe [10, 23], as the attack is repeatable without detection. Second, unlike prior work examining either infrastructure-side or vehicle-side vulnerabilities in isolation, we reveal how the same DIN 70121 protocol weaknesses enable both Autocharge bypass and forced discharge, demonstrating the systemic nature of protocol insecurity across the entire charging ecosystem. Third, we release low-cost Electric Vehicle Supply Equipment (EVSE) and EV simulators ($180 each) built on pyPLC [41] and OpenV2Gx [40], enabling reproducible security research and community-driven auditing, addressing the ecosystem's lack of accessible testing tools.

In this work, we make the following key contributions:

- **First practical Autocharge impersonation attack.** We demonstrate the first end-to-end EVCCID replay attack against production Autocharge infrastructure, successfully stealing 1.25 kWh of energy from a commercial charging network. Unlike prior work focusing on protocol-level relay attacks [12], our attack decouples reconnaissance from exploitation, enabling scalable energy theft. We validated the attack against 7 charging networks, revealing that current Autocharge deployments lack even basic fraud detection mechanisms such as geolocation anomaly detection or concurrent session monitoring.
- **Systematic dual-surface attack analysis.** We show that DIN 70121's reliance on unauthenticated identifiers such as the EVCCID exposes both sides of the ecosystem: charging infrastructure, where Autocharge is bypassed via EVCCID replay, and vehicles, where manipulated session parameters induce Battery Management System (BMS) state confusion and forced discharge. Because both vectors stem from the same protocol weakness, the failures are systemic rather than isolated bugs.
- **Comparative BMS security analysis.** We evaluated BMS implementations across four vehicle models from diverse manufacturers (Tesla, Luxgen, CMC, Hyundai), revealing that BMS security postures vary dramatically despite all being DIN 70121 compliant. Secure implementations (Tesla) require physical voltage measurements from hardware sensors before closing high-voltage contactors, effectively preventing forced discharge attacks. In contrast, vulnerable implementations (Luxgen, CMC, Hyundai) trust protocol-level voltage values without hardware verification, enabling attackers to manipulate the BMS state through crafted PreCharge messages. This reveals that 75% of our test vehicles prioritize protocol compliance over physical safety validation. We validate our findings through responsible disclosure with manufacturers, two of whom committed to firmware updates implementing mandatory hardware-based voltage verification.
- **Open-source testing framework.** To enable community-driven security auditing, we release a low-cost ($180) EVSE/EV emulator supporting both DIN 70121 and ISO 15118-2, with attack scenario templates for systematic vulnerability discovery. Our toolkit addresses the ecosystem's lack of accessible testing tools, which has hindered independent security research on EV charging protocols.

2 Background

This section provides the necessary technical foundation for understanding the vulnerabilities we exploit. We first describe

the communication architecture used in DC fast charging, then detail the DIN 70121 protocol and its security model, and finally explain the role of the BMS in controlling high-voltage battery access.

2.1 DC Fast Charging Communication Architecture

DC fast charging in the Combined Charging System (CCS) standard relies on a multi-layer communication stack between the EV and the EVSE. The physical layer uses Power Line Communication (PLC) over the charging cable itself, modulated via the HomePlug Green PHY (HPGP) protocol. Before any application-layer messages can be exchanged, both the vehicle and charger must join the same powerline network using the Signal Level Attenuation Characterization (SLAC) handshake protocol defined in ISO 15118-3 [1]. This physical and network layer architecture is shared by both DIN 70121 and ISO 15118; the protocols diverge only at the application layer. Once the physical link is established, the network layer uses IPv6 with stateless auto-configuration for address assignment. The vehicle sends a UDP discovery broadcast to locate the EVSE, which responds with a TCP endpoint. All subsequent application-layer communication occurs over this TCP connection; DIN 70121 uses dynamically assigned ports from the ephemeral range (49152-65535), while ISO 15118 uses the fixed port 15118. Messages are encoded using Efficient XML Interchange (EXI), a compact binary representation of XML.

2.2 DIN 70121 Protocol and Autocharge

DIN 70121 is a legacy German industrial standard that predates the international ISO 15118 specification. Despite its age, it remains widely deployed in European and North American charging infrastructure due to backward compatibility requirements [39]. The protocol defines a strict message sequence for establishing and maintaining a charging session, as illustrated in Figure 1. The session begins with `supportedAppProtocolReq` to negotiate the protocol version, followed by `SessionSetupReq`, in which the vehicle transmits its EVCCID, a 6-byte MAC address that uniquely identifies the vehicle's communication interface. Subsequent messages include `ChargeParameterDiscoveryReq` to exchange battery capacity and voltage limits, `CableCheckReq` to verify insulation integrity, and `PreChargeReq` to coordinate the pre-charging phase. The PreCharge phase is critical: the EVSE reports its output voltage via `EVSEPresentVoltage` in `PreChargeRes`, and the vehicle's BMS is expected to verify this voltage matches the battery voltage before closing high-voltage contactors. Once the contactors close, the charging loop consists of repeated `CurrentDemandReq` and `CurrentDemandRes` messages to regulate power flow.

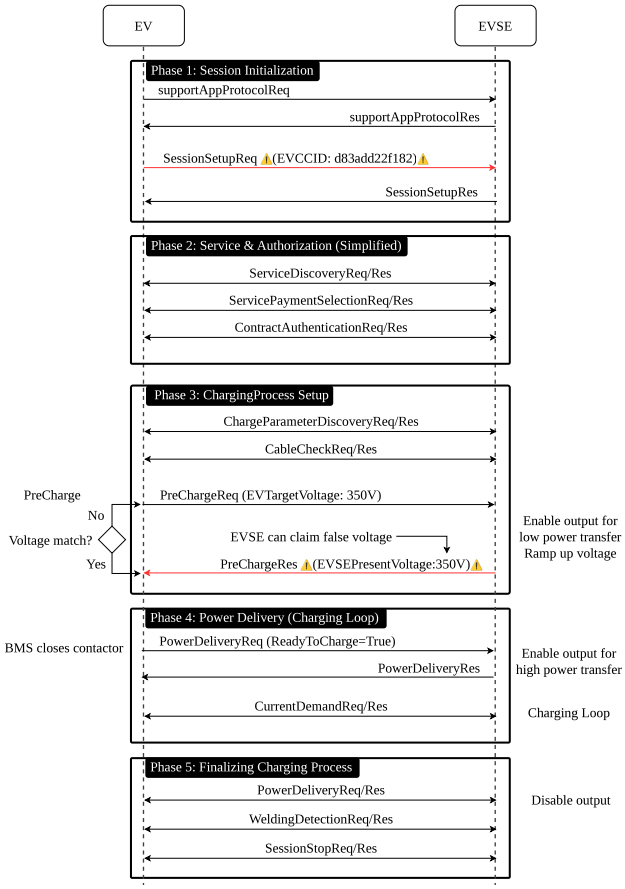


Figure 1: DIN 70121 message sequence for DC fast charging

A critical security weakness in DIN 70121 is the absence of any encryption or authentication. All messages, including the EVCCID, are transmitted in plaintext over the TCP connection. This enables the *Autocharge* [16] convenience feature, which streamlines charging by eliminating the need for manual authentication after initial registration. During the first charging session, the user authenticates using an RFID card or mobile application. The charging station records the EVCCID transmitted in `SessionSetupReq` and associates it with user account metadata in the backend database, including the account identifier, tokenized payment credentials, vehicle information, and billing preferences. This mapping (EVCCID $\rightarrow$ user account) enables the system to automatically recognize the vehicle on subsequent visits and initiate charging without requiring further authentication. The charging session is then billed directly to the registered account based solely on EVCCID recognition. However, this design creates an obvious impersonation attack vector where an attacker who captures a legitimate vehicle's EVCCID can replay it to steal charging services from any Autocharge-enabled station.

2.3 ISO 15118 and Protocol Security Evolution

ISO 15118-2 introduced incremental improvements over DIN 70121, including optional TLS encryption, but TLS remains non-mandatory and is rarely deployed in practice [39]. Without TLS, ISO 15118-2 shares the same authentication weaknesses as DIN 70121, as it transmits the EVCCID in plaintext and relies on MAC address-based identity. The newer ISO 15118-20 standard enforces mandatory TLS 1.3 and implements Plug and Charge (PnC) with PKI-based authentication, where vehicles present manufacturer-signed certificates. This cryptographic binding prevents the impersonation attacks demonstrated in this work. Recent implementations demonstrate that ISO 15118-20 with mandatory TLS 1.3 and PKI-based Plug and Charge effectively mitigates identifier replay attacks [21]. However, ISO 15118-20 adoption remains minimal, and most deployed infrastructure continues to support DIN 70121 as a fallback protocol for compatibility with older vehicles.

2.4 Battery Management System (BMS) Control Logic

The BMS serves as the safety controller for the high-voltage battery pack, monitoring cell voltages, temperatures, and the state of charge. Its most critical function is controlling the high-voltage contactors and electromechanical relays that physically connect or disconnect the battery from the DC charging pins. According to the DIN 70121 specification, the EVSE must first apply a "PreCharge" voltage to the DC pins that matches the vehicle's current battery voltage before the contactors close. This prevents dangerous inrush current spikes [11]. The BMS is expected to measure this external voltage and verify it matches the internal battery voltage before closing the contactors.

However, the DIN 70121 specification does not mandate how the BMS should perform this voltage verification. Implementations may choose to verify the external voltage through hardware sensors before closing contactors, or they may infer voltage matching from the successful completion of the `PreChargeReq`/`PreChargeRes` message exchange. This implementation ambiguity creates potential security implications that we examine in Section 4. For V2G-enabled vehicles, the security requirements extend to bidirectional authentication frameworks that verify both charging and discharging authorization [25], as unauthorized reverse power flow poses risks to both the vehicle battery and grid stability.

3 Threat Model

We define a threat model focused on adversaries targeting the EV charging ecosystem in public environments. Throughout this paper, we distinguish between two types of vehicles: the *victim vehicle*, whose EVCCID the attacker captures for later impersonation, and the *attacker's vehicle*, which the attacker uses to exploit stolen credentials or discharge attacks. Our model is grounded in the architectural constraints of DIN 70121 and ISO 15118-2, where authentication and encryption are optional and rarely deployed.

3.1 Environment and Assumptions

The victim vehicle is parked in a publicly accessible location, such as a street parking space, shopping center lot, or workplace charging facility. Although the victim vehicle may be locked and unattended, its charging port is presumed accessible, either because the vehicle is actively charging with an unlocked cable, or the attacker can open the charge port cover through wireless replay attacks (as demonstrated for Tesla vehicles [29]), by triggering an emergency stop to interrupt an ongoing session, or by physical force. The vehicle supports DIN 70121 or ISO 15118-2 via a CCS connector.

The vehicle does not require TLS for charging sessions, as TLS remains optional in both DIN 70121 and ISO 15118-2. The charging infrastructure may support Autocharge, which links vehicle identifiers to user accounts for billing without requiring RFID or app-based authentication. The vehicle's BMS implements safety logic to control high-voltage contactors, but we assume the BMS may trust protocol-level state transitions over physical sensor measurements.

3.2 Attacker Capabilities

The attacker can physically connect a rogue EVSE device to the vehicle's CCS charging port, or connect a simulated EV device to a public charging station. This access enables the attacker to establish a Power Line Communication (PLC) channel and participate in DIN 70121 protocol exchanges. For EVCCID capture, physical access need not be prolonged; the attacker can retrieve the EVCCID within seconds during the `SessionSetupReq` message exchange, then disconnect and use the captured identifier remotely at any Autocharge-enabled station.

For forced discharge attacks, the attacker connects a rogue EVSE with an attached resistive load to the victim vehicle's charging port. Once the DIN 70121 handshake is complete and the BMS closes the high-voltage contactors, the discharge process can proceed autonomously without further interaction from the attacker. The attacker may leave the device unattended, as the protocol state machine maintains the discharge session until the battery is depleted or the victim intervenes.

The attacker is familiar with the DIN 70121 and ISO 15118-2 message sequences, including session setup, PreCharge, and power delivery phases. The attacker can craft syntactically valid messages with arbitrary parameters, enabling deviation from standard charging station behavior to probe BMS implementations for state confusion vulnerabilities.

The attacker utilizes only commercially available components: a modified HomePlug PLC modem for physical-layer communication, a microcontroller for generating PWM pilot signals, and either a bidirectional power supply or a resistive load bank for power electronics. As we demonstrate in Section 5, such a device can be assembled for under $180 using off-the-shelf parts, with no requirement for automotive-grade test equipment or insider access to proprietary specifications.

3.3 Attacker Goals

An attacker can have two goals. First, the attacker aims to obtain A_1 *unauthorized Autocharge* that is billed to the victim's account. It is done by capturing vehicle EVCCIDs from target vehicles and replaying them at Autocharge-enabled charging stations. Second, A_2 *unauthorized energy extraction*, where the attacker seeks to discharge the high-voltage battery of a victim vehicle by exploiting BMS trust in protocol state over physical reality. Such unauthorized discharge serves multiple purposes: denial-of-service by stranding the victim with a depleted battery, or energy theft if the discharged power is used for productive purposes (e.g., powering equipment or reselling to the grid) [28] [2].

3.4 Out of Scope

Our analysis is limited to vulnerabilities in the EV–EVSE application-layer protocols accessible through the standardized CCS charging interface. We focus exclusively on implementations of DIN 70121 and ISO 15118-2 that operate without TLS. Security guarantees introduced in ISO 15118-20 are outside the scope of this study, as these mechanisms fundamentally prevent EVCCID replay and related impersonation attacks. Our goal is to identify protocol-level weaknesses that can be exploited solely through the CCS physical interface. Potential extensions of our attack to broader protocol-independent generalizations are discussed in Section 8.

4 Attack Methodology

In this section, we present HOTWIRE, which represents two complementary attacks against DIN 70121-based EV charging infrastructure. The first attack exploits the unprotected EVCCID identifier to enable impersonation and A_1 *unauthorized Autocharge* at Autocharge-enabled charging stations. The second attack, A_2 *unauthorized energy extraction*, leverages BMS state confusion to force unintended battery discharge by manipulating the PreCharge protocol phase. Both attacks require only physical access to CCS charging connectors of the victim vehicle and can be executed using commodity hardware assembled from off-the-shelf components. Together, these attacks demonstrate fundamental security weaknesses in the DIN 70121 protocol design, affecting millions of electric vehicles and charging stations deployed worldwide.

4.1 Attack 1: Unauthorized Autocharge

4.1.1 Attack Overview

As described in Section 2.2, Autocharge systems automatically recognize vehicles by their EVCCID and initiate charging without manual authentication. This convenience feature relies on a prior registration step that associates the EVCCID with user account credentials in the charging network's backend. An attacker who captures a victim's EVCCID can exploit this trust model to obtain A_1 unauthorized autocharging services.

4.1.2 Phase 1: EVCCID Harvesting

The attacker connects a rogue EVSE device to the target vehicle's CCS charging port and completes the standard DIN 70121 handshake (SLAC association [1], IPv6 autoconfiguration, TCP connection establishment using a dynamically assigned port). After protocol negotiation, the vehicle sends `SessionSetupReq` containing the EVCCID in the evccID field of the EXI-encoded message structure. The attacker extracts the 6-byte (12-hex-character) identifier (e.g., d83add22f182), logs it, and terminates the session. This process completes in under 10 seconds. Since the EVCCID is derived from the communication controller's MAC address and remains static throughout the vehicle's lifetime, a single successful capture yields a persistent credential that can be exploited indefinitely against any Autocharge-enabled charging station.

EVCCID harvesting does not necessarily require a physical connection to the victim's charging port. Because the unshielded CCS cable radiates the HomePlug Green PHY signal as common-mode emission, prior work has shown that the plaintext `SessionSetupReq`, and with it the EVCCID, can be recovered passively by radio-frequency sniffing of the powerline link from a nearby location, with no galvanic contact [7]. The two approaches trade off differently. The physical method used in this work is highly reliable and extracts an EVCCID in under 10 seconds, but it requires connector access to one vehicle at a time. Passive RF sniffing is receive-only and therefore stealthier, and it could enable opportunistic mass-harvesting of vehicles at a station, at the cost of a longer and less reliable capture that degrades in busy multi-vehicle settings [7]. In this work, we use the physical method for the controlled, reproducible captures.

4.1.3 Phase 2: Impersonating Victim Vehicle

The attacker reconfigures their PLC modem's MAC address to match the stolen EVCCID using vendor-provided configuration tools, then connects to an Autocharge-enabled charging station. When the station's backend receives the `SessionSetupReq` containing the spoofed EVCCID, it matches the identifier to the victim's registered account and

authorizes the session, associating all energy consumption with the victim's billing profile. The attacker then proceeds through the complete charging sequence (ChargeParameterDiscovery, CableCheck, PreCharge, CurrentDemand) to draw energy. From the charging station's perspective, the session is indistinguishable from a legitimate charging session initiated by the victim vehicle.

4.2 Attack 2: Unauthorized Energy Extraction

4.2.1 Attack Principle

The unauthorized energy extraction attack exploits BMS implementations that trust protocol state over physical sensor verification. The DIN 70121 protocol coordinates PreCharge through `PreChargeReq/PreChargeRes` exchanges, where the EVSE reports its output voltage via EVSEPresentVoltage. Vulnerable BMS implementations close contactors based solely on receiving matching voltage values in the protocol message, without independently measuring the actual voltage on DC pins.

However, this protocol design embeds a critical vulnerability: it assumes the BMS will independently verify the presence of external voltage through hardware voltage sensors before closing the contactors. Our research reveals that *some BMS implementations instead trust the protocol state machine itself as the primary safety check*. Threat modeling frameworks identify state confusion as a critical vulnerability in BMS control logic [27]. These vulnerable implementations reason that if the `PreChargeReq/PreChargeRes` exchange has completed successfully and the EVSEPresentVoltage value reported in the protocol matches the expected battery voltage, then the external voltage must actually be present. This *trust-in-protocol* approach eliminates the need for additional sensor validation logic, simplifying BMS firmware but creating an exploitable semantic gap between protocol state and physical reality.

4.2.2 Attack Execution

Under A_2, the attacker constructs a malicious EVSE that implements the DIN 70121 protocol state machine correctly, but connects a resistive load bank instead of a bidirectional power supply to the DC pins. The attack exploits the PreCharge phase to trick the BMS into closing contactors when no external voltage is present.

The attack follows the standard DIN 70121 handshake (SLAC, SessionSetup, ChargeParameterDiscovery, CableCheck) until reaching the PreCharge phase. When the vehicle sends PreChargeReq with its current battery voltage (e.g., 350V), the attacker responds with `PreChargeRes` claiming EVSEPresentVoltage matches the battery voltage ($V_{\text{batt}} \pm 5$V), despite the DC pins remaining at 0V. Vulnerable BMS implementations that trust this protocol assertion over physical sensor measurements close the high-voltage contactors, exposing the battery to the external load. The attacker then maintains the session through PowerDelivery and CurrentDemand message exchanges, manipulating reported voltage and current values to avoid triggering overcurrent or undervoltage protections. The adversary persists with the operation until a target level of battery depletion is reached or the battery is exhausted. We present detailed empirical results in the following section.

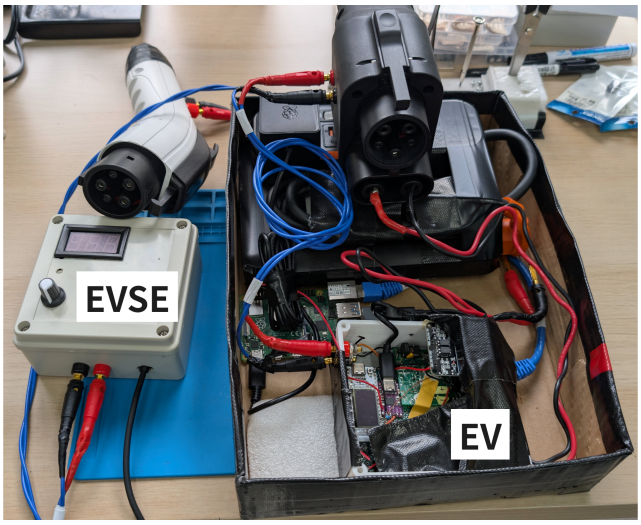


Figure 2: Physical implementation of the testing platform. Left: EVSE emulator with control interface and J1772 connector (for CP, PP, PE signals). Right: EV emulator showing Raspberry Pi 4, HomePlug adapter, Arduino control board, resistive load bank, and CCS1 connector. Both EVSE and EV emulators use commodity hardware, with a total cost of approximately $360 ($180 each).

5 Experimental Setup

To validate HotWire attacks described in Section 4, we developed a configurable physical hardware-in-the-loop EV/EVSE emulator capable of impersonating both EVSE and EV endpoints within the DIN 70121 protocol. This section describes the platform's architecture, implementation details, real-world EV models and charging stations, as well as the experimental methodology used to evaluate attack feasibility.

5.1 Hardware-in-the-Loop EV/EVSE Emulator

5.1.1 Software Architecture

The platform is implemented in Python 3.9 and built upon two open-source projects: pyPLC [41] for low-level SLAC association and HomePlug Green PHY management, and OpenV2Gx [40] for EXI message encoding/decoding. We extended these libraries with a

Table 1: Characteristics of Test Electric Vehicles

Vehicle	Battery (kWh)	Max DC Power	DC Interface
Tesla Model Y LR	75	250 kW	CCS2
Luxgen n7	60	135 kW	CCS1
CMC (unpublished)	76.5	80 kW	CCS1
Hyundai IONIQ 6	77.4	350 kW	CCS1

custom DIN 70121 state machine that provides programmatic control over all protocol phases (`SessionSetup`, `ChargeParameterDiscovery`, `CableCheck`, `PreCharge`, `PowerDelivery`, `CurrentDemand`). The implementation allows deviation from standard behavior by accepting arbitrary message parameters and response timing, enabling systematic exploration of BMS implementation variants and protocol edge cases. A graphical interface provides real-time visualization of protocol state transitions and message payloads for debugging and attack orchestration.

5.1.2 Hardware Implementation

We constructed two low-cost testing devices using commodity components to demonstrate attack feasibility with minimal resources: a malicious EVSE simulator for EVCCID harvesting and discharge attacks, and a rogue EV simulator for impersonation attacks at public charging stations. Both devices share the same core hardware platform (Raspberry Pi 4, HomePlug adapter, control board) but differ in resistive load capacity based on attack requirements.

Hardware Modification. The PLC front end uses a modified TP-Link TL-PA4010P adapter, reconfigured into a CCS endpoint via pyPLC [41]. This required three modifications: (1) powering the board via a regulated low-voltage DC supply instead of mains, (2) replacing the mains-coupling network with a capacitor/resistor tap to pass the Green PHY band while blocking the 1 kHz CP PWM, and (3) reprogramming the NVRAM Parameter Information Block (PIB) using the `open-plc-utils` [32] toolchain to forward SLAC frames and adopt the required EV or EVSE role.

EVSE Emulator. Our EVSE testing device (Figure 2, left) uses a modified TP-Link HomePlug adapter ($10) [30] connected to a Raspberry Pi 4 ($70) via Ethernet, interfaced to a CCS Type 1 connector through PLC coupling transformers ($50). The HomePlug adapter's MAC address is software-reconfigurable, enabling EVCCID capture during reconnaissance. For discharge attacks, we constructed a 1.25 kW resistive load bank (five 220V/250W light bulbs in parallel) ($10) with safety interlocks and emergency disconnect ($40). The total cost was approximately $180.

EV Emulator. Our EV testing device (Figure 2, right) uses the same hardware configuration as the EVSE simulator modified TP-Link HomePlug adapter [30], Raspberry Pi 4, Arduino control board and optocoupler-isolated relays for emergency disconnect. It includes a larger 2.5 kW resistive load bank (ten 220V/250W light bulbs in parallel) to actually draw energy during impersonation attacks at public charging stations. The device connects via a standard CCS cable and simulates a legitimate EV by replaying captured EVCCIDs during `SessionSetupReq`, enabling verification of both session authorization and actual energy theft. The total cost was approximately $180.

Table 2: Characteristics of Test Charging Stations

Provider	Max Power (kW)	Autocharge Support
EVALUE[†]	180	Yes
EVOASIS[†]	180	Yes
iCHARGING[†]	180	Yes
STAR Charger[†]	180	Yes
TAIL	200	Yes
U-POWER	360	Yes
YES! Charging[†]	180	Yes

[†]Operators deploy higher-power units (EVALUE: 640 kW; EVOASIS/STAR Charger/YES! Charging: 360 kW; iCHARGING: 350 kW). Tested units shown.

5.2 Real-world EV and Charging Stations

5.2.1 Representative EV Models

We evaluated our attacks on four production EVs spanning diverse manufacturers and battery architectures: the Tesla Model Y, Luxgen n7, an unpublished CMC model, and Hyundai IONIQ 6 (Table 1). They cover battery capacities from 60 kWh (Luxgen n7) to 77.4 kWh (IONIQ 6), support DIN 70121 or ISO 15118-2, span model years 2020-2024, and come from American (Tesla), Taiwanese (Luxgen, CMC), and Korean (Hyundai) manufacturers.

Their BMS sourcing is equally varied: Tesla uses a fully in-house design, Hyundai integrates a BMS from its Tier-1 supplier Hyundai Mobis (a proprietary Battery System Assembly), and Luxgen and CMC both source from Delta Electronics. We deliberately prioritize this implementation diversity over sample size, since our goal is to identify architectural security patterns (*trust-in-protocol* versus *trust-in-physics*) rather than to estimate statistical prevalence.

5.2.2 Representative Charging Stations.

For impersonation attacks, we tested against 7 public DC fast charging stations from major charging infrastructure providers deployed in an East Asian country: EVALUE, EVOASIS, iCHARGING, STAR Charger, TAIL, U-POWER, and YES! Charging. As mentioned in Table 2, these stations represent diverse charging controller implementations, with power outputs ranging from 180 kW to 360 kW CCS infrastructure, and span deployments by energy companies, automotive groups, and specialized charging service providers. All vehicle tests were conducted with explicit written consent from vehicle owners in controlled parking environments. Charging station

tests were conducted during off-peak hours, with prior coordination with network operators to minimize service disruptions. All experiments were approved by our institutional review board and conducted in accordance with local regulations regarding automotive testing and electrical safety.

5.3 Experimental Methodology

5.3.1 EVCCID Capture Testing

We connected our EVSE emulator to each test vehicle and initiated minimal DIN 70121 handshakes to extract EVCCIDs from SessionSetupReq messages. For each vehicle, we performed 5 capture attempts and measured capture time, protocol trace completeness, and visibility to vehicle diagnostic systems. All protocol exchanges were logged using Wireshark with the dsV2Gshark dissector [13] for post-hoc analysis.

5.3.2 Impersonation Validation

Using captured EVCCIDs, we tested replay attacks against the 7 public charging stations by configuring the platform in EV mode with spoofed MAC addresses. For each station, we performed 3 test sessions to verify: (1) successful session authorization without additional authentication, (2) energy delivery to a connected load, and (3) correct billing association with the victim EVCCID. We monitored charging network mobile applications to confirm fraudulent sessions appeared under victim accounts.

5.3.3 Discharge Attack Evaluation

We tested the forced discharge attack on each representative EV model by sending `PreChargeRes` messages with false voltage values while connecting the 1.25 kW resistive load bank to the DC pins. For each vehicle, we performed 3 test runs per voltage offset configuration ($V_{\text{batt}} \pm$ 0V, 5V, 10V) and recorded: (1) whether contactors closed despite zero external voltage, (2) discharge duration before session termination, (3) the estimated energy delivered to the resistive load (computed from its rated power and the discharge duration), and (4) BMS detection mechanisms. The 180-second cap applied to the per-offset trigger runs ($V_{\text{batt}} \pm$ 0/5/10 V), each of which ran until the vehicle either closed its contactors or terminated the session. For the Luxgen n7, we held a single session open to characterize sustained discharge before manually terminating it; the Hyundai IONIQ 6 and CMC discharges were confirmed over shorter continuous runs (Table 3). All protocol exchanges were automatically logged to timestamped files for post-hoc analysis. Safety precautions included isolation transformers, emergency disconnect switches, and fire suppression equipment to prevent equipment damage or safety hazards.

6 Real-World Attack Evaluation

This section provides the experimental results on implementing HOTWIRE attacks using the platform described in Section 5.

6.1 Unauthorized Autocharge Attack

We successfully executed the A_1 (unauthorized Autocharge attack) against a public DC fast charging station operated by a major East Asian charging network. We captured the EVCCID during the reconnaissance phase by connecting our EVSE simulator to a test vehicle in a controlled environment. The EVCCID was extracted from the SessionSetupReq message during the initial handshake, appearing unencrypted in the DIN 70121 message sequence. We then reconfigured our PLC modem's MAC address to match this identifier using standard network interface configuration tools and connected our simulator to the target charging station. Figure 3a shows the attack setup at the target charging station. The station's display confirmed session authorization within 3.2 seconds of cable connection, as the backend system authenticated the spoofed EVCCID, associated the session with the victim's pre-registered account, and authorized power delivery without requiring any additional user interaction.

Our platform proceeded through the complete DIN 70121 charging sequence, successfully drawing 1.25 kWh of energy over a 30-minute period (2.5 kW average power) before we voluntarily terminated the session. The charging station's communication logs, captured via our simulator's packet inspection interface, show no anomalies or security alerts—the infrastructure treated our emulated device as indistinguishable from the legitimate vehicle. Post-experiment analysis of the victim account's transaction history confirmed that the stolen energy was billed to the registered owner, with no fraud detection mechanisms triggering. This demonstration validates that Autocharge systems relying solely on EVCCID authentication are fundamentally vulnerable to replay attacks, enabling untraceable energy theft across any charging infrastructure that trusts this unencrypted identifier.

6.2 Unauthorized Energy Extraction Attack

Table 3 presents the outcomes of the A_2 unauthorized energy extraction attack across all four test vehicles. The Tesla Model Y demonstrated robust BMS protection, refusing to close its high-voltage contactors during the PreCharge phase when our malicious EVSE sent voltage-matching messages without applying actual DC voltage to the charging pins. The vehicle's error logs indicated "External voltage verification failed", suggesting Tesla implements hardware-based voltage sensing as a prerequisite for contactor closure. In contrast, all the Luxgen, CMC, and Hyundai models exhibited the hypothesized vulnerability: when presented with syntactically valid

Table 3: Forced Discharge Attack Results Across Test Vehicles

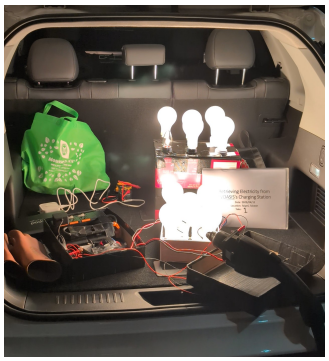
Vehicle	Vulnerable to Attack	Discharge Duration	Energy Drained (est.)	Detection Mechanism	Driver Alert
Tesla Model Y	No	N/A	N/A	HW voltage sensor	N/A
Luxgen n7	Yes	60 min	1.25 kWh	None detected	No
CMC (unpublished)	Yes	∼2 min	∼0.05 kWh	None detected	No
Hyundai IONIQ 6	Yes	∼26 min	∼0.5 kWh	None detected	No

Energy is estimated from the load bank's rated power (1.25 kW) and discharge duration, not externally metered. Durations are the longest continuous forced-discharge run observed per vehicle; all three vulnerable vehicles discharged into the load upon contactor closure.

`PreChargeRes` messages claiming correct voltage presence, their BMS closed the contactors despite the absence of external voltage, immediately initiating discharge into our resistive load.

Figure 3b shows the real-world forced discharge of the Luxgen n7, and Figure 4 reconstructs the corresponding DIN 70121 message trace. Upon contactor closure, the battery began discharging into our load bank, rated at 1.25 kW. The discharge continued for 60 minutes until we manually terminated the session, draining an estimated 1.25 kWh (computed from the load bank's rated power and the discharge duration) and reducing the battery's state of charge by an estimated 2.1%. While a single attack session causes minimal immediate impact, an overnight attack (8 hours) could drain 10 kWh, representing 25% of a 40 kWh urban EV's capacity or 50% of a vehicle's remaining charge if parked at 50% state-of-charge. For vehicles with smaller battery capacities or partial charge states, such attacks could render the vehicle inoperable by morning. Notably, none of the vulnerable vehicles displayed visible warnings to the driver during discharge, and the BMS did not autonomously open the contactors despite the anomalous power flow direction.

The implications of this vulnerability extend beyond individual vehicle attacks. High-capacity electric transportation assets, such as electric buses, delivery trucks, and maritime vessels, operating on fixed schedules with known charging locations, represent high-value targets. An adversary could covertly deploy a malicious EVSE at a fleet charging depot, inducing discharge overnight to render an entire fleet non-operational. Similarly, an attacker targeting electric ferries or emergency response vehicles could create safety-critical service disruptions by depleting batteries immediately before scheduled operations. The sustained discharge duration and lack of driver alerting make this attack particularly dangerous, as victims may not discover the energy theft until they attempt to use the vehicle and find insufficient range.



(a) Unauthorized autocharge attack at a charging station.

(b) Unauthorized forced discharge via rogue EVSE setup.

Figure 3: Real-world demonstrations of unauthorized EV charging attacks. (Left) Autocharge impersonation attack where a malicious actor triggers unauthorized charging at a public station. (Right) Forced discharge attack targeting a Luxgen n7, where a rogue EVSE redirects battery energy into an external resistive load, effectively extracting energy from the vehicle at a public charging infrastructure.

7 Countermeasures

The vulnerabilities demonstrated in this work require defense-in-depth countermeasures spanning multiple stakeholders in the EV charging ecosystem. We organize our recommendations into three categories: immediate mitigations deployable by Charging Point Operators without protocol changes, vehicle-side hardening by automotive manufacturers, and long-term industry-wide architectural transitions.

7.1 For Charging Point Operators

Charging Point Operators (CPOs) deploying Autocharge functionality must implement defense-in-depth strategies that extend beyond reliance on EVCCID authentication. We recommend a multi-factor authentication approach that requires users to verify their identity through a secondary channel, such as a mobile app push notification or an RFID card tap, before the first charging session with a previously unseen EVCCID. Protocol-level security enhancements in newer standards (e.g., OCPP 2.0.1) introduce stronger authentication and logging mechanisms [3], though adoption remains limited. Once a vehicle is initially authenticated, the system can cache the binding between EVCCID and user account for a limited period, allowing subsequent sessions to proceed with Autocharge convenience while mitigating impersonation risks

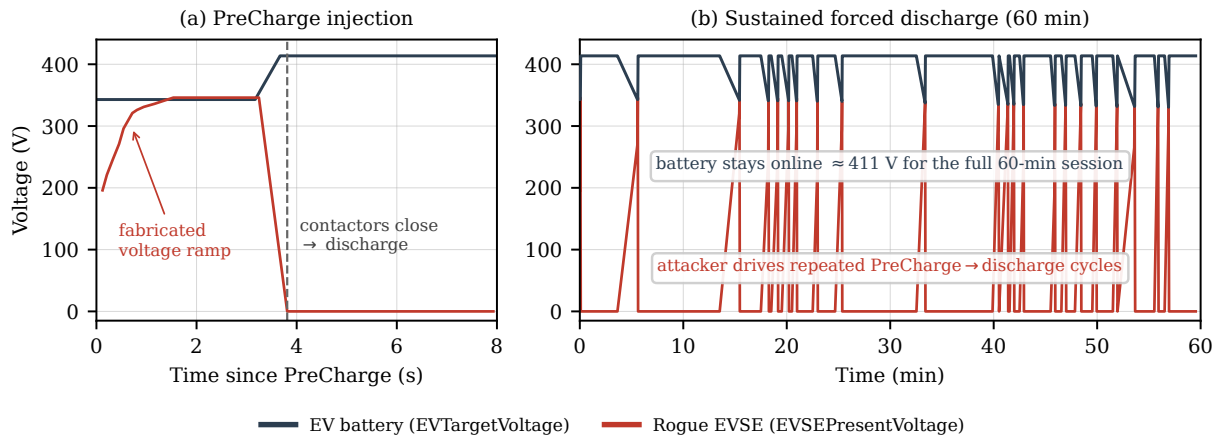


Figure 4: Forced-discharge message trace of the Luxgen n7, reconstructed from the recorded DIN 70121 session; all values are protocol-reported, not externally metered. (a) During PreCharge, the rogue EVSE ramps a fabricated `EVSEPresentVoltage` up to the battery voltage, inducing the BMS to close its high-voltage contactors, after which the reported voltage collapses to 0 V. (b) The attacker then sustains the forced discharge for 60 minutes through repeated PreCharge–CurrentDemand cycles, while the vehicle's reported battery voltage (`EVTargetVoltage`) remains near 411 V throughout.

during the critical first use. Additionally, CPOs should deploy backend anomaly detection systems that monitor for suspicious charging patterns [34], such as the same EVCCID appearing at geographically distant locations within implausibly short time intervals, multiple concurrent sessions from the same EVCCID at different stations, or deviations from a user's historical charging behavior. Statistical models such as Hidden Markov Models have demonstrated effectiveness in correlating anomalous behavior patterns across multiple charging sessions [15]. Machine learning models (e.g., temporal convolutional networks [9]) and deep learning-based detection mechanisms [18] achieve high accuracy in real-time attack detection, providing a complementary defense layer to static anomaly rules. These behavioral heuristics can flag potentially fraudulent sessions for manual review or automatic suspension, providing a safety net against sophisticated attackers who may have obtained EVCCIDs through reconnaissance.

7.2 For Automotive Manufacturers

Original Equipment Manufacturers (OEMs) must harden BMS implementations against protocol-level state confusion attacks by adopting a physics-first design principle. BMS control logic should never authorize high-voltage contactor closure based solely on syntactically valid protocol messages from an unauthenticated communication channel. Instead, the BMS must independently verify that physical conditions match the claimed protocol state before taking safety-critical actions. For the PreCharge phase, this means requiring hardware-based voltage sensors to confirm that the external voltage on the DC charging pins is present and matches the internal battery voltage within a specified tolerance before closing contactors, regardless of the EVSE's claimed voltage in the PreChargeRes message. Critically, our post-disclosure discussions with manufacturers revealed that vulnerable BMS implementations already possess the necessary voltage-sensing hardware for cell balancing and state-of-charge estimation, but do not utilize these sensors during PreCharge validation. The fix requires firmware updates rather than hardware modifications, implementing mandatory sensor-based verification logic that treats physical measurements as a non-bypassable prerequisite for contactor closure. Risk-based evaluation frameworks [37] can guide OEMs in prioritizing safety-critical firmware updates. Two of the four manufacturers we disclosed have committed to deploying such firmware updates via over-the-air mechanisms within 6 to 12 months. Our testing revealed that the Tesla Model Y implements this mitigation effectively, refusing to close contactors when presented with false voltage claims, while the Luxgen n7, a CMC unpublished model, and the Hyundai IONIQ 6 merely rely on the protocol state provided from the EVCC rather than physical reality. Furthermore, OEMs should implement continuous monitoring of current flow direction and immediately open contactors if reverse current is detected outside of authorized bidirectional charging contexts. Advanced V2G deployments require digital twin-based security frameworks [4] that create real-time virtual replicas of the charging session to detect anomalous energy flow patterns, providing an additional defense layer against forced discharge attacks by correlating protocol state with physical power measurements.

7.3 For the Industry as a Whole

The fundamental vulnerabilities demonstrated in this work stem from DIN 70121's lack of cryptographic security mechanisms, a design limitation that cannot be retrofitted without breaking backward compatibility. The industry must therefore accelerate the deprecation of DIN 70121 and mandate universal adoption of ISO 15118-20 with Plug and Charge enabled. The PKI-based authentication and mandatory TLS 1.3 encryption provided by ISO 15118-20 [21] eliminate both the EVCCID impersonation and the discharge attacks by cryptographically binding vehicle identity to manufacturer-issued certificates and protecting all protocol messages from tampering and replay. Regulatory bodies and industry consortia such as CharIN should establish sunset deadlines for DIN 70121 support in new vehicle models and charging infrastructure, similar to the deprecation timelines used for obsolete TLS versions in web security.

For legacy vehicles that cannot be upgraded to ISO 15118-20 via over-the-air software updates due to hardware limitations, CPOs should disable Autocharge functionality and require explicit user authentication for all sessions through RFID cards, mobile applications, or credit card payment terminals. While this imposes a usability penalty, the financial impact of widespread EVCCID impersonation attacks justifies accepting the trade-off in exchange for eliminating the replay attack vector. Finally, charging infrastructure manufacturers should adopt defense-in-depth approaches even when supporting legacy protocols, implementing comprehensive session logging, real-time fraud detection algorithms, and establishing an information-sharing framework similar to the financial sector's fraud detection networks to enable network-wide blacklisting of stolen identifiers. The forced-discharge attack also points to an architectural fix that belongs in the standards rather than in individual implementations: a protocol state transition that authorizes a high-voltage physical action should be bound to a corroborating hardware-sensor measurement. We recommend that standards bodies and consortia such as CharIN require the measured external DC voltage on the charging pins to agree with the claimed `EVSEPresentVoltage` within a defined tolerance before contactor closure is permitted. Because vulnerable battery management systems already contain the necessary isolated voltage sensing but do not consult it during PreCharge validation, this change is largely a matter of firmware and specification, and it would close the trust-in-protocol gap consistently across DIN 70121, ISO 15118-2, and ISO 15118-20.

7.4 Cost-Benefit and Feasibility

The two principal mitigations differ in where their cost falls. For the deployed fleet, hardware-grounded voltage verification (Section 7.2) is largely a firmware change rather than a hardware cost. The required voltage sensing already exists but is not consulted during PreCharge, which is why two of the four disclosed manufacturers committed to over-the-air updates within 6 to 12 months. The dominant expense is therefore the functional-safety process rather than silicon, since gating high-voltage contactor closure is plausibly a high-ASIL function under ISO 26262 and raises development and assessment effort severalfold. Adding new isolated sense hardware is a different matter: it touches the sealed high-voltage battery junction box and forces re-homologation, so it is uneconomic to retrofit and realistic only for next-platform designs, leaving the firmware path as the practical option for the legacy fleet. Stronger Autocharge enrollment (Section 7.1) has the opposite profile. Its bill-of-materials and certification cost is negligible because it is a software and account-management change, but it weakens the zero-friction convenience that motivates Autocharge. A first-use second factor limits this friction to the first session with a previously unseen EVCCID and stays within existing OCPP/OCPI roaming flows [3], whereas full certificate-based identity under ISO 15118-20 [21] removes the impersonation vector cryptographically but carries the highest implementation and roaming cost across the eMSP–CPO chain. A pragmatic deployment therefore combines the firmware voltage check with a first-use second factor as immediate, low-cost controls on the legacy fleet, while treating ISO 15118-20 migration as the longer-term goal.

8 Discussion

The Compliance Trap. The vulnerabilities demonstrated in this work expose a fundamental flaw in the validation of critical infrastructures: adherence to protocol specifications is mistaken for security assurance. DIN 70121 does not contain cryptographic authentication, message integrity protections, or encryption for sensitive identifiers. Both the impersonation and discharge attacks succeed by exploiting the gap between syntactic protocol correctness and semantic security guarantees. An attacker following the message sequence exactly as specified achieves authentication bypass and BMS manipulation without violating protocol rules. This compliance trap persists because industry validation emphasizes interoperability testing rather than adversarial testing, resulting in products certified as DIN 70121 compliant while vulnerable to trivial replay and state confusion attacks.

BMS Implementation Variance. The variance in BMS vulnerability across tested vehicles reveals concerning inconsistencies in safety-critical system design. Tesla Model Y demonstrated robust physical verification, refusing to close contactors when presented with false PreCharge claims, while Luxgen n7, a CMC unpublished model, and Hyundai IONIQ 6 trusted protocol state over physical sensor measurements. The DIN 70121 specification itself is ambiguous regarding mandatory physical voltage verification before contactor closure, stating PreCharge should match voltages without requiring hardware sensor confirmation, allowing compliant implemen-

tations to vary widely in security posture. Comprehensive vulnerability analysis confirms that BMS security postures vary significantly across manufacturers due to differing interpretations of safety-critical validation requirements [27].

Automotive manufacturers developing BMS firmware should adopt Tesla's defense-in-depth model as a reference architecture, implementing mandatory sensor-based validation as a non-bypassable prerequisite for any safety-critical operation, regardless of protocol state.

Attack Constraints and Detection. Despite attack severity, practical constraints limit adversary capabilities and create detection opportunities. The impersonation attack requires physical presence at both reconnaissance and exploitation phases, constraining geographic reach and creating observable movement patterns between victim vehicles and compromised charging sessions. Charging network operators can implement geolocation correlation algorithms that flag sessions where EVCCIDs appear at distant locations within implausible timeframes or exhibit behavioral deviations from historical patterns. While anomaly detection frameworks [15] can identify suspicious patterns, our validation across seven commercial charging networks revealed that none deployed such mechanisms in production. Mobile applications displayed only historical transaction logs rather than active session monitoring, preventing users from detecting concurrent fraudulent sessions in real-time. Infrastructure-wide security assessments confirm that fraud detection mechanisms remain largely absent in deployed charging networks [35]. This infrastructure gap enabled our impersonation attack to execute for 30 minutes without triggering any security alerts, despite the obvious geolocation anomaly of the same EVCCID appearing at our test location while the legitimate vehicle remained elsewhere. For the discharge attack, sustained cable connection over 60 minutes increases physical detection risk by vehicle owners or bystanders, limiting applicability to unattended vehicles in low-surveillance environments. The attack produces visible symptoms where the battery state-of-charge decreases without vehicle operation, providing forensic evidence detectable through onboard diagnostics or telematics systems that enable post-incident attribution if logs are preserved.

Protocol-Agnostic Vulnerability. The forced discharge attack demonstrates a protocol-independent vulnerability rooted in BMS implementation decisions rather than protocol-specific weaknesses. While the EVCCID impersonation attack is specific to DIN 70121 and ISO 15118-2 deployments without TLS, the BMS state confusion vulnerability affects any protocol where the battery management logic trusts protocol state transitions over physical sensor verification. Our experiments showed that three of four tested vehicles closed high-voltage contactors based solely on receiving syntactically valid PreChargeRes messages claiming correct voltage presence, without independently measuring external voltage. This trust-in-protocol design flaw could manifest in ISO 15118-2 implementations with TLS enabled, where message authenticity and integrity are cryptographically protected, but physical reality is still not verified. Even ISO 15118-20 with PKI-based authentication cannot prevent this attack if the BMS trusts authenticated protocol messages over sensor data. The root cause is architectural: safety-critical physical operations should never depend solely on protocol state, regardless of how secure the protocol's cryptographic protections are. This vulnerability extends beyond unidirectional charging, as V2G-enabled systems face additional risks where bidirectional power flow can be exploited to inject reactive power or destabilize grid frequency [33], demonstrating that physical-layer validation is essential even in cryptographically secured environments.

Protocol Migration Barriers. While migration to ISO 15118-20 with mandatory PKI eliminates the EVCCID impersonation vulnerability, this transition faces substantial practical barriers. The installed base of legacy vehicles supporting only DIN 70121 represents millions of units that cannot be upgraded via software due to hardware limitations in their communication controllers. Charging Point Operators face a dilemma where maintaining backward compatibility with DIN 70121 preserves the attack surface, while dropping support alienates customers with older vehicles. Industry consortia have not established concrete deprecation timelines for DIN 70121, unlike decisive sunset schedules imposed for obsolete TLS versions in web security. Furthermore, certificate lifecycle management introduces new operational complexity where vehicles must securely provision and rotate certificates, requiring reliable over-the-air update mechanisms and revocation infrastructure. If these PKI components are not implemented correctly, ISO 15118-20 deployments could introduce new vulnerabilities while simultaneously creating false security assurance.

9 Related Work

Recent comprehensive surveys [17, 20] categorize EV charging security research into physical-layer, protocol-layer, and application-layer vulnerabilities, highlighting the gap between protocol compliance and practical security assurance. The security of electric vehicle (EV) charging systems has recently gained growing attention, particularly regarding the vulnerabilities in the EV-to-charger communication channel defined by DIN SPEC 70121 and ISO 15118. These protocols employ HomePlug GreenPHY power-line communication (PLC) over the charging cable, yet lack robust physical- and link-layer protections. Early analyses in [7] demonstrated that unencrypted HomePlug signals can be sniffed using off-the-shelf SDRs, exposing identifiers, charging sessions, and even authentication exchanges. Later, the Brokenwire attack [22] showed that weak electromagnetic interference can disrupt ongoing CCS charging sessions from tens of meters away. These findings reveal that the PLC layer offers neither confidentiality nor integrity, leaving higher-layer authentication exposed to

low-cost eavesdropping or desynchronization. However, most of these works focus on denial-of-service or eavesdropping, rather than on active impersonation or discharge manipulation that could physically endanger the vehicle or grid.

At the electrical interface level, recent work [36] introduced Portulator devices capable of injecting rogue signals through the control pilot (CP) and proximity (CC) lines, spoofing valid charging states and forcing unsafe operations. By altering CP duty cycles or CC resistance, attackers can trick EVs into false connection states, trigger denial-of-service, or even force reverse current flow. These findings underscore the absence of hardware-level authentication in the IEC 61851 handshake. Yet, these experiments primarily demonstrated local DoS and charge disruption, and have not systematically explored energy-theft or controlled discharge scenarios. More recently, the PIBuster attack [38] exploited HomePlug modem firmware misconfigurations to achieve denial-of-service. However, these low-level attacks remain orthogonal to our application-layer protocol exploitation.

At the protocol level, ISO 15118's Plug-and-Charge mechanism continues to be a primary focus of research concerning impersonation. Attacks such as EVExchange [12] showed that an adversary can relay handshake messages between two charging stations to impersonate a victim EV, charging at the victim's expense or draining energy via unauthorized V2G discharge. A complementary analysis of OCPP protocol vulnerabilities demonstrates similar authentication weaknesses across EV charging communication standards [3]. However, EVExchange requires deploying malicious relay devices at two separate charging stations with simultaneous presence of both victims and attackers, and was validated only in MiniV2G simulation environments, rather than in production infrastructure. Nevertheless, these studies primarily consider logical replay and message relay scenarios, assuming an adversary on the data link—not one with direct physical access or the ability to modify low-level electrical signals and device identifiers simultaneously. Furthermore, prior impersonation research remained in laboratory settings without validation against commercial Autocharge systems deployed in public infrastructure. Charge manipulation attacks [18] demonstrate how adversaries can alter charging parameters to commit fraud or destabilize grid operations, complementing our findings on forced discharge.

A closely related forced-discharge attack, DrainDead [26], was published concurrently, and both efforts independently identify a BMS state-confusion vulnerability. DrainDead provides a broader evaluation across a European vehicle fleet, while our work focuses on a real-world EVCCID-impersonation attack in commercial charging networks. We also independently validate forced-discharge behavior in a hardware-in-the-loop setup on an East Asian fleet, with consistent results on the Hyundai IONIQ 6, the only overlapping model across both studies. Moreover, ecosystem-level vulnerability analyses [31] reveal that security failures in a single component (e.g., EVSE firmware) can cascade across the entire charging infrastructure, validating our findings that protocol-level weaknesses enable both infrastructure-side and vehicle-side attacks.

10 Conclusion

This work exposes critical vulnerabilities in the DIN 70121-based charging infrastructure that underpins millions of deployed electric vehicles worldwide. Through the HotWire attacks, we demonstrated the first practical end-to-end EVCCID impersonation attack against commercial Autocharge systems, enabling untraceable energy theft from public charging infrastructure, and uncovered a forced discharge vulnerability that allows adversaries to drain vehicle batteries through BMS state confusion. Our evaluation across four production EV models and seven charging stations confirms that these are not theoretical weaknesses but immediately exploitable flaws affecting real-world systems in daily use.

The attacks reveal a fundamental design failure where adherence to protocol specifications provides false security assurance while leaving systems vulnerable to logical exploitation. DIN 70121's lack of cryptographic authentication and the observed reliance on protocol state machines over physical sensor verification demonstrate that protocol compliance cannot substitute for defense-in-depth security design. Both vulnerabilities succeed because implementations trust message sequencing and syntactic correctness rather than enforcing cryptographic proof of identity or hardware-validated physical conditions. This gap between standards compliance and security robustness represents a systemic risk that extends beyond EV charging to other cyber-physical systems, where safety-critical operations depend on unauthenticated communication channels. To accelerate remediation and enable community-driven security validation, we will release our open-source testing platform following coordinated disclosure timelines.

LLM Usage Considerations

LLMs were used for editorial purposes in this manuscript, and all outputs were inspected by the authors to ensure accuracy and originality.

Acknowledgments

This research was supported in part by the U.S. National Science Foundation under Grant No. 2235232 and by the Taiwan National Science and Technology Council under Grant No. NSTC 114-2634-F-011-002-MB.

References

[1] ISO 15118-3 Road vehicles – Vehicle to grid communication interface – Part 3: Physical and data link layer requirements, 2015.

[2] Samrat Acharya, Yury Dvorkin, Hrvoje Pandžić, and Ramesh Karri. Cybersecurity of smart electric vehicle charging: A power grid perspective. *IEEE access*, 8:214434–214453, 2020.

[3] Cristina Alcaraz, Javier Cumplido, and Alicia Triviño. Ocpp in the spotlight: threats and countermeasures for electric vehicle charging infrastructures 4.0. *International Journal of Information Security*, 22(5):1395–1421, 2023.

[4] Muhammad Nouman Ali, Georges Kaddoum, Wei Li, Chau Yuen, Muhammad Tariq, and H. Vincent Poor. A smart digital twin enabled security framework for vehicle-to-grid cyber-physical systems. *IEEE Transactions on Information Forensics and Security*, 18:5258–5271, 2023.

[5] Joseph Antoun, Mohammad Ekramul Kabir, Bassam Moussa, Ribal Atallah, and Chadi Assi. A detailed security assessment of the ev charging ecosystem. *IEEE network*, 34(3):200–207, 2020.

[6] Luca Attanasio, Mauro Conti, Denis Donadel, and Federico Turrin. Miniv2g: An electric vehicle charging emulator. In *Proceedings of the 7th ACM on Cyber-Physical System Security Workshop*, CPSS '21, page 65–73, New York, NY, USA, 2021. Association for Computing Machinery.

[7] R. Baker and I. Martinovic. Losing the car keys: Wireless phy-layer insecurity in ev charging. *USENIX Security Symposium*, pages 407–424, 2019.

[8] Kaibin Bao, Hristo Valev, Manuela Wagner, and Hartmut Schmeck. A threat analysis of the vehicle-to-grid charging protocol iso 15118. *Computer Science-Research and Development*, 33(1):3–12, 2018.

[9] Imen Benfarhat, Victor Goh, C. L. Siow, Muhammad Sheraz, and Teong Chee Chuah. Temporal convolutional network approach to secure open charge point protocol (ocpp) in electric vehicle charging. *IEEE Access*, 13:15272–15289, 2025.

[10] Brennan Borlaug, Shawn Salisbury, Matthew Gerdes, and Matteo Muratori. Levelized cost of charging electric vehicles in the united states. *Joule*, 4(7):1470–1485, 2020.

[11] Claire Chang and Tilden Chen. Why pre-charge circuits are necessary in high-voltage systems. *TI, Accessed: Online 08/2024*, 2021.

[12] Mauro Conti, Denis Donadel, Radha Poovendran, and Federico Turrin. Evexchange: A relay attack on electric vehicle charging system. In *European Symposium on Research in Computer Security*, pages 488–508. Springer, 2022.

[13] dSpace Group. dsv2gshark: Wireshark dissector for ISO 15118 and DIN 70121. https://github.com/dspace-group/dsV2Gshark, 2024. Accessed: 2025-04-30.

[14] Zacharenia Garofalaki, Dimitrios Kosmanos, Sotiris Moschoyiannis, Dimitrios Kallergis, and Christos Douligeris. Electric vehicle charging: A survey on the security issues and challenges of the open charge point protocol (ocpp). *IEEE Communications Surveys & Tutorials*, 24(3):1504–1533, 2022.

[15] Mohit Girdhar, Junho Hong, Hyunwoo Lee, and Taewon Song. Hidden markov models-based anomaly correlations for the cyber-physical security of ev charging stations. *IEEE Transactions on Smart Grid*, 13(5):3903–3914, 2022.

[16] A. Heinrich and R. Heddergott. Secure and user-friendly ev charging: A comparison of autocharge and iso 15118's plug & charge. Technical report, V2G Clarity and Hubject, 2019. Accessed: 2025-11-14.

[17] Xuefei Hu, Xinghua Jiang, Jiangfan Zhang, Shuhang Wang, Minghai Zhou, Bingxin Zhang, Zhipeng Gan, and Bin Yu. Electric vehicle charging network security: A survey. *Journal of Systems Architecture*, 159:103337, 2025.

[18] Hossein Jahangir, Subhash Lakshminarayana, and H. Vincent Poor. Charge manipulation attacks against smart electric vehicle charging stations and deep learning-based detection mechanisms. *IEEE Transactions on Smart Grid*, 15(5):5182–5194, 2024.

[19] Jay Johnson, Benjamin Anderson, Brian Wright, Jimmy Quiroz, Timothy Berg, Russell Graves, Josh Daley, Kandy Phan, Michael Kunz, Rick Pratt, et al. Cybersecurity for electric vehicle charging infrastructure. Technical report, Sandia National Lab.(SNL-NM), Albuquerque, NM (United States), 2022.

[20] Amandeep Kaur, Navid Valizadeh, Dhruv Nandan, Tomasz Szydło, Jaganathan Rajasekaran, Vinod Kumar, Masoud Barika, Jie Liang, Rajiv Ranjan, and Rana Omer. Cybersecurity challenges in the ev charging ecosystem. *ACM Computing Surveys*, 2025.

[21] Ahmet Kilic. Secure and convenience charging communication between electric vehicle and charging station with plug and charge. *Electric Power Systems Research*, 243:110371, 2025.

[22] S. Köhler, R. Baker, M. Strohmeier, and I. Martinovic. Brokenwire: Wireless disruption of ccs electric vehicle charging. *ArXiv*, abs/2202.02104, 2022.

[23] Lukas Lanz, Benjamin Noll, Tobias S. Schmidt, and Björn Steffen. Comparing the levelized cost of electric vehicle charging options in europe. *Nature Communications*, 13(5951), 2022.

[24] Seokcheol Lee, Yongmin Park, Hyunwoo Lim, and Taeshik Shon. Study on analysis of security vulnerabilities and countermeasures in iso/iec 15118 based electric vehicle charging technology. In *2014 International conference on IT convergence and security (ICITCS)*, pages 1–4. IEEE, 2014.

[25] Yining Liang, Yining Liu, Xuhui Zhang, and Guangjie Liu. Physically secure and privacy-preserving charging authentication framework with data aggregation in vehicle-to-grid networks. *IEEE Transactions on Intelligent Transportation Systems*, 25:18831–18846, 2024.

[26] Jakob Löw, Dominik Bayerl, Kevin Mayer, and Hans-Joachim Hof. Draindead: Emptying batteries of parked electric vehicles. In *Proceedings of the 3rd USENIX Symposium on Vehicle Security and Privacy (VehicleSec '25)*, Seattle, WA, USA, August 2025.

[27] Sai Murlidharan, Vineeth Ravulakole, Jayanth Karnati, and Haroon Malik. Battery management system: Threat modeling, vulnerability analysis, and cybersecurity strategy. *IEEE Access*, 13:37198–37220, 2025.

[28] Tony Nasr, Sadegh Torabi, Elias Bou-Harb, Claude Fachkha, and Chadi Assi. Power jacking your station: In-depth security analysis of electric vehicle charging station management systems. *Comput. Secur.*, 112(C), January 2022.

[29] National Vulnerability Database. CVE-2022-27948: Tesla vehicles charge port door can be opened by spoofed radio signals. https://nvd.nist.gov/vuln/detail/CVE-2022-27948, 2022. Accessed: 2025-04-30.

[30] OpenInverter Community. PyPLC: HomePlug Modem Modification Guide for EV Charging Communication. https://openinverter.org/wiki/PyPLC, 2024. Accessed: 2025-04-30.

[31] Richa Plaka, Mikael Asplund, and Simin Nadjm-Tehrani. Vulnerability analysis of an electric vehicle charging ecosystem. In *Critical Information Infrastructures Security (CRITIS 2023)*, pages 155–173, 2023.

[32] Qualcomm Atheros. open-plc-utils: Powerline Communication utility software. https://github.com/qca/open-plc-utils, 2024. Accessed: 2026-06.

[33] Bardia Raouf and Saman Mousavian. Active to reactive power attack in interconnected electric power systems and electric vehicle charging stations. *IEEE Access*, 13:39600–39609, 2025.

[34] Dharavath Ronanki and Harish Karneddi. Electric vehicle charging infrastructure: Review, cyber security considerations, potential impacts, countermeasures, and future trends. *IEEE Journal of Emerging and Selected Topics in Power Electronics*, 12:242–256, 2024.

[35] Khaled Sarieddine, Malek Sayed, Chadi Assi, Ribal Atallah, Sadegh Torabi, Joe Khoury, Mahdi Pour, and Elias Bou-Harb. Ev charging infrastructure discovery to contextualize its deployment security. *IEEE Transactions on Network and Service Management*, 21(1):1287–1301, 2024.

[36] Hetian Shi, Yi He, Shangru Song, Jianwei Zhuge, and Jian Mao. Physical-layer signal injection attacks on ev charging ports: Bypassing authentication via electrical-level exploits. *arXiv preprint arXiv:2506.16400*, 2025.

[37] Seyedeh Shirvani, Yasaman Baseri, and Ali Ghorbani. Evaluation framework for electric vehicle security risk assessment. *IEEE Transactions on Intelligent Transportation Systems*, 25(1):33–56, 2024.

[38] Marcell Szakály, Sebastian Köhler, and Ivan Martinovic. Pibuster: Exploiting a common misconfiguration in CCS EV chargers. In *Proceedings of the 3rd USENIX Symposium on Vehicle Security and Privacy (VehicleSec '25)*, Seattle, WA, USA, August 2025.

[39] M. Szakály, S. Köhler, and I. Martinovic. Current affairs: a security measurement study of ccs ev charging deployments. In *Proc. 34th USENIX Security Symp. (USENIX '25)*, 2025.

[40] uhi22. Openv2gx: An open-source implementation of the v2g (vehicle-to-grid) communication protocol iso/iec 15118. https://github.com/uhi22/OpenV2Gx. Accessed: 2025-04-30.

[41] uhi22. pyPLC: Open-source EV charging communication simulation, 2023. Accessed: 2025-04-30.

[42] World Resources Institute. These countries are adopting electric vehicles the fastest, 2023. Accessed: 2025-04-30.

A Ethics Considerations

All experiments were conducted under strict ethical protocols to prevent harm to individuals, property, and critical infrastructure. For the EVCCID impersonation attack validation, we used only our own pre-registered user accounts at public

charging stations, ensuring no third-party victim was financially burdened by our testing. The charging session was terminated after confirming successful authentication bypass and energy delivery, limiting energy consumption to 1.25 kWh paid through our registered account. We did not conduct sustained energy theft or target accounts belonging to unaffiliated individuals. For EVCCID reconnaissance, we obtained identifiers exclusively from vehicles owned by our research team or provided by collaborating automotive manufacturers under non-disclosure agreements, avoiding unauthorized data collection from the general public.

The forced discharge attack evaluations were conducted entirely within controlled environments on private property, with no experiments performed on vehicles in public spaces or fleet operations. All test vehicles were owned by participating manufacturers or our institution and were under continuous monitoring throughout discharge experiments. We implemented multiple safety interlocks, including emergency contactors, current limiting circuits, and automated session termination triggers set at 10% state-of-charge reduction thresholds to prevent battery deep-discharge or thermal stress. No vehicle sustained battery damage or experienced state-of-charge depletion below manufacturer-recommended safe operating limits. All experiments were performed with vehicles in a parked state with parking brakes engaged and high-voltage safety gear worn by researchers to prevent electrical injury.

We initiated responsible disclosure several months before submission, following coordinated-disclosure norms. We provided detailed technical reports (vulnerability descriptions, proof-of-concept sequences, affected versions, and recommended countermeasures) to two of the four automotive manufacturers and the seven charging network operators we evaluated, and also filed reports with an East Asian national vulnerability reporting platform to coordinate with affected vendors in the region.

As of the submission date, two manufacturers have acknowledged the BMS state confusion vulnerability and committed to firmware updates that implement hardware-based voltage verification before contactor closure, with deployment timelines of 6 to 12 months via over-the-air updates. The 180-day coordinated-disclosure embargo has since elapsed, and we have publicly released the toolkit. We withhold specific EVCCID values, charging station identifiers, and implementation details that could enable adversaries to target specific victims or infrastructure.

B Open Policy and Data Access

To promote reproducibility and enable community-driven security research, we release the HOTWIRE toolkit as open-source software under the GNU General Public License v3.0 (GPLv3) following the coordinated disclosure period described in Section A. The toolkit includes complete Python implementations of bidirectional DIN 70121 emulation, hardware schematics for QCA7005-based PLC interfaces, parameterized attack scenario templates, and comprehensive documentation with build instructions and safety protocols. The archived artifact (with a permanent DOI) is available at https://doi.org/10.5281/zenodo.20596315, and the actively maintained development version is at https://github.com/sickcell6000/HotWire. To protect privacy, we do not release raw experimental data containing EVCCID values, charging station identifiers, or geographic locations; instead, we provide anonymized datasets including BMS behavioral profiles, protocol compliance metrics, and attack success rates sufficient for validating our findings.

The HOTWIRE toolkit is designed exclusively for defensive security research, authorized penetration testing, and academic investigation. Users must obtain explicit written authorization from infrastructure owners and vehicle owners before conducting security testing. The GPLv3 license ensures that derivative works and improvements remain open-source, preventing proprietary weaponization of our research tools while enabling the security community to collaboratively strengthen EV charging infrastructure defenses. We acknowledge the dual-use risk, but transparent disclosure under a copyleft license accelerates ecosystem-wide remediation more effectively than security through obscurity, empowering defenders to find and fix vulnerabilities before adversaries exploit them at scale.