Current Affairs: A Security Measurement Study of CCS EV Charging Deployments

Marcell Szakály
University of Oxford

Sebastian Köhler
University of Oxford

Ivan Martinovic
University of Oxford

Abstract

Since its introduction in 2012, the Combined Charging System (CCS) has emerged as the leading technology for EV fast charging in Europe, North America and parts of Asia. The charging communication of CCS is defined by the ISO 15118 standards, which have been improved over the years. Most notably, in 2014, important security features such as Transport Layer Security (TLS) and usability enhancements such as Plug and Charge were introduced.

In this paper, we conduct the first measurement study of publicly deployed CCS DC charging stations to capture the state of deployment for different protocol versions and to better understand the attack surface of the EV charging infrastructure. In our evaluation, we examine 325 chargers manufactured between April 2013 and June 2023, and installed as late as May 2024 by 26 manufacturers across 4 European countries. We find that only 12% of the charging stations we analyzed implement TLS at all, leaving all others vulnerable to attacks that have already been demonstrated many years ago. We observe an increasing trend in support for ISO 15118-2 over the years, reaching 70% of chargers manufactured in 2023. We further notice that most chargers use a decade-old firmware for their HomePlug modems, which could contain vulnerabilities that have been patched since. Finally, we discuss design flaws with the Public Key Infrastructure system used in EV charging, and propose changes to improve the adoption and availability of TLS.

1 Introduction

Electric Vehicles (EVs) are rapidly emerging as an important transportation technology, seeing increasing deployment as both personal vehicles and in critical fleets such as logistics [38, 49], healthcare [43], government [16], mining [2], ferries [47] or public transport [39]. The Combined Charging System (CCS) is the most widely used standard for DC fast charging of vehicles in Europe [33], and it is also widely deployed in other regions. CCS is a complicated protocol

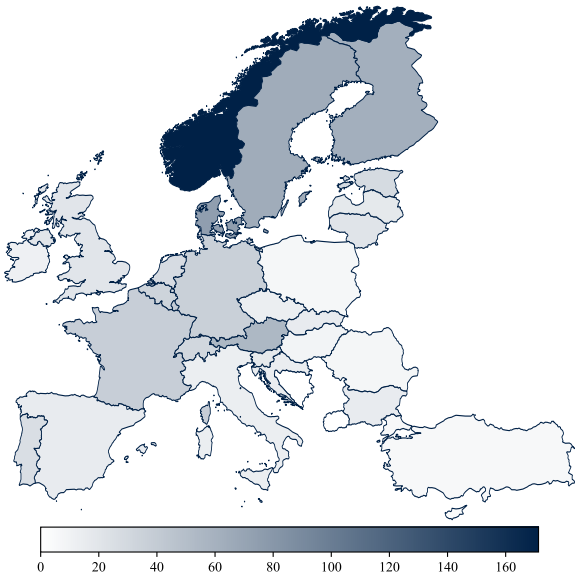

Figure 1: DC Chargers in Europe per 100,000 population, based on data from the European Union as of September 2024 [19].

that offers convenience features in addition to power transfer and uses a modern, digital communication scheme. This communication carries essential information, including safety-critical power limits. Researchers have identified a variety of high-impact attacks [1, 5, 22], such as Denial of Service [35], tampering [14], information theft [4] or electricity theft [10]. They have also shown that despite CCS using a wired communication medium, the physical layer creates an unintentional wireless channel [4, 35], which exposes all of these communication attacks to wireless adversaries. Modern versions of the standard aim to combat some of these issues by introducing state of the art security, such as TLS 1.3, however older versions remain in use for compatibility.

While TLS addresses many of the security vulnerabilities identified by researchers, we lack information about its actual

deployment. Interoperability is essential for users and regulators to ensure a smooth transition to all-electric vehicles and this requires that each charger and vehicle supports a common version of the protocol. This is most easily achieved if everyone implements the first and oldest version of CCS as a common fallback. However, if all chargers and vehicles support a newer version, then old versions can be phased out. As a result, a key open research question is whether the newer, more secure versions of the standard are being deployed and whether the oldest and insecure 2012 version is being phased out. In this paper, we address this question with a large-scale experimental study of DC CCS chargers across Europe.

It is often assumed in a variety of domains that insecure and outdated practices remain in use long after better alternatives exist. However, for EV charging, secure CCS has existed for almost as long as CCS itself, and the field has attracted involvement and standardization from governments. We believe that regardless of expectations, providing a domain specific snapshot of the industry is important. To our knowledge, no previous work has examined the deployment of CCS versions. The most closely related paper [42] scanned the Internet for exposed management back-ends of EV chargers, whereas our work focuses on the interface between vehicles and chargers. We summarize our key contributions and findings as follows:

- We designed and implemented an EV emulator, enabling us to collect the first and largest real-world dataset of CCS implementations, comprising data from 325 unique chargers. Our design and data will be made publicly available upon publication.
- Our study reveals that support for Transport Layer Security (TLS) is lacking across all the chargers tested, with only a small fraction (12%) supporting it.
- The results also show that ISO 15118-2, a decade-old protocol, has only recently started to gain traction.
- We discuss the security benefits and implementation cost of TLS.
- During the discussion we identify a trust issue with the current use of TLS certificates.
- We propose easy-to-implement and backwards-compatible countermeasures to combat this issue, making TLS in CCS more effective and accessible.

2 Security of CCS

In this section, we introduce CCS and explain how the protocol works. Along the way, we identify key security-related design decisions and features, discuss how they are adapted in different versions of the protocol, and pose experimental questions for our study.

In addition to DC charging, CCS also defines AC charging and bi-directional power transfer using the same protocol. Furthermore, newer versions of the standard allow for Plug and Charge (PnC), where the vehicle is able to pay automatically.

Besides CCS, other EV charging technologies such as the North American Charging Standard (NACS), formerly known as Tesla Supercharger, CHAdeMO and GB/T exist. Out of these, the European Union legally requires high-powered DC chargers to offer CCS [18], and the US government only supports charging infrastructure projects that offer CCS [21]. CCS and NACS differ only in the physical connector, but use the same protocols described in the ISO 15118 standards [58]. Due to this wide adoption and standardization, we chose to study public DC CCS charging in this work. Figure 1 provides an overview of the current deployment of DC charging stations across Europe.

2.1 Basic Signaling

The basic signaling process was developed for use in AC charging and remains a part of CCS for compatibility. It is a simple Pulse Width Modulated (PWM) signal and does not carry any digital information. Previous research has demonstrated that this process can be attacked in AC charging by inserting a device into the cable [63], while wireless attacks on PWM signals have also been demonstrated outside the EV context [11]. However, since CCS uses only a simplified version of the basic signaling for presence detection, these attacks are not applicable to CCS.

2.2 Physical Layer

The ISO 15118-3 [30] standard defines the use of HomePlug Green PHY (HPGP) power line communication as the physical layer for all higher layer protocols. HPGP is designed to carry Ethernet traffic over just two household mains wires, making it well suited for use in noisy environments over unshielded cables. To achieve these features, HPGP mimics wireless protocols in structure, using OFDM modulation and robust forward error correction. However, this RF-like design of the physical layer also allows it to couple into devices either via shared power lines or even wirelessly [3]. This makes the wired communication channel wirelessly accessible, allowing attackers to intercept [4] and hijack the charging communication in a way that could normally only be possible via a wired Man-in-the-Middle (MitM). We therefore consider attacks targeting this communication channel to be feasible.

2.2.1 SLAC Process

In HPGP, modems join encrypted networks based on a 128-bit Network Membership Key (NMK), allowing different networks to coexist securely on the same medium. The NMK is the basis of physical-layer encryption in each network, and

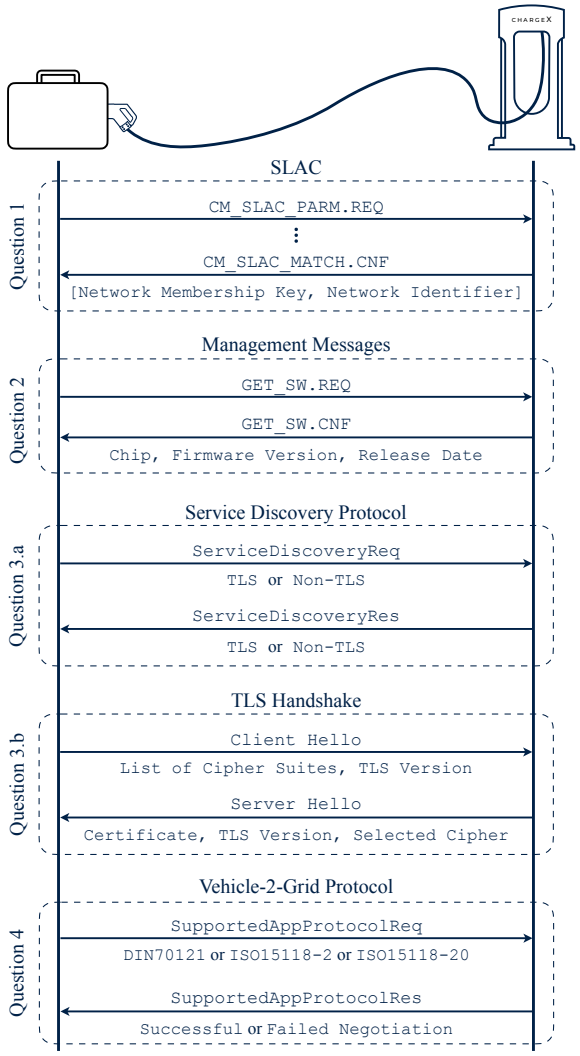

Figure 2: The design of our experiments, which follows the same flow as the CCS protocol. We show what data is exchanged at each stage in the protocol and how this maps to our experimental questions.

knowledge of it allows attackers to join and interact with the traffic flowing through it [14]. Additionally, if attackers have recorded the traffic, they could potentially decrypt it later [4]. In CCS, the charger and vehicle share the NMK using the Signal Level Attenuation Characterization (SLAC) process.

SLAC serves two purposes: in addition to distributing the NMK, it allows the vehicle to measure which charger it is connected to. This measurement is necessary when, due to the leakage of HPGP signals, a vehicle can communicate with multiple chargers. The vehicle measures its attenuation (signal strength) to each charger and selects the best one. Then, the charger sends the NMK in cleartext to the vehicle. This allows any attacker present at the start of the charging session to capture the NMK, and access the network [4, 14].

Alternatively, if an attacker can predict the NMK, they can equally join the network and access the higher level communication at any point during the charging session. No previous work has studied the existence of weak NMKs, instead capturing the cleartext at the start [4]. Being able to predict the key and join later during an active charging session would however greatly increase the attack surface and, for example, make drive-by attacks practical.

Each network also has a 54-bit Network ID (NID), which is broadcast in regular unencrypted beacons. According to the standard [26], the NID should be calculated deterministically from the NMK using PBKDF1 (a type of hash function) without any additional salt. In the case of a low entropy NMK, knowing the NID can allow the attacker to determine the NMK via offline computation or a hash table, using attainable resources. Since the NMK is intended to prevent unauthorized access to the network, a weak or easily guessed NMK could make it possible for an attacker to manipulate the charging communication. As a result, we ask the following question:

Q 1: *What is the entropy of charger NMKs? Can they be determined from the NID?*

2.2.2 HPGP Modem

Like all complex software, firmware in embedded systems can contain bugs such as buffer overflows and memory corruption. These can often be turned into code execution attacks, making their potential impact high. HPGP chips have a complex firmware, handling a large number of management messages, variable length data and networking protocols. Popular HomePlug chips such as Qualcomm's QCA 7500 have had many public security advisories for vulnerabilities in recent years [45]. Hence, it is important to ensure that HomePlug modems have the latest firmware, leading us to the following question:

Q 2: *What chip and firmware versions do HPGP modems in chargers use?*

2.3 Connection Establishment

Over the HPGP link, the charger and vehicle communicate using IPv6. The vehicle begins by sending a multicast Service Discovery Protocol (SDP) request to determine the IP address and port of the charger. In addition, this process negotiates support for TLS. The vehicle indicates in the request if it supports TLS, the charger decides what to offer based on the request and its capabilities. The charger opens the appropriate server socket and sends the IP, port, and TLS support to the vehicle. If the charger does not offer a TLS connection when asked for one, then it does not implement any form of TLS. The SDP process is by design vulnerable to a downgrade attack, which could allow attackers to force an unencrypted

connection [62]. The simplest mitigation to this is to deprecate non-TLS connections entirely.

During the TLS handshake, the client and server negotiate the supported TLS version, cipher suites, and exchange certificates. Outdated TLS versions, insecure cipher suites or weak certificates could compromise the security of the TLS connection. Similar to the NMK, TLS would provide an additional layer of security, making it more difficult for an adversary to eavesdrop on and interfere with the charging communication. To understand the attack surface, we pose the following questions:

Q 3: *(a) How many chargers support TLS, and have any deprecated non-TLS sessions? (b) How is it implemented?*

2.4 Vehicle-to-Grid

The Vehicle-to-Grid (V2G) protocol carries the application layer information for CCS, including power delivery negotiation or payment information. Three versions of this protocol are publicly available, released in three different standards throughout the years. Newer versions introduce both usability and security features, which we briefly summarize below.

DIN SPEC 70121: The first version of the V2G protocol published in 2012, DIN SPEC 70121 contains only the bare minimum needed for power transfer. It does not use TLS or any other methods to protect the communication.

ISO 15118-2: Published in 2014, ISO 15118-2 improves on DIN by introducing optional TLS connections, where the charger is the server, and EV is the client. When TLS is used, it also introduces optional Plug and Charge (PnC), where the vehicle automatically authenticates and pays using a PKI scheme. It further introduces scheduled charging plans, to take advantage of expected electricity price changes.

ISO 15118-20: The newest version, ISO 15118-20 introduces new features such as bi-directional power transfer. On the security front, it requires mandatory mutual TLS, i.e., the charger and the vehicle both authenticate using certificates [41].

While the standards share many similarities, making it possible to implement them using largely shared code, they are not compatible. To offer compatibility and allow chargers to implement multiple versions simultaneously, V2G communication starts with a protocol version negotiation.

Q 4: *Which CCS protocol versions do chargers and vehicles support?*

A simplified, graphical representation of the CCS protocol and its mapping to the questions we will answer in this study is shown in Figure 2.

3 Experimental Methods

Our experimental questions about chargers can be answered by performing multiple CCS charging sessions and studying their behavior. To achieve this, we developed a vehicle emulator, which implements CCS and saves all relevant information for further analysis. Unlike a normal vehicle, our emulator implements multiple versions of CCS and alternates between them, thereby querying the charger about its capabilities. Reading the standards and implementing them ourselves gave us detailed insights into CCS implementations, which aids our discussion later.

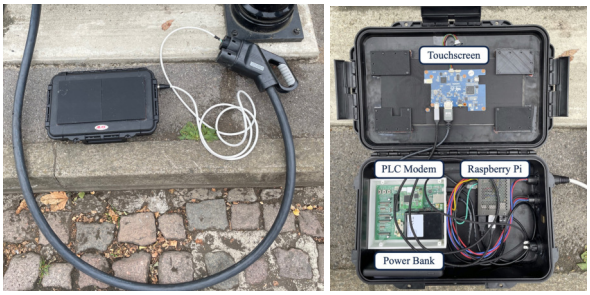

Figure 3: The data collection box during one of our experiments. The box contains a touch screen in the top half of the case and power bank, Raspberry Pi and PLC modem in the bottom half.

3.1 Emulator Design

Our vehicle emulator implements the hardware necessary for basic signaling and HPGP, and has the software implementation for the SLAC, service discovery, and V2G communication. It is built inside of small transport cases as seen in Figure 3, with an integrated powerbank and touchscreen for portability. Additionally, a web interface on a connected smartphone can control the emulator and provides GPS and camera access for data tagging.

The data collection software runs on a Raspberry Pi 4, extended with a custom versatile PCB that contains the electronics needed to perform basic signaling as an EV. The Pi is widely available, offers enough performance for a modern graphical operating system and high level programming languages, can easily be powered from a power bank, and has many IO pins for interfacing with custom hardware, which are used by our custom PCB. To provide HPGP capabilities, a Devolo "dLAN Green PHY eval board II" board is connected to the Pi using Ethernet, and configured to EV mode following the instructions in [46]. Others have shown that cheap consumer HomePlug AV modems can be converted to CCS-compatible HPGP modems via appropriate configuration [25], but we opted to use a device specifically designed for HPGP EV charging applications. Our device connects to the charger via a 3D-printed CCS socket, as it would be found on a vehicle. For safety reasons, we only connected to the data and ground pins necessary for communication and not the power pins.

The Raspberry Pi runs Raspbian, and uses the Linux ker-

nels implementation for the IPv6 and TCP/UDP stacks. We converted the SLAC and firmware querying tools from the `open-plc-utils` project by Qualcomm [46] into a C Python module. The SDP and V2G protocol stack were written in Python and used a modified version of V2GDecoder [13] to translate between the binary and structured representation of V2G messages.

For the purpose of our evaluation, we extensively logged all valuable data that might help to answer our research questions. In addition, `tcpdump` is used to collect full packet captures of all traffic sent over the HPGP network link for manual analysis.

To ensure a correct implementation, we tested our emulator against the `SwitchEV iso15118` [55] project, an open source implementation of an ISO 15118-2 and -20 charger, as well as against our own implementation of a charger. We are thus confident that our implementation is able to collect accurate and meaningful results. The log files from our script and the raw packet captures are processed automatically into a distilled version of the data. Additionally, we examined the data for any anomalies that are not part of our pre-existing experimental questions.

Our implementation differs from real devices in one way: to simplify experiments and facilitate data collection, our circuit board can electrically unplug itself using relays, without the need for a physical disconnection of the plug. This allows the data collection at each charger to be executed fully automatically, as the emulator can re-connect itself and perform multiple different charging sessions after each other automatically.

3.2 Charger Measurement Procedure

To answer our questions about chargers, at each device we perform multiple experiments. Each experiment consists of a full charging session, as it would be done by a real vehicle, including connecting our emulator, basic signaling, SDP, connection establishment, and protocol negotiation. After this, the V2G communication is terminated in a proper manner before power delivery, and the emulator electrically unplugs itself, allowing the charger to reset before the next experiment. Between each experiment, we change the properties of our EV emulator to test for different versions and parts of the protocol. Some experiments are automatically skipped based on the results of others: for example, if a charger indicates that it does not support TLS, all further experiments that aim to detect the TLS server version are skipped.

To answer Q 1 we collect the NMK and NID from multiple SLAC processes on the same charger. As each experiment on a charger contains a new SLAC exchange, this data is passively collected. In addition, to answer Q 2, the HPGP device information is queried after every successful SLAC. To measure TLS support (Q 3), in some experiments we send an SDP query requesting a TLS connection, and in other cases request a non-TLS session.

Table 1: TLS configurations for experiments to answer Q 3.

TLS	Configuration
1.3	Mutual authentication for ISO 15118-20
$\geq$1.2	Only required cipher suites for ISO 15118-2
1.2	Non-standard “recommended” cipher suites
1.2	Non-standard and “not recommended” cipher suites
$\leq$1.1	-

For chargers that support TLS at the SDP level, we perform further experiments, each using differently configured TLS clients, collecting more data to answer Q 3. Table 1 provides the configuration details for the experiments. We used the IANA list of TLS cipher suites [61] to classify TLS ciphers into “recommended” and “not recommended” categories. A “recommended” cipher must be widely standardized, considered secure, and offer unique features that other recommended ciphers do not. Many of the “not recommended” ciphers have known security vulnerabilities, including non-ephemeral key exchange, short authentication tags (such as CCM8), and outdated algorithms such as DES.

Finally, with each connection type, we perform experiments to determine the list of supported protocols (Q 4). In all cases, we initiate a V2G session and offer all supported protocols, allowing the charger to indicate the newest version it supports. In addition, with the TLS 1.3, TLS 1.2 and standard TCP connection types, we perform additional experiments, where each protocol is offered alone in a separate experiment. This allows us to clearly determine which protocols the charger supports on each connection type.

As we did not have access to a valid ISO 15118-20 vehicle certificate for mutual authentication, we instead generated a self-signed certificate with the correct format. While it is unlikely that a real -20 charger would accept this, we are still able to infer their support for mutual TLS: During the handshake, the client (vehicle) does not proactively send its certificate, instead it is sent as a response to a Certificate Request message from the server. The presence of this request from the server indicates that the charger implements mutual TLS, which is only done for ISO 15118-20.

3.3 Charging Station Selection

Due to the large number of EV chargers, we studied a diverse subset of deployments. To make our data representative of a random subset of devices, we applied a geometric selection strategy, identifying regions or routes with a high charger density, regardless of their manufacturer or network, and attempted to visit all devices in the region. We noticed that cities, rural areas and highways often host different companies, so we included all of these environments in our dataset, in multiple countries. We collected enough data to cover most large

manufacturers and network operators, with multiple samples in various countries.

In total, we collected data from 149 charging installations (defined as one or more chargers deployed by the same Charge Point Operator (CPO) in close proximity), encompassing 325 chargers and 397 CCS plugs in total. The chargers were distributed in 4 countries: UK 144 (1.1%), Switzerland 117 (4.6%), Croatia 16 (2.9%), Hungary 48 (6.3%). In percentages we show the fraction of the total number of DC chargers in each country as of July 2024 [19] when we conducted our study. They spanned 26 different manufacturers, with the most plugs tested from ABB (113), Alpitronics (74), Tesla (48), Evtec (25), Efacec (24). The plugs were located along highways (85), cities (199), and smaller towns (113). Devices were manufactured between 2013 and mid 2023, and installed as late as May 2024. All but one tested charger was manufactured after the public release of ISO 15118-2 and TLS support in 2014, so these features could have been included directly from the manufacturer, without the need for software updates in the field.

4 Results

In this section, we present our measurements for each of the key areas investigated and highlight their implications. Later, the discussion looks at CCS security more generally based on our findings. When presenting our findings, we report the numbers as seen in our dataset, but later we use information about the known size of various networks to extrapolate our key findings to the wider area. In rare cases, it happened that an experiment on a particular charger could not be completed while other experiments on the same charger were successful. For example, we faced time pressure from an EV waiting to charge and could only run the most important experiments. In such situations, the specific charger was omitted from the particular analysis we did not have data for, resulting in each analysis having a slightly different total number of devices.

4.1 TLS in Chargers

Answer to Q 3

All chargers supported non-TLS sessions, 12% supported TLS, and 6% implemented standards-compliant TLS 1.2. None implemented mutual TLS.

Only 12 % of chargers from 5 manufacturers in our dataset responded to a TLS SDP request offering a TLS session. Figure 4 shows the support for ISO 15118-2 compatible TLS, broken down by the manufacturing date of devices, and a full detailed breakdown of all important results is shown in Table 2. Our most important observations from the TLS experiments are summarized in Table 4.

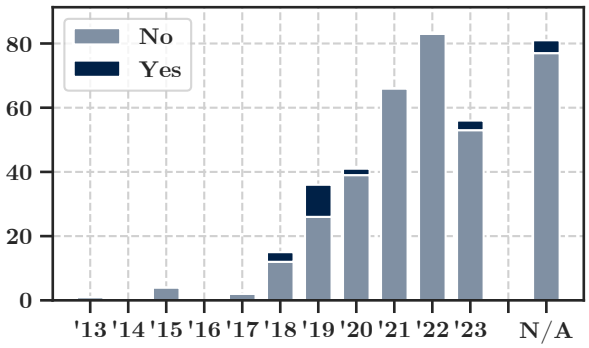

Figure 4: Support for TLS according to ISO 15118-2 based on charger manufacturing year in our data. We see no clear correlation with age, but instead a large spike in years when a particular manufacturer actively deployed many new installations across multiple countries.

4.1.1 Legacy Implementation

In our testing, one manufacturer used by two networks in multiple countries, offered TLS on all their tested devices, however they all refused connections from a TLS 1.2 client configured according to the standard. The standard requires using elliptic curve key exchange and certificates, instead these devices accepted TLS 1.2 and TLS 1.1 connections using an RSA based key exchange. They all had the exact same RSA-1024 certificate, that expired in 2013, long before their manufacturing date. We assume that this was implemented as part of testing during the standardization of ISO 15118, and was not removed from production devices. In addition, they do not advertise Plug and Charge capabilities. For further analysis we do not count these devices as supporting TLS, as they are not compatible with standard compliant vehicles expecting elliptic curves or up-to-date certificates. Accordingly, their security is equivalent to that of a charger with no TLS support.

4.1.2 Certificates

Considering only the implementations of TLS 1.2 and above, we examined the charger certificates, which could be traced back to root certificates from two of the largest V2G PKI providers, Hubject or Entrust. Both PKI providers implement the certificates correctly, following the certificate types and structure described in the standard. All of the European PnC networks used a Hubject root certificate.

The Entrust certificate was used by all tested devices from one of the manufacturers, deployed by 2 different networks. Furthermore, these devices shared one of only two leaf certificates, with a precisely 1 year shift in their window of validity. The certificates appeared to not be updated, since one of the two certificates had expired 3 months prior to testing. We

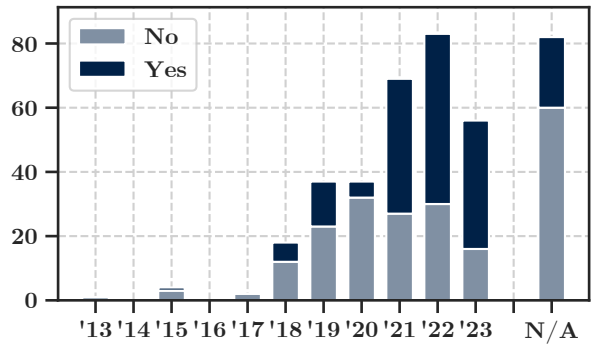

Figure 5: Support for ISO 15118-2 based on charger manufacturing year in our data. We see that new devices increasingly deploy this new version.

were already in contact with this company due to a vulnerability explained later, and also reported this. They confirmed that the devices were not meant to have TLS enabled, and were shipped with a development version and certificates. This is further confirmed since neither the manufacturer, nor the two networks using them currently advertise Plug and Charge capabilities, and the certificate content indicated that they were meant for the US market, using the US Entrust root. Our assumption is further backed up by observations of one of the two networks, who only had TLS enabled on their chargers from this manufacturer, but not on devices from other manufacturers.

4.1.3 Version Support

ISO 15118-2 requires the use of TLS 1.2 or higher, while -20 requires mutual TLS 1.3. Older versions should not be used, and cipher suites should be limited to those listed in the standard. In our dataset we found no chargers performing mutual TLS, and only ChargePoint had TLS 1.3 enabled. TLS 1.2 was implemented on devices by 4 manufacturers (Alpitronics, Ekoenergetyka, ChargePoint, Porsche) supplying 4 networks (Ionity, Instavolt, ChargePoint, Porsche), of which 2 networks (Ionity, Porsche) advertised Plug and Charge capability. Out of these 4 manufactures, one implemented unnecessary ciphers, however this was an IANA recommended cipher, and thus safe by current standards. However, this still highlights that real-world implementations can contain misconfigurations and deviations from the standard, exposing a larger attack surface than necessary. Only the company who used RSA certificates implemented not recommended ciphers.

Out of the Plug and Charge compatible networks, Ionity was supplied by two manufacturers (Alpitronics, Ekoenergetyka), but implemented TLS and Plug and Charge in both cases. Finally, Porsche uses only their own custom chargers and also implemented TLS consistently.

4.1.4 Implementation Strategy

One of the largest manufacturers, Alpitronics, supplies many different network operators. Their Ionity chargers use TLS and PnC, but none of the others offer PnC or have TLS enabled. Based on these observations, we assume that the TLS server software is implemented by the manufacturer, but the network operator decides whether to enable the feature and provides the certificates to do so. In the case of the company that used RSA or shared Entrust certificates, they released a development firmware with TLS enabled using development certificates into public devices, as we observed their devices exhibiting the same behavior on different networks with the same certificates. In networks where TLS and PnC are intentionally deployed (Ionity, Porsche), the certificates are supplied by the network operator.

4.1.5 Additional Observations

One manufacturer did not implement RFC 5746 [48] from 2010, which signals mitigation for the CVE-2009-3555 TLS renegotiation vulnerability. This was a vulnerability in the TLS protocol, and alongside fixing the issue, a new extension was introduced to TLS, allowing clients and servers to signal that they implement the revised version of the protocol. To our knowledge, both the mitigation and this signaling are implemented and enabled by default in all major TLS libraries, indicating either that it was manually disabled, or that they are using a very outdated library. The vulnerability allows any attacker to inject data into the start of a TLS session. When TLS is used as part of HTTPS, this exposes a powerful attack against the HTTP protocol. However, we are not aware of a way this could be usefully exploited against the binary encoding of the V2G protocol. Also, for ethical reasons we did not actively exploit this vulnerability, so it remains unknown if the device is vulnerable to the underlying attack. As per their vulnerability disclosure program, “Missing best practices in SSL/TLS configuration” and “Previously known vulnerable libraries without a working Proof of Concept” are out of scope.

One manufacturer’s chargers sent cleartext UDP packets to the EV during the TLS handshake. These packets contained information in the NSS Key Log format [12], and when their contents are loaded into standard tools such as Wireshark, they allow the TLS connection to be decrypted [60]. A similar behavior is described in [36], who explain that sending key info in UDP packets exactly as we observed is used in debugging tools by automotive vendors to decrypt and debug the TLS connections. However, this could similarly be performed by any attacker who has access to the physical layer, defeating the Diffie-Hellman key exchange in TLS. We reported this via email to a contact at the manufacturer in July 2024, who confirmed that it was intended as a debugging feature that accidentally made it into production.

Table 2: Detailed results for the key experimental questions, broken down per manufacturing year. Each cell contains the number of plugs as Yes/No. Note that not all experiments produced useful data, so the total number of experiments in each case may be different.

		Manufacturing Year											
	All	Unknown	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
TLS in SDP	47 / 344	7 / 76	0 / 1	0 / 0	0 / 4	0 / 0	0 / 2	12 / 6	18 / 19	5 / 36	0 / 66	2 / 81	3 / 53
TLS 1.3 for ISO 15118-20	4 / 380	4 / 77	0 / 1	0 / 0	0 / 4	0 / 0	0 / 2	0 / 14	0 / 36	0 / 41	0 / 66	0 / 83	0 / 56
TLS 1.2+ for ISO 15118-2	22 / 363	4 / 77	0 / 1	0 / 0	0 / 4	0 / 0	0 / 2	3 / 12	10 / 26	2 / 39	0 / 66	0 / 83	3 / 53
TLS 1.2 recommended ciphers	3 / 371	0 / 76	0 / 1	0 / 0	0 / 4	0 / 0	0 / 2	0 / 12	0 / 33	0 / 41	0 / 66	0 / 83	3 / 53
TLS 1.2 not recommended ciphers	3 / 371	0 / 76	0 / 1	0 / 0	0 / 4	0 / 0	0 / 2	0 / 12	0 / 33	0 / 41	0 / 66	0 / 83	3 / 53
TLS 1.1 and older	14 / 369	0 / 80	0 / 1	0 / 0	0 / 4	0 / 0	0 / 2	6 / 8	6 / 30	2 / 39	0 / 66	0 / 83	0 / 56
ISO 15118-20 DC	0 / 380	0 / 80	0 / 1	0 / 0	0 / 2	0 / 0	0 / 2	0 / 17	0 / 37	0 / 36	0 / 68	0 / 83	0 / 54
ISO 15118-2:2013	183 / 206	22 / 60	0 / 1	0 / 0	1 / 3	0 / 0	0 / 2	6 / 12	14 / 23	5 / 32	42 / 27	53 / 30	40 / 16
ISO 15118-2:2010	33 / 348	2 / 79	0 / 1	0 / 0	0 / 2	0 / 0	0 / 2	0 / 17	1 / 36	0 / 36	1 / 67	20 / 63	9 / 45
DIN SPEC 70121	389 / 0	81 / 0	1 / 0	0 / 0	4 / 0	0 / 0	2 / 0	18 / 0	37 / 0	39 / 0	69 / 0	82 / 0	56 / 0

4.2 Standard Support

In our experiments, chargers were offered all known CCS protocol versions individually. This allowed us to unambiguously determine which protocols a device supports, based on whether it accepts the protocol. Our results about supported protocols in chargers can be seen in detail in Table 2.

Answer to Q 4

All chargers support DIN SPEC 70121, and 47% implement ISO 15118-2. No chargers implemented 15118-20. All 8 tested vehicles supported DIN, and 7 supported 15118-2.

Despite ISO 15118-20 capable cars being advertised and sold, we are not aware of any public charger advertising this capability. Our testing included PnC capable chargers deployed at dealerships where ISO 15118-20 capable vehicles are sold, and even in this case we did not detect support for TLS 1.3, mutual TLS or ISO 15118-20.

Much like how all chargers offer non-TLS connections for compatibility, as the oldest and simplest version, DIN is still widely used as the common fallback option. However, an important trend visible in the data is a slow rise in ISO 15118-2 support based on manufacturing year, as shown in Figure 5. While most of these devices offered only the insecure version of ISO 15118-2, it is nonetheless important for newer versions of the protocol to be implemented.

4.3 HPGP Firmware

Answer to Q 2

All chargers used Qualcomm HPGP chips, and 62% had more than 10 years old firmware.

The breakdown of chip type and firmware versions can be seen in Figure 6. In all of our testing, devices used one of two different HPGP chips, the QCA 7000 (78%) and QCA 7005 (22%). Based on available information these chips appear to be nearly identical: they are advertised as pin compatible, share the same internal design and even firmware. The only publicly known difference between them is their temperature rating and release date. The most common firmware versions across a wide variety of manufacturers was 1.1.0.727 from 2013 for the QCA 7000 and 1.2.5.3207 from 2018 for the QCA 7005. However, the newest versions seen were 3.1.0.14 from 2021 and 3.0.0.18 from 2020 respectively, showing that new revisions are still being developed. In one instance, a charger manufactured in 2020 was using firmware from 2021, indicating either that it had a hardware replacement, or that the HPGP firmware can be updated.

Qualcomm does not provide much public information about these chips, or their firmware, since they are not intended directly for end users. As such, we do not have access to the change logs and cannot assess the risk of outdated firmware.

According to the Qualcomm Security Bulletin [45], there are no public vulnerabilities in the QCA 7000/7005. However, we were able to find entries for many different chips, including the QCA 7500 chip, a HomePlug AV2 (HPAV2) modem. Therefore, we believe it is likely for the QCA 7000 firmware to also contain vulnerabilities, including some that may have been discovered or patched. A culture of up-to-date firmware will help prevent issues when they are discovered.

Brokenwire is a known attack against HPGP, which wirelessly performs a highly efficient jamming and Denial of Service (DoS) against the wired communication [35]. While jamming is an unfixable issue, Brokenwire combines the fact that HPGP modems are extremely sensitive to a weak packet preamble, and that they use Carrier Sense Multiple Access with Collision Avoidance. This means that an attacker repeatedly transmitting a preamble at the same power as the noise floor will cause transmitters to stop transmitting entirely, causing the CCS charger to perform an emergency stop. This behavior should be controlled by firmware, making it possible

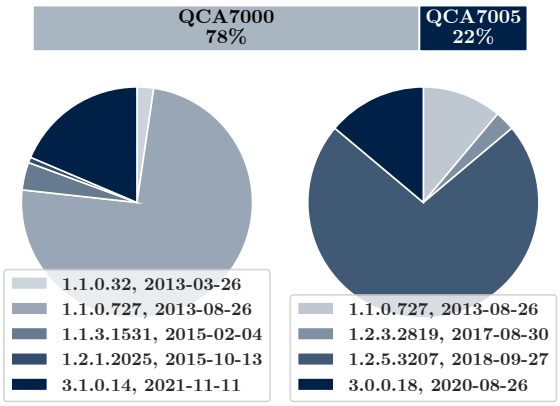

Figure 6: Firmware versions used by the QCA 7000 (left) and QCA 7005 (right) chips deployed in EV chargers.

for Brokenwire to largely be fixed by software. According to the ethics of our work, we did not test for the attack, however no charger used firmware released after the disclosure of the attack in 2022, so it must be currently unmitigated. Additionally, the outdated state of firmware indicates that even if a patch were released, it will not be widely deployed for a long time.

4.4 Encryption Keys

Answer to Q 1

Most chargers used random, ephemeral NMKs and standard compliant NIDs, with a few exceptions.

In line with the standard [30], we found that in most cases a new, random NMK is used for each vehicle connecting, and the NID is derived from the NMK using PBKDF1, as specified by [26]. Assuming the random seeming bytes are generated by a high quality random generator, these NMKs have 128 bits of entropy. This cannot be feasibly cracked, even using the information from the 54 bit NID.

Our analysis revealed 2 manufacturers where the NMK contained 12 ephemeral random bytes, as well as 4 fixed bytes, and the NID was still calculated using PBKDF1. We do not know why reducing the key space is practical, particularly when the random generator has already been implemented for the remaining bytes. This reduced 96 bit entropy could make cracking the key easier, but it is still sufficiently secure. As no salt is used, and the fixed bytes are shared between many chargers of the same model, hash tables may be practical to accelerate the attack.

Additionally, one manufacturer exhibited a very unique behavior, where many of their NMKs contained long sections of previous keys, often shifted by one byte. This behavior could allow attackers who captured a single NMK to determine subsequent ones in a greatly reduced search space.

Finally, we found one manufacturer who did not use PBKDF1 to derive the NID from the NMK. Instead, they generated 4 random bytes, which were then padded with a fixed pattern to get both the NID and NMK. Not only does this NMK only have 32 bits of entropy, it can trivially be derived from the NID.

In all cases, the NMK only protects against attackers who are not present at the start of the charging session. By design, the NMK is sent in clear text during the initial SLAC process and can be easily captured by wireless attackers [4].

5 Discussion

The charging communications carry safety critical information about the battery voltage and capabilities of the vehicle. However, an attacker with access to the communications could modify these values and cause the battery to over-charge. A well designed vehicle should perform an emergency disconnect when it detects this, but this requires a physical disconnection of contactors while under a very high current (up to 500 A is used in DC charging), which could easily damage them due to arcing. Previous work [14] has shown that MitM access to V2G communication is possible, and it is also known that wireless access is feasible [4]. Therefore, it is essential to secure CCS communication against tampering.

Without major changes to the standard, there are two avenues for protecting the communications. Firstly, the HPGP network could be protected by improving how the NMK is distributed, thereby securing all other parts of the protocol. No currently existing standard revision addresses this issue, but we highlight a potential avenue below. Secondly, the TCP link that carries the data could be upgraded to TLS. This method is not new, as optional TLS was introduced in 2014 by the ISO 15118-2 standard. Our results show a rising trend in support for 15118-2, but in 2024 it is still common to see newly deployed chargers that only support DIN 70121, and most devices do not support TLS at all.

Recommendation 1: *All chargers and vehicles should be upgraded to support at least ISO 15118-2 with TLS. Government regulation or subsidies can be used to encourage companies to update quickly. Once a sufficient threshold is reached, insecure communications should be deprecated.*

In addition to the clear security benefits, ISO 15118-2 and TLS also enable use cases beneficial to consumers:

PnC allows EVs to authenticate and pay autonomously, allowing owners to charge without interacting with an app or payment terminal. This user experience is so desirable that the Autocharge system [40] was developed to offer the same capabilities with simpler technology on the older standards. It continues to be used, despite significant known security issues that can allow attackers to easily impersonate victims

and steal electricity from them [4]. Some companies refuse to implement Autocharge because of these security issues [40].

PnC provides the same user experience with added security, but based on our observations it is not currently widely used. It will take additional work to implement the PnC protocol on the front and back ends, but this should be comparable to other payment solutions that are already in use. Open source reference implementations exist, and additionally the Open Charge Point Protocol (OCPP) describes a standardized and interoperable system for the necessary back-end communications. In addition, by design, PnC requires collaboration between EV manufacturers, charger operators, and payment providers. This also requires negotiations and business relations between the relevant companies.

Bidirectional and Scheduled Charging are important new features for the future of the power grid, as they allow vehicles to charge at times of high supply, or to feed energy back into the grid during peak demand. Such features can be particularly useful for owners of home photovoltaic installations, or large vehicle fleets, who can optimize their energy usage. In addition, a distributed network of EVs plugged in and acting as battery buffers are often considered to be an important element of a stable, renewable energy grid. Charging station manufacturers often make devices for small home and office installations, private fleets, and public DC fast charging. So, even if some of these features might not make sense in a fast charging environment, manufacturers have a clear incentive to implement them for their other customers. These drive the implementation of the underlying new standards, which can then be deployed on all their devices.

5.1 Implementation

With these benefits and motivation in mind, we consider the cost of implementing TLS and modern protocol versions. Implementation of new standards requires additional engineering work, since each version has incompatible data structures and binary encoding. However, the technologies involved are largely similar, allowing manufacturers to easily update. All hardware aspects, including basic signaling and HPGP are unchanged between CCS standard versions, ensuring that no hardware changes are necessary. Additionally, SLAC, and SDP are also identical. The difference is in the V2G messages, and their binary encoding. These are clearly documented in the standard, and multiple open source implementations can serve as reference [20, 55]. Further, in our experience, DIN and ISO 15118-2 are so similar that they can be implemented with essentially the same code, containing only minor differences. Consequently, adding ISO 15118-2 to a charger that already implements DIN is only a small fraction of the original effort needed to implement it.

To implement TLS, simple, free, and extensively tested libraries exist for all major programming languages. Modern micro-controllers should easily handle the additional calculations, and PnC also does not require new hardware. Despite this, for some car models [7], support for PnC depends on the date of manufacturing. We assume that this is because manufacturers are required to use Hardware Security Modules (HSMs) to store private keys [27, 36], which are not available in older hardware.

Recommendation 2: *All devices should start shipping with the necessary TLS hardware as soon as possible, even if the software deployment is delayed.*

5.2 Public Key Infrastructure

In addition to the simple implementation work, TLS requires a functioning Public Key Infrastructure (PKI) to provide roots of trust. The standard [29] does not define a central Certificate Authority (CA), but in the notes it describes a vision where each continent has no more than one dominant operator. This would allow all manufactured vehicles to ship with a list of trusted certificates, much like how browsers and operating systems come pre-installed with trusted root CAs for the web.

In our measurements, we conclude that the market has converged on a single dominant operator in Europe, as we have found that all PnC networks use the same Hubject root certificate. Additionally, we saw evidence of an Entrust root certificate meant for the US market in some of our tests. We only found this in the case where devices were shipped with a development TLS server enabled, as discussed earlier. The limited number of root certificates allows vehicles to easily include a comprehensive list from the factory, allowing them to validate chargers, regardless of PnC membership.

Based on their product page, Hubject currently charges a one time fee of €3900 per company, and a further subscription fee of €0.99 per charger per year for access to a PnC certificate [28]. We think that both of these fees are well within the budget of an EV charger company, and therefore should not discourage the implementation of TLS.

Based on the results of our study, we believe that TLS is being treated as a necessary condition to enable PnC, instead of as a security feature for power delivery messages. In our work, we did see chargers that deployed TLS without PnC, however as described in our results section, these appears to be development tests instead of real deployments.

5.3 TLS Design Issue

During our work analyzing the results of the study, we identified a previously unknown flaw with the current PKI system. This flaw could allow attackers with a single valid TLS certificate for any charger to attack all communications using the same root CA. To explain this issue, we highlight a key difference between TLS as it is used on web, and in CCS.

In both cases, a TLS certificate needs to be signed by a root CA that is trusted by a client. These roots come preinstalled in devices, or can be added by the user. A website or

charger owner can approach a CA, and request a certificate for their website or charger. The CA verifies the identity or ownership necessary for the request, and the EVSE ID or the website URL are encoded into the issued certificate. When a browser connects to a specific website `good.example`, but an attacker performs a MitM attack and uses their certificate for `evil.example`, this will be rejected by the browser.

Similarly, the charger certificates contain the EVSE ID, which is unique to each charger. However, the same check cannot be performed by the car, as it does not know which charger it is expecting to connect to.

Any charger certificate issued to any charger by any trusted root CA will be accepted in any location. There are many ways a certificate could be compromised, e.g., via extracting it from a charger in the wild, or by an attacker working in the supply chain. With this certificate, the attacker can MitM all TLS protected charging sessions globally for that CA, until their certificate expires or is revoked. To address this, the CAs must strictly evaluate any entity they issue certificates to, increasing the cost and difficulty of implementing TLS significantly.

We propose two avenues to increase the resistance of the PKI system against such an attack, greatly restricting the capabilities of an attacker with a stolen certificate.

Location Restriction A vehicle should be able to check if the certificate presented belongs to the charger it is connected to, using only information it can obtain from a trusted source. Therefore, we propose to add the GPS coordinates of the charger into the certificate, which could be done by using the Subject Locality attribute, which is not currently used. Since most vehicles nowadays contain GPS, they could easily verify that their location is close to the chargers claimed location. When issuing certificates, CAs could require proof that a charger is being installed at a specific location, and monitor for overlapping requests or an entity requesting suspiciously high numbers of new locations. With this method, the impact of a single attacker controlled certificate will be limited to a small area.

OCSP Stapling If a compromised certificate is discovered, it is essential to quickly revoke it. The most used solutions to this are the Online Certificate Status Protocol (OCSP), as well as Certificate Revocation Lists (CRLs) [9]. OCSP provides a method for a client to query the CA about the current validity of a certificate. If the certificate needs to be revoked, the CA can decline all further queries for validity. CRLs are lists published by CAs, listing all certificates they have issued, which have been revoked but not yet expired. Both of these methods require the vehicle to access the internet to contact the CA. While many modern vehicles contain mobile data connection, this may not always be available. Additionally, there are privacy concerns associated with OCSP, as it could allow the CA to track clients. OCSP Stapling [51] addresses both these issues.

In OCSP stapling, the TLS server sends the results of a recent OCSP query to the client, along with their certificate. The ISO 15118-2 standard requires all chargers to provide OCSP responses in their TLS handshake for Sub-CA certificates in the chain, but not the leaf [29][V2G2-070, Note 1]. Vehicles are also not required to verify the leaf by other means.

In our measurements, the chargers did not provide an OCSP value for the leaf. As the attacker is most likely to compromise the leaf certificate, we believe this this is an important safety feature, which can be introduced retroactively.

Recommendation 3: *Chargers should add OCSP responses for the leaf certificate, and vehicles should validate the leaf.*

5.4 Secure SLAC

Finally, we discuss a method to protect the communication at a layer below TLS. While TLS provides confidentiality and authentication of the V2G data, an attacker who is able to access the HPGP network is presented with a large attack surface, including the HPGP modems, Ethernet interface of the car and charger, SDP process, or TLS implementation flaws. A simple solution to all of these issues is to prevent third parties from interacting with the network, thereby adding an additional layer of defense. HPGP provides full protection of the network from anyone who does not have access to the NMK. However, in the SLAC process currently used, the NMK is distributed in clear text visible to any attacker. The HPGP standard defines the Secure SLAC process [26], where the SLAC process (and key exchange) are cryptographically protected by PKI based cryptography. However, all versions of CCS explicitly specify using only insecure SLAC. To our knowledge, no implementation of secure SLAC exists, nor has it been studied by researchers. The secure SLAC key exchange process encrypts and authenticates the NMK using public key cryptography, therefore our previous discussion of PKI applies to this protocol as well. Future versions of the standard should modify the SLAC process to protect the NMK, such as by implementing a combination of Secure SLAC, and the Diffie-Hellman protocol proposed in [4].

5.5 Future Outlook

At the time of our study, there were approximately 147,208 DC chargers across Europe [19] (data from September 2024). This number is rapidly increasing, and their deployment seems to be accelerating. Therefore, it is essential that newly deployed devices come equipped with all the necessary hardware and potentially software directly from the factory, in order to avoid costly in-field upgrades.

In addition to this, a paradigm shift in AC charging will soon majorly boost the deployment of CCS. Currently, most

AC chargers are very simple devices, acting as an electricity meter and switch between the electrical supply and the charging cable. For safety reasons, basic signaling is used for presence detection of the vehicle before powering the cable. However, the CCS standard defines using the same sophisticated communication scheme for AC charging in addition to DC. This allows users to schedule charging based on varying electricity prices, and use PnC.

As of our data from September 2024, 84% of all chargers in Europe are AC [19], and we believe that most of these do not yet use CCS. As ISO 15118 capable AC chargers are adopted, they will rapidly outnumber CCS DC chargers. The security implications of AC charging communication attacks must be studied further, but attackers could increase the current drawn by vehicles, potentially damaging the cable or tripping fuses. Additionally, they could tamper with scheduled charging, denying service or inflating electricity costs.

Our work focused on chargers, however we also briefly investigated the protocol deployment in EVs. Based on an online dataset of EV capabilities discussed in Appendix A, newer and premium vehicles are the first to adopt TLS support and most vehicles that have been sold do not support TLS. In some cases, even within the same model only newer vehicles support PnC, while older ones do not [7]. In order to phase out non-TLS protected charging sessions, both vehicles and chargers will need to support the feature.

6 Limitations and Extrapolation

We acknowledge that our survey provides only a snapshot of the current state of EV charging infrastructure deployment across Europe. Our study included countries with mature and developing EV networks, as well as diverse locations such as dense urban cores, rural deployments, and large highway infrastructure projects. Because of this, we believe that our key findings are representative of the state of EV charging in Europe, as of early September 2024. This assertion is further supported by the widespread presence of many network operators in different countries, and their use of the same charging station manufacturers.

We observed that the chargers deployed by a given network and manufactured by a specific company exhibited consistent behavior regardless of location. Therefore, based only on information about the network and manufacturer of each charger, we can make predictions about their behavior. Motivated by this observation, and the existence of large international networks, we are able to extrapolate our existing measurements, and identify the portion of the market not covered by our experiments. We used Zap-Map [15], a large database of EV chargers across Europe. As a UK based company, they provide detailed information about the UK, so we chose to extrapolate our findings to this country. From this data source, we obtained information about the size of various charging networks.

To estimate the usage of various manufacturers by a given network, we used public photos of a random subset of their chargers and identified the device based on distinctive visual features. For some networks, it was even possible to identify the exact model of the charging stations based on the unique id, which in addition to the manufacturer included the exact model.

6.1 TLS Support

Using this collected data, we counted the TLS supporting networks we identified. In total, we found that 3.1 % of the chargers are from networks and manufacturers where we expect TLS support. Similarly, we estimate that 74.5 % of chargers are from networks that do not support TLS. The remaining devices are from a combination of many networks which did not appear in our dataset. Based on our observation that TLS is deployed either by networks with Plug and Charge, or by devices from a manufacturer who ships a TLS server with development certificates, we assume that the remaining chargers are unlikely to support TLS.

7 Related Work

Survey studies are commonly done in many different areas, to allow future researchers and the public to understand the state of affairs. In the security context, non-malicious internet scans are regularly performed by researchers [50, 59] and cyber security companies [53, 54] to understand the status of public facing infrastructure, or to analyze long term trends. In particular, the configuration of TLS servers on the internet has been measured over multiple years to analyze trends [34]. In the EV context, researchers have scanned for web interfaces of chargers intended for home use [42], as well as for endpoints of the Open Charge Point Protocol (OCPP) [52]. In both cases, they identified a large number of public devices, and discovered new vulnerabilities in them. Non-security related EV charging studies have also been conducted. In [8], the authors present a review of EV charging in the UK, with a focus on geographic distribution, power usage, and the planning process. In addition, multiple studies offer a comprehensive overview of EV charging, discussing non-CCS technologies, capabilities of EVs, legislation and market trends [6, 37]. To our knowledge, this paper is the first project performing a study of chargers via the CCS interface, instead of via the network, complementing the existing work.

7.1 Implementations

Similar to our EV emulator, various open source projects [20, 25, 55, 56] implement the communication stack of CCS, including power delivery messages. Some of them feature implementations of Plug and Charge, and act as valuable research tools for those wishing to study this protocol in action.

7.2 Attacks

Due to its importance, many papers examine the security of CCS and EV charging in general. Overview papers such as [5] enumerate the possible motivations and entry points for attackers.

Researchers have demonstrated the extraction of the NMK from the SLAC [14], even wirelessly [4]. Dudek et al. [14] further demonstrated that they can join the network and inject packets into the communication. A TLS based session secures against passive eavesdroppers and should even remain secure against most forms of active MitM attacker, as long as they do not possess a trusted certificate belonging to a charger. As we discussed, a single compromised certificate could enable TLS attacks globally, however it is still increases the bar for attackers, and therefore TLS should be enabled. Physical layer wireless jamming such as [35] could potentially be counteracted at the HPGP firmware level.

The EVExchange [10] attack has been proposed to allow an attacker to charge their vehicle while the victim pays. The authors claim that their attack can operate fully without modifying packets, leaving even TLS connections vulnerable. We argue that unlike the testbed evaluation conducted in the paper, additional real-world challenges would complicate the attack without MitM access to the communication. A state transition in basic signaling is synchronized with a transition of the protocol state machine, and measurements of the current should be compared to the reported values. If messages are passively forwarded as the paper describes, a competent implementation should notice and trigger an emergency stop. Therefore, enabling TLS would defend against the attack in the real world.

7.3 Protocol Improvements

Forward looking researchers are proposing improvements to ISO 15118 standards and the PKI system, such as enabling multiple users to share a PnC enabled vehicle [44]. Others have discussed using HSMs to store and generate the PnC credentials [23, 24]. Proposals have also been made to replace PKI [31] with Self-Sovereign Identities, and to transition to quantum safe cryptography [32].

8 Conclusion

In this paper, we conducted the first and largest real-world measurement study of the EV charging infrastructure, measuring 325 unique charging stations. According to our results, the majority of the current charging infrastructure (88% of tested devices) does not implement TLS and modern parts of the ISO 15118 standard. While support for the decade-old ISO 15118-2 is slowly rising in new installations, there is no known public deployment of the latest and most secure ISO 15118-20 standard. We presented results about other implementation details of CCS, and identified vulnerable behavior in the NMK selection of some devices, which lowers the bar for attackers trying to join the HPGP network. Based on our study, we recommend swiftly deploying TLS, and making a plan to deprecate insecure connections.

In the discussion, the paper presented an overview of the security benefits of TLS, as well as the implementation costs. Our analysis of the TLS ecosystem compared to the use of PKI on the web highlighted an important and previously unidentified design flaw. To combat this, we proposed three countermeasures, designed with backwards compatibility and privacy in mind, to detect and limit the impact of a single compromised certificate. Finally, we discussed the need for improvements to the SLAC process.

Acknowledgments

We would like to thank armasuisse Science + Technology for their support. Marcell was funded by the Engineering and Physical Sciences Research Council (EPSRC) and Sebastian was supported by the Royal Academy of Engineering and the Office of the Chief Science Adviser for National Security under the UK Intelligence Community Postdoctoral Research Fellowships programme.

Ethics Considerations

For both practical and ethical reasons, we modeled our research after commonly conducted Internet-wide scans. As such, our experiments perform non-malicious CCS charging sessions and collect data in the process. All tested chargers were installed for public use and are part of critical infrastructure, so we did not want to risk damaging them, or compromising any user data. We analyze the ethics of our work from the below angles:

Data Privacy: All of our data was collected using our EV emulator and public chargers. We did not collect data on the charging sessions of real users charging their car, and there was no foreseeable way in which data from a previous charging session could be leaked to us. Since the tested devices were provided and owned by companies, none of the information we collected about them could be classified as personal information.

Infrastructure Damage: Our experiments mostly followed standard-compliant behavior, but deviated in minor non-malicious ways, such as by attempting a connection with a TLS 1.1 client instead of the required 1.2. Therefore, any CCS implementation should handle our experiments gracefully and we are confident that we caused no damage to tested devices.

Public Safety: We believe that documenting the current state of security in EV charging is important and necessary.

Our results will inform researchers, companies and legislators, allowing them to push for changes in the industry that will benefit everyone. In cases where implementations used older, less secure versions of CCS, we treated this as a design choice by manufacturers, which does not require disclosure. However, in cases where we discovered actual flaws in the implementation, we disclosed them to the affected parties.

Data Availability: In the paper, we discuss the statistics seen in our dataset, and the companies that implemented TLS. The dataset is made publicly available consisting of a list of each specific charger we tested, including location, serial numbers, time of test, and key findings. During our evaluation we found certain issues and potential vulnerabilities which are discussed anonymously. Our raw data files contain information about these, as well as more sensitive data such as TLS certificates. Therefore, this detailed data is only made available upon request.

Open Science Policy

The code and hardware instructions for the measurement system, basic signaling PCB design files, the dataset, and the data analysis code are available on Zenodo [57] at https://zenodo.org/records/14712107. The dataset includes information about all tested chargers, including location, manufacturer and test results. Additionally, the measurement code is also available at https://github.com/ssloxford/current-affairs to support ongoing development. Our C Python module extension to `open-plc-utils` is included in the Zenodo archive, as well as at https://github.com/ssloxford/open-plc-utils.

References

[1] 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.

[2] Nnamdi Anyadike. Around the world of mining vehicle electrification. https://www.mining-technology.com/features/mining-vehicle-electrification/?cf-view, 08 2023. Accessed 2023-11-05.

[3] Richard Baker and Ivan Martinovic. EMpower: detecting malicious power line networks from EM emissions. In *ICT Systems Security and Privacy Protection: 33rd IFIP TC 11 International Conference, SEC 2018, Held at the 24th IFIP World Computer Congress, WCC 2018, Poznan, Poland, September 18-20, 2018, Proceedings 33*, pages 108–121. Springer, 2018.

[4] Richard Baker and Ivan Martinovic. Losing the car keys: Wireless PHY-Layer insecurity in EV charging. In *28th USENIX Security Symposium (USENIX Security 19)*, pages 407–424, Santa Clara, CA, August 2019. USENIX Association.

[5] Kaibin Bao, Manuela Wagner, Hristo Valev, and Hartmut Schmeck. A threat analysis of the vehicle-to-grid charging protocol ISO 15118. *Computer Science - Research and Development*, 09 2017.

[6] Amel Benmouna, Laurence Borderiou, and Mohamed Becherif. Charging stations for large-scale deployment of electric vehicles. *Batteries*, 10(1), 2024.

[7] BMW USA. Plug and charge eligibility. https://www.bmwusa.com/modals/plug-and-charge.html.

[8] Tianjin Chen, Xiao-Ping Zhang, Jianji Wang, Jianing Li, Cong Wu, Mingzhu Hu, and Huiping Bian. A review on electric vehicle charging infrastructure development in the uk. *Journal of Modern Power Systems and Clean Energy*, 8(2):193–205, 2020.

[9] Taejoong Chung, Jay Lok, Balakrishnan Chandrasekaran, David Choffnes, Dave Levin, Bruce M. Maggs, Alan Mislove, John Rula, Nick Sullivan, and Christo Wilson. Is the web ready for OCSP must-staple? IMC '18, page 105–118, New York, NY, USA, 2018. Association for Computing Machinery.

[10] Mauro Conti, Denis Donadel, Radha Poovendran, and Federico Turrin. EVExchange: A relay attack on electric vehicle charging system. In Vijayalakshmi Atluri, Roberto Di Pietro, Christian D. Jensen, and Weizhi Meng, editors, *Computer Security – ESORICS 2022*, pages 488–508, Cham, 2022. Springer International Publishing.

[11] Gökçen Yılmaz Dayanıklı, Sourav Sinha, Devaprakash Muniraj, Ryan M. Gerdes, Mazen Farhood, and Mani Mina. Physical-layer attacks against pulse width modulation-controlled actuators. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 953–970, Boston, MA, August 2022. USENIX Association.

[12] Firefox Source Tree Documentation. NSS key log format. https://nss-crypto.org/reference/security/nss/legacy/key_log_format/index.html. Accessed 2024-09-04.

[13] Sébastien Dudek and contributors. V2Gdecoder. https://github.com/FlUxIuS/V2Gdecoder, 2022.

[14] Sébastien Dudek, Jean-Christophe Delaunay, and Vincent 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.

[15] Jade Edwards. EV charging statistics 2024. https://www.zap-map.com/ev-stats/how-many-charging-points, 2024. Accessed 2024-09-04.

[16] electrek. President Biden will make entire 645k federal vehicle fleet electric. https://electrek.co/2021/01/25/president-biden-will-make-entire-645k-vehicle-federal-fleet-electric/, 01 2021.

[17] Electric vehicle database. https://ev-database.org/.

[18] European Commission. Directive 2014/94/EU of the european parliament and of the council. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014L0094&from=en, 10 2014.

[19] European Commission. Alternative Fuels Observatory. https://alternative-fuels-observatory.ec.europa.eu/transport-mode/road/eu27-uk-norway-iceland-switzerland-turkey-liechtenstein, 2024. Accessed 2024-09-04.

[20] EVerest developers. EVerest. https://github.com/EVerest/everest-core.

[21] Federal Highway Administration. 88 FR 12724, national electric vehicle infrastructure standards and requirements. https://www.federalregister.gov/d/2023-03500, 2023.

[22] Steffen Fries and Rainer Falk. Electric vehicle charging infrastructure – security considerations and approaches. In *Proceedings of The Fourth International Conference on Evolving Internet*, ARES '23, 06 2012.

[23] Andreas Fuchs, Dustin Kern, Christoph Krauß, and Maria Zhdanova. HIP: HSM-based identities for plug-and-charge. In *Proceedings of the 15th International Conference on Availability, Reliability and Security*, ARES '20, New York, NY, USA, 2020. Association for Computing Machinery.

[24] Andreas Fuchs, Dustin Kern, Christoph Krauß, and Maria Zhdanova. TrustEV: trustworthy electric vehicle charging and billing. In *Proceedings of the 35th Annual ACM Symposium on Applied Computing*, SAC '20, page 1706–1715, New York, NY, USA, 2020. Association for Computing Machinery.

[25] Uwe Hennig, Johannes Huebner, Arend Jan Kramer, and Jorrit Pouw. pyPLC. https://github.com/uhi22/pyPLC, 2024.

[26] HomePlug Powerline Alliance. HomePlug Green PHY specification, release version 1.1.1. Standard, 2013.

[27] Hubject. Plug & Charge multi-contract handling. https://cdn.prod.website-files.com/602cf2b08109ccbc93d7f9ed/61951da439c57d1d75e28b9c_Plug%26Charge_VW_Multicontract.pdf. Accessed 2024-09-04.

[28] Hubject. Plug & Charge pricing. https://www.hubject.com/pricing. Accessed 2024-12-27.

[29] ISO 15118-2. vehicle to grid communication interface. part 2: Network and application protocol requirements. Technical report, 2014.

[30] ISO 15118-3. vehicle to grid communication interface. part 3: Physical and data link layer requirements. Technical report, 2015.

[31] Adrian Kailus, Dustin Kern, and Christoph Krauß. *Self-sovereign Identity for Electric Vehicle Charging*, page 137–162. Springer Nature Switzerland, 2024.

[32] Dustin Kern, Christoph Krauß, Timm Lauser, Nouri Alnahawi, Alexander Wiesmaier, and Ruben Niederhagen. QuantumCharge: Post-quantum cryptography for electric vehicle charging. Cryptology ePrint Archive, Paper 2023/430, 2023.

[33] Bertel King. What Is CCS? The Most Common Standard for Fast-Charging EVs. https://www.makeuseof.com/what-is-ccs/, 07 2023. Accessed 2025-01-04.

[34] Platon Kotzias, Abbas Razaghpanah, Johanna Amann, Kenneth G. Paterson, Narseo Vallina-Rodriguez, and Juan Caballero. Coming of age: A longitudinal study of TLS deployment. In *Proceedings of the Internet Measurement Conference 2018*, IMC '18, page 415–428, New York, NY, USA, 2018. Association for Computing Machinery.

[35] Sebastian Köhler, Richard Baker, Martin Strohmeier, and Ivan Martinovic. Brokenwire : Wireless disruption of CCS electric vehicle charging. In *NDSS Symposium*, 2023.

[36] Spandan Mahadevegowda. Secure communication networks for connected vehicles. Master's thesis, Virginia Tech, 12 2022.

[37] Muhammad Shahid Mastoi, Shenxian Zhuang, Hafiz Mudassir Munir, Malik Haris, Mannan Hassan, Muhammad Usman, Syed Sabir Hussain Bukhari, and Jong-Suk Ro. An in-depth analysis of electric vehicle charging station infrastructure, policy implications, and future trends. *Energy Reports*, 8:11504–11529, 2022.

[38] Arriana McLymore. Amazon says it has 10,000 rivian electric vans in its delivery fleet. https://www.reut

ers.com/business/autos-transportation/amazon-says-it-has-10000-rivian-electric-vans-its-delivery-fleet-2023-10-18/, 08 2023.

[39] Max Molliere. Battery-electric is now the most popular for new city buses in the EU. https://www.transportenvironment.org/articles/battery-electric-is-now-the-top-powertrain-type-for-new-city-buses-in-the-eu, 07 2024. Accessed 2024-09-01.

[40] Marc Mültin. Autocharge: What it is – and why it's a bad idea. https://www.switch-ev.com/blog/autocharge-what-it-is---and-why-its-a-bad-idea. Accessed 2024-07-08.

[41] Marc Mültin. The new features and timeline for ISO 15118-20. https://www.switch-ev.com/blog/new-features-and-timeline-for-iso15118-20. Accessed 2024-07-19.

[42] Tony Nasr, Sadegh Torabi, Elias Bou-Harb, Claude Fachkha, and Chadi Assi. ChargePrint: A framework for internet-scale discovery and security analysis of EV charging management systems. In *NDSS*, 2023.

[43] NHS England. NHS rolls out new electric vehicles to help patients and the planet. https://www.england.nhs.uk/2022/08/nhs-rolls-out-new-electric-vehicles-to-help-patients-and-the-planet/, 08 2022.

[44] Christian Plappert, Lukas Jäger, Alexander Irrgang, and Chandrasekhar Potluri. Secure multi-user contract certificate management for ISO 15118-20 using hardware identities. In *Proceedings of the 18th International Conference on Availability, Reliability and Security*, ARES '23, New York, NY, USA, 2023. Association for Computing Machinery.

[45] Qualcomm. Security bulletins | qualcomm documentation. https://docs.qualcomm.com/product/publicresources/securitybulletin.

[46] Qualcomm Atheros. Open Plc utils. https://github.com/qca/open-plc-utils.

[47] Chris Randall. World's largest electric ferry launches in Norway. https://www.electrive.com/2021/03/02/worlds-largest-electric-ferry-yet-goes-into-service-in-norway/, 03 2021. Accessed 2023-11-05.

[48] Eric Rescorla, Marsh Ray, Steve Dispensa, and Nasko Oskov. RFC 5746 - Transport Layer Security (TLS) renegotiation indication extension. 2010.

[49] Jesse Norman Richard Holden. Government invests £200 million to drive innovation and get more zero emission trucks on our roads. 10 2023.

[50] Suood Al Roomi and Frank Li. A large-scale measurement of website login policies. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 2061–2078, Anaheim, CA, August 2023. USENIX Association.

[51] Stefan Santesson, Michael Myers, Rich Ankney, Ambrish Malpani, Slava Galperin, and Carlisle Adams. RFC 6960 - X.509 internet public key infrastructure online certificate status protocol - OCSP. 2013.

[52] Khaled Sarieddine, Mohammad Ali Sayed, Sadegh Torabi, Ribal Attallah, Danial Jafarigiv, Chadi Assi, and Mourad Debbabi. Uncovering covert attacks on EV charging infrastructure: How OCPP backend vulnerabilities could compromise your system. In *Proceedings of the 19th ACM Asia Conference on Computer and Communications Security*, ASIA CCS '24, page 977–989, New York, NY, USA, 2024. Association for Computing Machinery.

[53] Shadowserver. Shadowserver dashboard. https://dashboard.shadowserver.org/.

[54] Shodan. https://www.shodan.io/.

[55] SwitchEV. ISO15118. https://github.com/SwitchEV/iso15118.

[56] SwitchEV. RISE-V2G. https://github.com/SwitchEV/RISE-V2G.

[57] Marcell Szakály, Sebastian Köhler, and Ivan Martinovic. Artifacts for "Current Affairs: A security measurement study of CCS EV charging deployments". https://doi.org/10.5281/zenodo.14712107, January 2025.

[58] North american charging standard. Standard, Coordination Office Charging Interface, c/o Carmeq GmbH, 2022.

[59] Chuhan Wang, Kaiwen Shen, Minglei Guo, Yuxuan Zhao, Mingming Zhang, Jianjun Chen, Baojun Liu, Xiaofeng Zheng, Haixin Duan, Yanzhong Lin, and Qingfeng Pan. A large-scale and longitudinal measurement study of DKIM deployment. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 1185–1201, Boston, MA, August 2022. USENIX Association.

[60] Wireshark Wiki. TLS. https://wiki.wireshark.org/TLS.

[61] Nick Sullivan Yoav Nir, Rich Salz. Transport layer security (TLS) parameters. https://www.iana.org

/assignments/tls-parameters/tls-parameters.txt.

[62] Maria Zhdanova, Julian Urbansky, Anne Hagemeier, Daniel Zelle, Isabelle Herrmann, and Dorian Höffner. Local power grids at risk – an experimental and simulation-based analysis of attacks on vehicle-to-grid communication. In *Proceedings of the 38th Annual Computer Security Applications Conference*, ACSAC '22, page 42–55, New York, NY, USA, 2022. Association for Computing Machinery.

[63] Ce Zhou, Qiben Yan, Zhiyuan Yu, Eshan Dixit, Ning Zhang, Huacheng Zeng, and Alireza Safdari Ghanhdari. ChargeX: Exploring state switching attack on electric vehicle charging systems. https://arxiv.org/abs/2305.08037, 2023.

A EV Survey

The security of a real-world charging session will be determined jointly by the car and chargers capabilities. As such, it is also important to understand the protocol support in current vehicles. Gaining access to vehicles for testing is significantly more challenging than gaining access to chargers. Therefore, to understand the current state of the market we utilized an online survey of public information.

Car manufacturers often publish information about their vehicles, particularly support for ISO 15118-2 Plug and Charge, and ISO 15115-20. Public databases such as [17] exist to easily look up this information, and we present our findings in the results section.

However, this online survey leaves important questions unanswered. Vehicles which do not advertise support for PnC could still implement it, or they could implement a much simpler ISO 15118-2 TLS client without PnC. This implementation requires only a list of trusted root certificates, and enabling TLS has clear security benefits. We study this possibility by additional experiments on real cars, using a charger emulator we developed.

Support for TLS is only possible if it is implemented by both sides of the communication. Therefore, it is important to understand the state of deployment in EVs. Additionally, unlike chargers, not all EVs are constantly connected to a back-end system, which can make software updates harder to deploy.

Based on data from [17], we found that about half of newly announced cars support Plug&Charge (PnC) using ISO 15118-2, but only 4 out of 146 EV models scheduled for release in 2024 support ISO 15118-20 PnC. We plot this trend in Figure 7. It is important to note that these results are not weighted for the sales of each model, the breakdown considers the year a vehicle was first released, and that these features are introduced first into premium vehicles. Due to these factors, real world adoption of these new standards comes from new or premium vehicles, significantly reducing their current real world market share compared to our data.

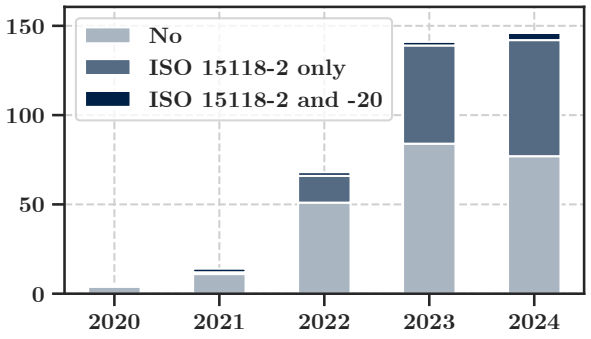

Figure 7: Number of EV models supporting Plug and Charge, by year of first availability. Data from [17]. 2024 data includes upcoming announced EVs.

B Additional Observations

In this section, we present results that do not have clear security implications, but are interesting and may be useful for future researchers and implementers to better understand the details of real-world CCS deployments.

B.1 MAC Addresses

We collected the MAC addresses of the chargers, and analyzed their Organizationally Unique Identifier (OUI) to gain insights into the manufacturers of the embedded systems. In most systems, MAC addresses can be overwritten by the software or firmware, so our results are merely indicative. Table 3 shows the statistics for the observed OUI fields.

Our results can be classified into three different behaviors between devices. Some devices were set to a MAC address belonging to an EV charger specific manufacturer, some devices were set to a MAC corresponding to a large generic electronics supplier, and some had special addresses. Most special addresses had the locally administered bit set, meaning that the address does not need to be unique. We re-tested some of these chargers a few days apart, and found that they had changed addresses. For one charger, we also observed it using an address from an IANA region, used for special purpose addresses.

We also noticed that the manufacturer using the NXP Semiconductors OUI set the same, human chosen pattern for the remaining bytes of the address.

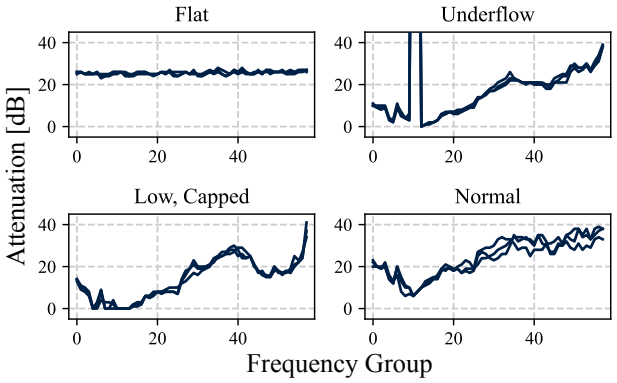

Figure 8: Plot of various attenuation profiles received.

Table 3: HLE MAC Addresses of the charger, grouped by the Organizationally Unique Identifier region. We further indicate generic electronics manufacturers, charger manufacturers, and ranges with special purposes.

OUI	Devices	Type
Atheros Communications	1	Generic
congatec GmbH	2	Generic
EcoG	6	Charger
GloQuad	2	Charger
Huawei Technologies Co.,Ltd	1	Generic
I2SE GmbH	34	Generic
ICANN, IANA Department	1	Special
Kempower Oyj	10	Charger
KSE GmbH	4	Generic
Locally Administered	108	Special
Microchip Technology Inc.	138	Generic
NXP Semiconductors	7	Generic
Tesla,Inc.	48	Charger
Tritium Pty Ltd	20	Charger
Unknown	4	Special
Wall Box Chargers, S.L.	1	Charger

B.2 IP Addresses

We collected the IPv6 address given by the charger during the SDP process. As per the standard [29][V2G2-051], link local IPv6 addresses should be used, and all devices should generate it from their MAC address following RFC 4291. We validate that most devices follow this method, however some devices chose different seemingly random link local addresses. Because of the SDP process, no specification compliant vehicle should require the IP address to be generated in this way, so we do not expect this to be an issue. Being able to predict the IP address could be an important step in certain MitM spoofing attacks.

B.3 Server Ports

The V2G communication happens using a TCP socket. The server port is chosen by the charger, and send to the vehicle in the SDP response. We analyzed the choice of server port, as it reveals information about the internal implementation.

Based on our observations, we were able to classify devices into three categories based on server port selection. We found devices with ephemeral random, ephemeral incrementing, and constant ports. By comparing the constants between identical charger models, we can further divide constant ports which appear to be hard coded, and ports which appear to be chosen randomly at system startup.

While there is no clear security implication of this choice based on known attacks, a predictable server port could assist with potential MitM and spoofing attacks.

B.4 Attenuation

During the SLAC process, the charger measures the signal strength of the HPGP packets from the vehicle, and sends this information to it. Due to the RF nature of the HPGP protocol, this information is provided as a function of frequency.

We observed that all devices returned different attenuation profiles on subsequent measurements, indicating that they do not have a hard coded value, and instead perform a real measurement. However, we observed three anomalies, and we plot the corresponding signals in Figure 8.

First, we observed the shape of the attenuation profile. Most chargers respond with a similar shape, showing higher attenuation at low frequencies due to the high-pass filter separating the PLC signal from the basic signaling PWM signal, as well as higher attenuation at high frequencies due to various losses. The difference between min and max attenuation is often in the range of 10 – 40 dB. However, one charging manufacturer responds with a very flat profile, within ± 1 dB of the average. Given that the measurements still contain noise, which varies for each subsequent run, we argue that these are also based on real measurements, but they are likely calculated after some form of channel equalization.

Secondly, different charger models have different attenuation levels. This could be an issue when two such chargers are installed in close proximity, since a vehicle might accidentally connect to the wirelessly coupled, low attenuation charger as opposed to the wired high attenuation one. Discrepancies may be due to variations in PLC chips, internal attenuation or charging cables. In our findings, we see differences of about 10 dB to be common.

Finally, we occasionally observed an underflow in the data. As per the specification, the attenuation for each frequency is an unsigned byte, however one charger manufacturer would regularly underflow, and send very high (255 dB) attenuation. It is possible that an implementation averages all the unsigned bytes to determine the total attenuation. Having a few of these very high values in the average can easily cause the vehicle

to calculate a higher average attenuation for the charger it is directly connected to, then for a charger that it is not connected to, and which therefore does not underflow.

We believe that charging station manufacturers should work to calibrate their signal strength measurements to provide consistent, and real results. The calibration should be done end-to-end, to compensate for the cable, analog front end and PLC chip. Furthermore, steps should be taken to avoid underflows when reporting the result, as we saw some manufacturers correctly cap their measurements at 0.

From a security perspective, inconsistent measurements during the SLAC process can open the door for a wireless attacker to interfere with the process, and hijack the session.