Comput Sci Res Dev (2018) 33:3–12
https://doi.org/10.1007/s00450-017-0342-y

energieinformatik2017
The Swiss-German-Austrian Research Summit on Energy Informatics

SPECIAL ISSUE PAPER

A threat analysis of the vehicle-to-grid charging protocol ISO 15118

Kaibin Bao[1] · **Hristo Valev**[1] · **Manuela Wagner**[1] · **Hartmut Schmeck**[1]

Published online: 1 September 2017

Abstract This work performs a security analysis of the vehicle-to-grid charging protocol ISO 15118 and presents various scenarios of how to compromise the availability of the charging service or the integrity, authenticity, or confidentiality of the communication on a protocol level. Furthermore, it analyzes processes related to the authentication, transfer of information, and the certification hierarchy for vulnerabilities, which could be used by an adversary to gain unfair advantage over the charging process and use it for his own self-interest, mostly harming legitimate users or other participants.

Keywords Electric vehicle · ISO 15118 · Vehicle-to-grid · Charging protocol · Thread analysis

1 Introduction

With the increasing popularity of electric vehicles, challenges of the charging process like capacity limitations of the electric distribution network or generation limitations of energy need to be addressed by coordination mechanisms throughout the charging process. At the end-user side of such a coordination mechanism, the standard ISO 15118 [1–3] specifies the communication protocol between an electric vehicle and its charging station. In addition to the coordination of the charging process, the standard addresses aspects of billing, authentication, provisioning of authentication, and *Value Added Services* that can be provided by connecting the electric vehicle to the Internet over the charging station.

The security considerations of ISO 15118 are mostly bounded by the scope of the communication protocol between electric vehicles and charging stations. That is why in this paper we carry out an adversary-centric threat analysis of the ISO 15118 protocol and expose implicit assumptions which need to be fulfilled by the deployment context of a charging point infrastructure to guarantee security, especially focusing on the scope boundaries. This threat analysis is based on the published parts 1, 2 and 3 of ISO/IEC 15118:2015.

This paper is structured in the following way: First, in Sect. 2, we present related work. In Sect. 3, we provide an overview of the system and the background information on the charging processes as well as stakeholders involved in a successful charging scenario and applicable data protection law. In Sect. 4, we define adversaries, their capabilities and motivation as well as assets which can be the target of these adversaries. In Sect. 5, we identify threats and analyze whether these threats can be exploited. Whenever we conclude that the mitigation of a threat requires assumptions which are not well documented in the published standard, we point out these implicit assumptions in Sect. 6. Furthermore, some flaws are identified in Sect. 7, which can be regarded as potential vulnerabilities that may be utilized by the adversaries. In Sect. 8, we describe how some flaws and assumptions can be avoided. Lastly, we summarize our findings and conclude in Sect. 9.

This work is partially supported by the project *Inductive and InteroperabLe charging Systems for Electric vehicles (IILSE)* (No. 01MX15004), part of the funding program *ELEKTRO POWER II: Electric Mobility Positioning Along the Value Chain* by the *German Federal Ministry for Economic Affairs and Energy* (BMWi) and by the project *Security for interconnected infrastructures* (No. 16KIS0521) within the KASTEL competence center of the *German Federal Ministry of Education and Research* (BMBF).

✉ Kaibin Bao
bao@kit.edu

[1] Karlsruhe Institute of Technology, Kaiserstrasse 12, 76131 Karlsruhe, Germany

2 Related work

Threat analyses of the ISO 15118 standard have been carried out by Falk and Fries [11,12] and Lee at al. [16]. In contrast to these works, we incorporate the first published revision of the ISO 15118 parts 1, 2 and 3 into our threat analysis. Also, the exploitability, which considers the security requirements in detail, has not been discussed in previous threat analyses before. Höfer et al. [14] carried out a privacy impact assessment of ISO 15118 and propose the protocol extension POPCORN to enhance the privacy of the charging protocol, focusing on privacy enhancement and data protection. Compared to this work, we focus on possibilities of fraud rather than privacy issues. Although Mültin [17] describes some security considerations concerning the protocol, his work did not conduct a thread analysis.

3 System overview

An electric vehicle is a motor vehicle propelled by electricity, allowed to make use of the public electrical grid infrastructure for charging and discharging purposes. The charging point is the equivalent of a gas station.

The ISO 15118 standard specifies a communication protocol between an electric vehicle and the charging station for the purpose of transferring energy (see Fig. 1). The entities involved in the process are the *Electric Vehicle* (EV) and the charging station called *Electric Vehicle Supply Equipment* (EVSE). Each entity has their component responsible for the communication, the *Communication Controllers* (EVCC and SECC).

Further roles involved in the charging process are the *Original Equipment Manufacturer* (OEM) who has produced the EV, the *Charging Point Operator* (CPO) who operates the charging stations, and the *Mobility Operator* (MO) who is a intermediary between EV user and charging point operators.

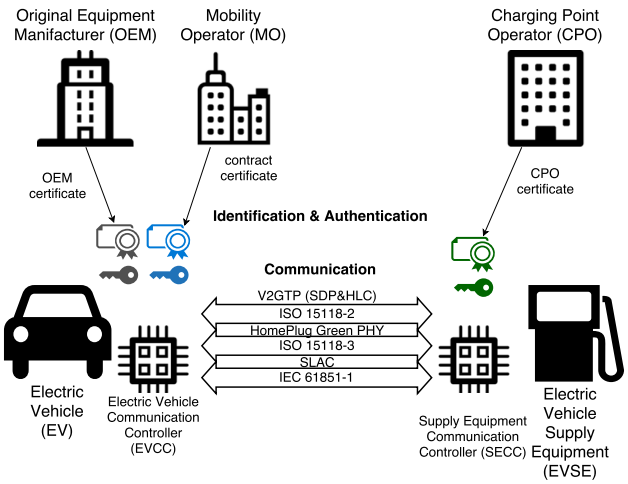

Fig. 1 System overview of the ISO 15118 protocol

3.1 Environments

To differentiate between deployment scenarios, the ISO 15118 standard defines environments, which will dictate the behavior and the required and optional functionality of EV and EVSE [2, Sect. 3]:

In *Public Environments*, physical accessibility to the EVSE is not bound to a specific group of EVs. Regarded as the most unprotected environment, most security requirements are mandatory in this environment.

EVSEs in *Private Environments* are intended for the usage by a small fixed set of EV users. Some security requirements are lifted in favor of an easier operation or cheaper operation costs of the charging point.

Also intended for a small set of EV users, a *Trusted Environment* is required to have some external means to limit the accessibility of the EVSE. In contrast to a *Private Environment*, the protocol does not guarantee security and all security mechanisms could be omitted.

Depending on the physical accessibility of the charging spot, home users require an EVSE intended for *Private* or *Trusted Environments*.

3.2 Public key infrastructure (PKI)

The ISO 15118 protocol defines its own PKI tree hierarchy to provide digital certificate authentication for actors involved in the charging process [2, Annex E]. As depicted in Fig. 2, a vehicle-to-grid root certificate (V2G Root) is used to issue certificates to subordinate certification authorities (Sub-CA) authorized to issue certificates restricted within specific roles such as MO, CPO, or OEM. Concerning potential memory limitations of the EVs, a maximum certificate chain length of four certificates (path length 3) is established, which allows for up to two Sub-CAs per branch in this hierarchy. Those would most likely be utilized to delegate the issuing of certificates on the level of different institutions. The standard requires the EV to be able to store at least one V2G root certificate [2, Requirement V2G2-008] and the supply equipment to store at least 10 root certificates [2, Requirement V2G2-877].

3.3 Authentication mechanisms for the EV

For authenticating the EV to the EVSE in order to get access to the electrical grid, ISO 15118-2 [2] conceptualized the mechanisms *Plug'n'Charge* (PnC) and *External Identification Means* (EIM).

PnC automates authentication through the use of digital certificates supplied by the PKI for authentication and subse-

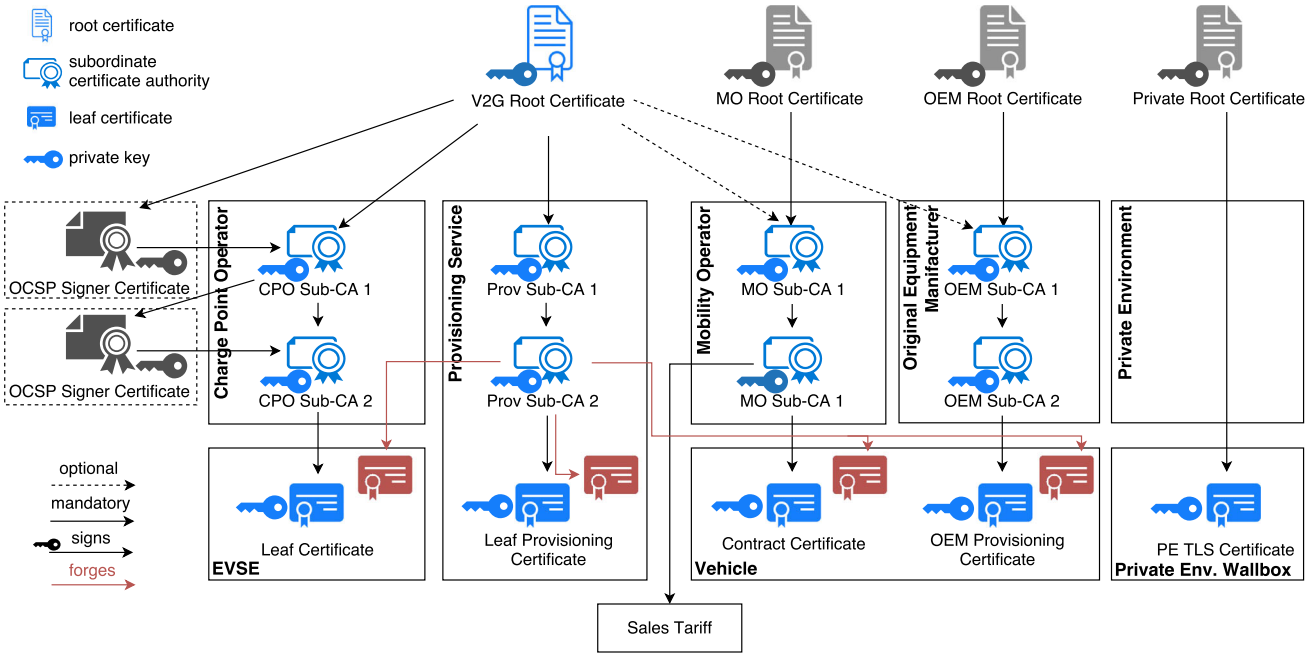

Fig. 2 Certificates structure in ISO 15118 [2, Annex E]

quently authorization. The communication session is further secured through the application of Transport Layer Security (TLS) with unilateral authentication, where the EVCC checks the authenticity of the SECC. Authenticity of the EV is guaranteed by a digital signature scheme.

EIM describes unspecified external means of identification (and payment) to authorize access of an electric vehicle to the grid. This mechanism does not make use of digital certificates, however optionally can utilize TLS to secure the communication between EVCC and SECC. Examples for EIM authentication are RFID identification, credit card payment, prepaid cash, mobile payment or indirect payment via parking fees.

3.4 Lower level protocols

The ISO 15118 standard uses ISO 61851-1 for low-level signaling. Specifically, the *Control Pin* is used to detect the plug-in and plug-out of the EV.

Power line communication (PLC) technology is used for the high-level communication between EV and EVSE. The media for PLC is the *Control Pilot Pin* of the charging cable. The physical and the data link layer is a modification of the HomePlug Green PHY protocol, which is specified in ISO 15118-3. Due to possible crosstalk between multiple EVSEs, the EV needs to find the right EVSE using *Signal Level Attenuation Characterization* (SLAC) which is a protocol to find the EVSE with the strongest signal level [3].

On the network layer, IPv6 is used in conjunction to *Stateless address auto-configuration* (SLAAC) to assign the EV a link-local address. After address assignment, the SECC Discovery Protocol (SDP) is used to find the IPv6-address of the EVSE and to negotiate the transport and security protocols and their versions employed in the further communication. Depending on the environment, the transport protocol may be plain TCP or additionally secured with Transport Layer Security (TLS). SDP by itself does not provide any authentication mechanisms to protect authenticity or integrity of the data transmissions.

Subsequently, the messages exchanged between EV and EVSE as part of the *Higher Level Communication* (HLC) utilize the XML-EXI format, which is a binary XML format. The message sets and schemas are specified in detail in ISO 15118-2 [2].

3.5 IT security and applicable data protection law

The appropriate level of security depends on the applicable data protection law. Under the upcoming *General Data Protection Regulation* (GDPR) a trade-off between risks of potential threats and costs of implementation is necessary taking account of the state of the art to ensure an "appropriate level of security". While the GDPR governs the use of personal data, the sector specific *German Metering Point Operation Act* (*Messstellenbetriebsgesetz*—MsbG) addresses all data derived from the metering point. It stipulates encryption as a minimum requirement while detailed security provisions are expected to be drawn up by the *Federal Office for Information Security* (BSI) until the year 2020. Identified flaws of the security concept of

ISO 15118 could be addressed by this upcoming provisions, depending on the applicable legal framework.

With the legal reform regarding the digitalization of the energy system transformation, sector specific data protection rules of German energy law were specified in the MsbG. Due to the definition of the CPO as end consumer, the relationship between EV and EVSE is not addressed by energy law and thus could also fall outside the scope of the MsbG. However, an explicit exception limited to certain provisions regarding protection profile and technical guidelines for smart meters by the BSI until 2020 shows, that all other MsbG provisions are applicable [9]. The aim of the MsbG is to achieve data protection, security and interoperability for data communication in the smart grid. Under the MsbG, only explicitly authorized parties are entitled to process personal data. The grid connection user (end consumer) can authorize additional parties by consent, which is necessary in case of the CPO. As the end consumer is defined as CPO, the direct application of the MsbG based on the explicit wording seems problematic, especially in case of *Public Environments*. Apart from a legitimation by law, a key element of data protection law is the possibility to give and withdraw consent to the processing of personal data by the data subject, which is the natural person the data is related to. However, the German legislator assumes that both CPO and EV user are end consumers at the same time [9], so that interpreted in compliance with fundamental constitutional rights, consent must derive only from the EV user (or EV owner). The commentary by the German legislator states that the obligation of encryption addresses all kind of communication by the authorized parties [8], which pleads for a wide scope. But if the MsbG only addresses data derived from the metering point, this could exclude the communication from EVCC to SECC in case the metering point is located in the EVSE. To prevent inconsistencies, the whole communication process should be subject to one comprehensive regulatory framework. This would correspond with the objective of an overall approach to regulate smart-grid-communication, which is underlined by the fact that also non-personal data are addressed.

Despite the findings above, the MsbG could be replaced by the GDPR, which will be directly applicable starting May 25th 2018. Unlike a directive, which has to be transformed in national law by the member states and provides a certain level of leeway, the regulation is directly applicable and will replace many German data protection provisions. But as the GDPR is an atypical hybrid between regulation and directive [15], there are so called opening clauses, enabling the member states to create or maintain more specific rules in certain cases by determining more precisely requirements for the processing. This is the case, if data processing is necessary for compliance with a legal obligation or a task carried out in the public interest or in the exercise of official authority. The MsbG could be seen as such more specific provision, as in Germany the energy supply is part of the public service tasks [5]. Metering is required for energy supply, in principle assigned by law to a *metering point operator* (MPO) and the installation of smart meters is obligatory according to the stated preconditions. As legal compulsion should be compensated by sector specific, precise data protection rules, the MsbG should remain applicable besides the GDPR [6].

In conclusion—even if wording and scope of the MsbG should be clarified by the legislator adjusting to the differing role concept regarding CPO and EV user—the CPO requires explicit consent of the EV user to process personal data. Thus, CPO as well as the MPO would have to provide encrypted communication. A charging protocol should take this legal considerations into account.

4 Adversaries

The basis for the threat analysis are formed by the goal and capability definitions of the adversaries. We assume the adversaries to know the ISO 15118 protocol in depth in order to exploit the protocol, but they are still limited to the following reasonable capabilities:

- Following the Dolev–Yao model [10], the adversaries are not capable to break the contemporary encryption schemes efficiently. They may be able to eavesdrop and manipulate the unencrypted communication if they have physical access to the media.
- An adversary is able to modify their own electric vehicle, but is unable to access or modify the internal hardware and software of other electric vehicles.
- The adversaries cannot access the internal hardware and software of the supply equipment. We assume that the EVSE will always fully comply with the protocol specification. However, an adversary may modify a supply equipment externally or set up a counterfeited EVSE which is completely under the control of the adversary.

Four different types of adversaries have been defined and labeled according to their goal. They do not have a particular affinity for certain types of attacks and would utilize all threats as described in Sect. 5 to accomplish their goal and acquire the targeted asset:

Freeloader The freeloader wants to charge his EV without payment or with reduced payment. He may achieve this by spoofing his identity, by repudiating a charging session, by manipulating charing tariffs or by skimming energy from a legitimate charging session. His aim is to target electricity directly or to export the costs to a legitimate user or the mobility operator.

Contract-Sharer The contract-sharer tries to apply a scheme similar to sharing conditional access modules for Pay-TV.

He colludes with other contract-sharers in order to re-use one mobility contract for a number of electric vehicles. This is especially profitable for the adversaries if the tariff of the contract applies a flat fee for charging.

Denial-of-service-attacker This adversary has the goal to prevent legitimate EV user(s) from charging and thereby attacking the availability of the charing service. This could be accomplished by identifying a bottleneck in the EVSE hardware or specifications and target specific components such as CPU-time, RAM-memory, bandwidth or others. His motivation could be to target a specific EV user or to discredit a specific mobility or charging point operator. While not directly benefiting from his actions, he could be compensated outside the scope of ISO 15118.

Eavesdropper An Eavesdropper aims to collect information of legitimate users such as charging times or identification of EV and EVSE. His goal could be to distribute or sell the acquired information and target the privacy of specific users or user groups.

5 Threats

Based on the goals of the previously defined adversaries, we enumerate threats which originate from these adversaries. We analyze how these threats can be exploited with regard to the security concept of the ISO 15118 standard. Often, threats can only be mitigated under certain assumptions which are outside the scope of ISO 15118. We reveal these assumptions and non-trivial requirements which are essential to the security concept. These assumptions are collected in Sect. 6.

5.1 Masquerade as an electric vehicle

In this threat, we look at the possibilities of an adversary to make the supply equipment believe that it is communicating with an authenticated electric vehicle with an identity chosen by the adversary. The adversary *Freeloader* has the intention to masquerade as an arbitrary victim so that he can charge his vehicle at the expense of the victim. Lee et al. [16] describes this threat as "Changing ID number". The intention of the *Contract-Sharer* is to use only one contract for a number of vehicles.

Masquerading can either be implemented by (a) Initiating an authenticated charging session or by (b) Hijacking an authenticated charging session. The two variants are discussed in Sects. 5.1.1 and 5.1.4

5.1.1 Initiating an authenticated charging session

For the adversary to initiate an authenticated charging session, he has to attack one of the two authentication mechanisms, *Plug'n'Charge* (PnC) or *External Identification Means* (EIM).

For EIM, ISO 15118 defines the security of these mechanisms outside the scope of the standard, but it remains clear that we have to require the infeasibility of external identification means spoofing in Assumption 6.1 to protect against adversaries like *Freeloader* or *Contract-sharer*.

For PnC, contract certificates are used to authenticate an EV and to associate the EV to a specific mobility contract which has been concluded between EV owner and mobility operator. The contract certificate consists of a X.509 certificate and the private key, which are stored on the EV so that the EV itself is sufficient to authenticate a charging session. The standard mandates the usage of TLS for the communication session when PnC authentication is used and the authentication uses a signature scheme [2, Clause 7.3.4]. As we assume our adversaries are not able to break the signature scheme efficiently, the only two ways for the adversary to initiate charging sessions is either to obtain a valid certificate and private key or to use an expired or revoked certificate. We discuss both possibilities in the Sects. 5.1.2 and 5.1.3.

5.1.2 Obtaining a contract certificate

This threat discusses the locations where contract certificates are prone to disclosure. ISO 15118 specifies that the private key of the contract certificate is generated by the mobility operator. The private key is installed either *online* during the first charging session, or *offline* by the EV owner using a provided PKCS#12-file (cf. [2, Clause 8.4.3.11]). In the online installation case, the private key is encrypted using the pre-installed OEM provisioning certificate of the EV (cf. [2, Table 45]). Key generation inside the EV or even on a hardware security module inside the EV would be more secure, but requires more interaction between EV owner and EV. This design decision introduces several points of attack which need to be protected from disclosing the private key:

1. The mobility operator generates the private key of the contract certificate. Key generation needs to be secure (e.g. not re-using keys) and the private keys must be protected from disclosure. Otherwise, the consequences of disclosed key (databases) could affect a high number of EV users. This leads to Assumption 6.2.
2. Additionally, online certificate installation depends on the proper key management of the OEM. If an adversary is able to obtain the OEM provisioning certificate, he can initiate an ISO 15118 charging session and request a certificate installation by masquerading as contractor's EV. The adversary is able to decrypt the private key of the contract certificate by using the private key of the OEM provisioning certificate. To prevent this point of attack, Assumption 6.3 has to be fulfilled.

3. If the certificate is installed using the offline certificate installation procedure, the EV owner receives the certificate and the private key as PKCS#12-file. Any password used to encrypt the private key is also known to the EV owner. As adversary *Contract-Sharer*, the EV owner colludes with other contract-sharers and is able to easily distribute his certificate in this way. The ISO 15118 standard does not prevent this threat, so we have to assume the tariff to be unattractive for contract-sharing in Assumption 6.4. The adversary *Freeloader* wants to obtain the secrets from the EV owner without his permission. The standard describes in a note [2, Note 3, Clause 7.9.2.2] how the transmission of contract certificate can be kept safe from disclosure.
4. The private key of either OEM provisioning certificate or contract certificate could also be obtained by tampering or stealing the communication controller of the electric vehicle. Thus, we have to rely on Assumption 6.5 to hold. Falk and Fries [11] describe this as part of the threat "Tampered / Substituted Component".

Another point of attack are the (sub) certificate authorities in the public key infrastructure:

5. If the adversary gains access to the private key of any certificate authority (CA), he would be able to generate arbitrary contract certificates. We need Assumption 6.6 that CA keys are sufficiently protected. Furthermore, the PKI certification hierarchy does provide a unique identifier field "Domain Component" to X.509 certificates, which is only mandated for leaf certificates. Thus, the Sub-CAs technically have the authority to issue certificates beyond their conceptualized domains. In theory, the theft of a private key of any Sub-CA of any domain would leave the possibility of creating a valid certificate for any domain role including contract certificates. We identify this unnecessary privilege extension as Flaw 7.4.

5.1.3 Using an expired or revoked contract certificate

Instead of obtaining a currently valid certificate, the adversary may also use an already expired or revoked certificate. Revocation and Expiration of certificates are also mechanism to limit the impact of a stolen certificate. However, the ISO 15118 standard does not specify any requirements on time synchronization for the supply equipment. The standard also declares revocation-checking with OCSP as optional for the supply equipment. Under these conditions, an adversary may be able to turn back the clock of the supply equipment and use a stolen contract certificate indefinitely. We identify these points as Flaw 7.1 "Missing requirement for secure clock synchronization of the supply equipment" and Flaw 7.2 "No requirement for the supply equipment to check EV certificate validity using OCSP" in the security concept.

5.1.4 Hijacking an authenticated charging session

A possibility for the *Freeloader* adversary to get his car charged at the expense of a victim is to hijack an already authenticated charging session. The adversary waits for the victim to start an authenticated charging session. As soon as the charging operation has concluded, the adversary prevents the charging session from ending by pausing the charging session. To the victim, it appears that the charging session is closed and the process has concluded. After the victim has departed, the attacker resumes the charging session and charge on the expense of the victim.

To resume the charging session, a Session-ID and Charging Parameters are required, which need to be eavesdropped using a man-in-the-middle attack. Eavesdropping is only possible if TLS is disabled which means that this hijacking threat can only be exploited in trusted environments using EIM as authentication mechanism. Under these conditions, the adversary can force the communication to use plain TCP instead of TLS using the man-in-the-middle attack described in Sect. 5.2. Additionally, the adversary must prevent that the EVSE is able to detect the plug-out of the victim's EV by keeping the *Control Pilot Pin* in state B even if the victim plugs out. This can be implemented using a modified cable or an adapter plug installed on the EVSE.

We think that exploiting this threat is feasible with some effort. The threat could have been mitigated with the consistent use of TLS. The standard however abandons TLS for trusted environments with EIM as authentication method. We see this as Flaw 7.3 of the security concept.

5.2 Man-in-the-middle attack

As Fries and Falk [11,12] already envisioned, a man-in-the-middle attack can be achieved by a modified charging cable or by positioning a fake charging point placed between victim's EV and the supply equipment. If the adversary is only targeting the communication, only the *Control Pilot Pin* and the *Control Pin* (signal range within 12 V) need to be intercepted.

Another man-in-the-middle attack is possible if one power line communication (PLC) interface handles many EVs [1, Annex A.2]. The matching process described in ISO 15118-3 [3] is unauthenticated and as such, an adversary can claim to be the supply equipment with the highest signal strength. The victim's EV then connects to the adversary and the adversary can forward and modify all messages to the real supply equipment. The adversary's PLC interface needs to be modified in such a way that it spoofs a high signal strength and that it can

also act as Central Coordinator (CCo), which ISO 15118-3 forbids by requirement V2G3-A06-02 [3].

A third possibility is by using the SECC Discovery Protocol (SDP) (cf. [2, Clause 7.10.1]). This protocol is unauthenticated such that any adversary on the same logical network can claim to be a supply equipment. Joining the logical network can be achieved by using the before-mentioned attack.

The effects of these attacks can be mostly mitigated using end-to-end authentication provided by TLS. However, TLS is optional if the supply equipment is located in a *Trusted Environment*, which is a serious flaw in the security concept (see Sect. 7.3).

5.3 Masquerade as a supply equipment

Masquerading on physical and data link level is feasible on the basis of the unauthenticated matching process as described as part of the man-in-the-middle-attack in Sect. 5.2. Masquerading in a TLS-based charging session requires stolen certificates or the installation of a false root certificate. In contrast to the requirements for the supply equipment, application of OCSP is mandatory for the electric vehicle such that stolen certificates of public supply equipments can be revoked effectively. For private supply equipments, deinstallation of the certificate is described in Clause E.2 of ISO 15118-2 [2]. The remaining threats are investigated in the following subsections.

5.3.1 Physical energy skimming

Falk and Fries [11,12] described this threat as a variant of the man-in-the-middle attack. The adversary *Freeloader* may manipulate a charging cable or position a faked charging point and wait for a victim to use it for charging. The cable or charging point is connected to the adversaries' car which is in turn connected to a genuine charging point. All the ISO 15118 high level communication is transparently forwarded between the victim's EV and the genuine charging point. When the grid circuit is closed for charging, the adversary is able to physically skim some energy from the legitimate charging session. Such an attack could be detected by the EV using meter readings during the charging loop, but support for meter readings are optional.

5.3.2 Discharging a victim's EV using vehicle-to-grid support

An adversary masquerading as supply equipment may take advantage of the vehicle to grid support (see [1, Use Case F5]) and extract energy from the battery of a victim's EV. With the 2015 revision of ISO 15118-2, the technical details about V2G are not yet published. But we expect V2G functionality only to be available for PnC authentication as the billing of such services is complex. Thus, TLS also becomes mandatory for the communication and in turn, the adversary has to be able provide a legitimate charging point certificate in order to mount this attack.

5.3.3 Eavesdropping on charging sessions

Except in *Trusted Environments*, TLS is mandatory such that eavesdropping on identifying information like the E-Mobility Account Identifier and the MAC address of the EVCC (see *EVCCID* in [2, Table 26]) is only feasible if an adversary is able to obtain valid supply equipment certificates. However, on the data link layer (ISO 15118-3 [3]), each vehicle can be identified by the MAC address of the PLC interface. Additionally, on the network layer, the MAC address could also be derived from the IPv6 address. The communication on these layers is not encrypted so that an *Eavesdropper* adversary is able to identify charging EVs connected to the same SECC. Höfer et al. [14] describe the implications on privacy in detail.

5.4 Repudiate charging session

Repudiation becomes feasible if doubts of the authenticity of the involved parties can be raised. Especially the threats described in Sect. 5.1 can be used to raise such doubts. We identified no new threats specific to this category. Falk and Fries [11] describe this threat as "Transaction Falsifying / Repudiation".

5.5 Denial of service (DoS)

It is likely that in a real-world deployment, for cost-efficiency reasons, not every charging point will have a dedicated supply equipment communication controller (SECC). When multiple users share the same SECC, it is possible to conduct an effective Denial-of-Service attack on the SECC. The effects of a DoS attack depend on how many charging points are serviced by a single SECC. In the worst case scenario, there is only one SECC handling a whole infrastructure of a charging point operator. A successful DoS-attack would cause an outage of a whole infrastructure.

A possible DoS attack is to request and maintain multiple charging communication sessions simultaneously. If the attacker is successful in doing this, without necessarily having to invest heavily in resources to do so, more and more connections could be created over time, so that the SECC reaches a connection threshold. Legitimate users will then no longer be able to connect to the SECC. This threat is related to the threats "Attack Network (DoS)" by Falk and Fries [11] and "Shutting off service of EVSE" by Lee et al. [16].

5.5.1 Jamming the local network media

Many charging points may share one power line communication (PLC) media. The *DoS-Attacker* adversary can jam the PLC media by generating noise in the spectrum used by ISO 15118-3. However, the impact of this threat is limited to a local area only.

5.5.2 Diverting communication

Lee et al. [16] describe the threat "Shutting off service of EVSE" by means of manipulating the EVSE status in order to deny charging service to legitimate EV users. We consider this particular approach impractical due to the use of TLS in *Public* and *Private Environments*, which will detect manipulation of the message content.

However, this threat can be realized only based on the man-in-the-middle attack described in Sect. 5.2. By letting the EV continuously connect to a spoofed supply equipment, the adversary can effectively shut off any high level communication between EV and the real supply equipment.

5.5.3 Consuming the session limit

Another possible DoS attack would be to leverage a potential session or connection limit implemented by the SECC. Even though the standard does not stipulate a session or connection limit, any implementation may still have this limit. The *DoS-Attacker* could manage to occupy all available sessions by creating an arbitrary number of sessions and keep the SECC on hold as long as possible, similar to the SlowLoris Attack [7]. Although the implementation of several timeouts [2, Clause 8.7.2 and 8.7.3] are required, the adversary may be able to leverage cycles in the communication state machine (see [2, Fig. 103]) to keep each charging session open with a low bandwidth usage.

5.5.4 Time synchronization

An accurate date and time is required to check the validity of TLS certificates. If an adversary is able to manipulate the time, he can easily invalidate all certificates. As the standard does not require an accurate time source or an authenticated clock synchronization for the charging point, this threat is feasible. We refer this as Flaw 7.1 in the security concept.

6 Implicit assumptions in the security concept of ISO 15118

As result of the threat analysis in Sect. 5, the following assumptions were identified to be essential for the infeasibility of these threats. These assumptions need to be diligently checked for the application context and deployment of ISO 15118.

6.1 Unforgeable external identifications means (EIM)

To protect from masquerading threats, external identifications means need to be unforgeable. Otherwise, the billing process cannot rely on the identity given by the external identification means. History showed that this assumption is not always fulfilled [13,18,19].

6.2 Proper contract certificate key generation and disclosure protection

The contract certificate and its corresponding private key is generated by the mobility operator. It is the responsibility of the mobility operator to generate the private key such that it contains enough entropy. After generation, the mobility operator has to keep the private key safe from disclosure, e.g. by encrypting the private key with the OEM provisioning certificate and erase the plain private key immediately after encryption.

6.3 Proper OEM provisioning certificate key generation and disclosure protection

Safe key generation and disclosure protection is also required for the OEM provisioning certificate. The standard suggests that the private key is generated outside the vehicle and installed on the vehicle during production [2, Clause E.3.2.1]. It is required that the private keys are kept safe from disclosure, e.g. by erasing it after installation or generating the key on the EV.

6.4 The EV owner has no interest in sharing his contract

Directly contradicting the adversary *Contract-Sharer*, we need to assume the mobility tariff is designed in such a way that the EV owner has no interest in installing his contract on multiple electric vehicles. This is easily possible due to the offline installation procedure described in Clause 8.4.3.11.4 [2].

6.5 The adversaries are not able to tamper the communication controller of the electric vehicles

By requiring this, we want to prevent any adversary from using the contract and provisioning certificate's private keys. Clause 7.9.2.2 of the ISO 15118-2 [2] proposes the use of a hardware security module (HSM), but this alone is not sufficient. A HSM only prevents the disclosure of the secrets but the adversary may still use the keys for encryption and signing.

6.6 All (subordinate) certificate authorities protect their private keys properly

This is a basic requirement for the security of the public key infrastructure. Achieving this is not easy for the mobility operator as he requires his CA key to sign the SalesTariff (see Fig. 2).

7 Flaws in the security concept of ISO 15118

Another result of the threat analysis is the identification of the following flaws in the security concept of ISO 15118.

7.1 Missing requirement for secure clock synchronization of the supply equipment

A reliable time source is required for the correct operation of TLS. The standard does not require the supply equipment to have such a time source. However, such a requirement exists for the electric vehicle: Requirement V2G2-886 states that the accuracy of time source of the electric vehicle "should be at least one day" [2]. Such a requirement needs to be extended to also apply for the supply equipment.

Also, the standard should give some hints on which time source can be regarded as reliable. The prominent methods for time synchronization: DCF77, Cellular, GPS and NTP are (usually) not authenticated. Due to this missing specification, an adversary could assume control over the clock of either EV or EVSE.

7.2 Missing requirement for the supply equipment to check EV certificate validity using OCSP

Proving the validity of an electric vehicle certificate through the usage of the OCSP protocol is not designated as mandatory for the supply equipment. Again, such a requirement only exists for the electric vehicle (see V2G2-875 and V2G2-910 [2]). Such a requirement needs to be extended to supply equipments to guarantee an effective revocation mechanism for contract certificates.

7.3 Optional TLS encryption in a trusted environment

The standard requires the mandatory application of TLS in the communication between electric vehicle and supply equipment. The only exception is the case when external identification means (EIM) are used for the authentication of the charging session in a trusted environment (cf. Requirement V2G2-631 [2]).

In this scenario, TLS is not utilized and the communication is not protected against tampering or manipulation. Mültin [17] also recognizes this as serious flaw which "should have never been standardized". Through the introduction of such an exception, it is possible that implementation errors or improper configuration could lead to a downgrade of TLS in other use cases. Such potential weaknesses are targeted for man-in-the-middle attacks.

7.4 The jurisdiction of subordinate certificate authorities (Sub-CAs) is not limited

The certificate profiles of Sub-CAs in different roles are not distinguishable (cf. [2, Annex F]). This way, the certificates signed by a Sub-CA can assume any role. For example in Fig. 2, the Sub-CA of a Charge Point Operator (CPO) can issue certificates for electric vehicles. The structure of the subordinate certificate authorities should include technical means to bind Sub-CAs to a certain role.

8 Recommendations

After identifying the assumptions and flaws of the security concept of ISO 15118, we compiled some recommendations to enhance the security concept.

8.1 Authenticated time synchronization

To prevent time manipulation, only authenticated mechanisms to synchronize time should be used. The time accuracy requirements have to be extended especially for the EVSE to prevent fraud using expired certificates. Also, references on how to achieve authenticated time synchronization would be helpful. For example, the technical guideline TR-03109-1 [4] for German Smart Meter Gateways propose NTP over HTTPS or TLS.

8.2 Mandatory certificate verification with OCSP

The specification should mandate the verification of the validity status of contract certificates of an EVCC to restrict the time-frame a stolen certificate can be used. This can be accomplished by mandating the application of the Online Certificate Status Protocol (OCSP) in public environments, including EVSE.

8.3 Withdraw trusted environments and optional TLS

Whenever possible, optional security mechanism should not be standardized. This only provokes implementation errors and mis-configuration. The standard should require the usage of TLS in all environments and remove the notion of a trusted environment altogether.

8.4 Restricting roles of certificates a Sub-CA can issue

To limit the impact of a stolen Sub-CA key, the types of certificates a Sub-CA can issue should be limited. A technical solution could be the inclusion of the role across Sub-CAs as part of the certificate. Such a "branding" could be applied to the certificates at the end of the certificate chain. The specification should also mandate the role verification in such a solution.

8.5 Redesigning certificate key generation

In our analysis, Assumptions 6.2 to 6.4 are required to protect the key of the contract certificate. These assumptions are not necessary if the key is generated on the EVCC and never has to be transmitted. Key generation in the EV may require one additional round-trip in the online certificate installation process. Usability of offline certificate installation can even be improved if optical transmission of binary data like QR-codes are used to transfer the public key to the mobility operator.

9 Conclusion

In this paper, we performed an up-to-date threat analysis of the electric vehicle charging process described in the ISO 15118 standard. The reasonable security concept of the standard already considers many threats, but the standard weakens it by introducing exceptions. In our work, we revealed assumptions which are not explicitly described in the standard, but nonetheless are required to guarantee the security against fraud in the charging process. In the analysis, we point out four conceptual flaws in the security concept of ISO 15118:

1. Missing requirement for secure clock synchronization of the supply equipment,
2. No requirement for the supply equipment to check EV certificate validity using OCSP,
3. Optional TLS encryption in a trusted environment,
4. No limitation on the jurisdiction of subordinate certificate authorities.

Finally, we proposed recommendations to remedy these flaws.

References

1. ISO 15118-1:2013. Road vehicles—vehicle to grid communication interface—Part 1: general information and use-case definition. International Organization for Standardization
2. ISO 15118-2:2014. Road vehicles—vehicle-to-grid communication interface—Part 2: network and application protocol requirements. International Organization for Standardization
3. ISO 15118-3:2015. Road vehicles—vehicle to grid communication interface—Part 3: physical and data link layer requirements. International Organization for Standardization
4. BSI TR-03109-1 (2013) Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems. Federal Office for Information Securtity (BSI)
5. Bräuchle T (2017) Datenschutzprinzipien in IKT-basierten kritischen Infrastrukturen
6. Bretthauer S (2017) Smart Meter im Spannungsfeld zwischen Europäischer Datenschutzgrundverordnung und Messstellenbetriebsgesetz. Zeitschrift für das gesamte Recht der Energiewirtschaft, pp 56–61
7. Damon E, Dale J, Laron E, Mache J, Land N, Weiss R (2012) Hands-on denial of service lab exercises using slowloris and rudy. In: Proceedings of the 2012 information security curriculum development conference, InfoSecCD '12, pp 21–29. ACM, New York, NY, USA. doi:10.1145/2390317.2390321
8. Deutscher Bundestag: Drucksache 18/7555, Entwurf eines Gesetzes zur Digitalisierung der Energiewende (17.02.2016). http://dip21.bundestag.de/dip21/btd/18/075/1807555.pdf
9. Deutscher Bundestag: Drucksache 18/8919, Beschlussempfehlung und Bericht zum Entwurf eines Gesetzes zur Digitalisierung der Energiewende (22.06.2016). http://dip21.bundestag.de/dip21/btd/18/089/1808919.pdf
10. Dolev D, Yao A (1983) On the security of public key protocols. IEEE Trans Inf Theory 29(2):198–208
11. Falk R, Fries S (2012) Electric vehicle charging infrastructure security considerations and approaches. In: Proceedings of INTERNET, pp 58–64
12. Falk R, Fries S (2013) Securely connecting electric vehicles to the smart grid. Int J Adv Internet Technol 6(1 & 2): 57–67
13. Garcia FD, de Koning Gans G, Muijrers R, van Rossum P, Verdult R, Schreur RW, Jacobs B (2008) Dismantling MIFARE classic. Springer, Berlin, pp 97–114. doi:10.1007/978-3-540-88313-5_7
14. Höfer C, Petit J, Schmidt R, Kargl F (2013) Popcorn: privacy-preserving charging for emobility. In: Proceedings of the 2013 ACM workshop on security, privacy & dependability for cyber vehicles, pp 37–48. ACM
15. Kühling J, Martini M (2016) Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht? Europäische Zeitschrift für Wirtschaftsrecht, pp 448–454
16. Lee S, Park Y, Lim H, Shon T (2014) 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), pp 1–4. IEEE
17. Mültin M (2014) Das Elektrofahrzeug als flexibler Verbraucher und Energiespeicher im Smart Home. Ph.D. Thesis. http://digbib.ubka.uni-karlsruhe.de/volltexte/1000042102. Karlsruhe, KIT, Diss
18. Nohl K, Evans D, Starbug S, Plötz H (2008) Reverse-engineering a cryptographic RFID tag. In: USENIX security symposium, vol 28
19. Verdult R, Garcia FD, Balasch J (2012) Gone in 360 seconds: Hijacking with Hitag2