telio EV

SECURE
YOUR DATA
STAY
IN COMMAND

www.telioev.com

The world has been facing extreme challenges to its survival, much credit to emissions that wreak havoc on our climate and threaten our peaceful existence. Emissions from mobility are a major reason cause for global warming and damage the earth's ecological balance. Electric mobility offers a great solution to enable human locomotion while ensuring that we are doing it in a sustainable manner that does not cause emissions and tip the balance of the earth to the worse. However, e-mobility comprises of multiple micro-processes brought together to build a solution which is practical for the masses too adopt and use. E-mobility comprises of a lot of devices and communication between them, which essentially, is a lot of data sharing. Subsequently, we face the need to make sure that the data remains secure throughout the entire flow of processes. In this white paper, we see the security threats that we can face and the solution to those threats that Teliolabs EV software solution offers.

Introduction:

EV charging stations which are essentially IoT devices are vulnerable due to a lot of reasons, such as using a variety of protocols, communication medium and devices. There are two interfaces here; one for electricity (electric energy) and the other is for the control messaging. It is of paramount importance to find a way to integrate both these interfaces in order for the charging sessions to be executed. Open Charge Point Protocol (OCPP) offers a way to coordinate communication and ultimately power flows between CPs (Charge Points) and CMS (Charger Management System) along with maintaining consistent communication with EVs and the grid. The Teliolabs EV charging software solution ensures that the charging processes run smoothly along with linked processes such as payment in a secure manner. For it, one of the things done by it is to ensure that the charging process is initiated only after it is authorised by a billing system. However, the protocol assumes that the individual components involved are trustworthy and cannot be compromised.

Problem definition:

An adversary can attack the infrastructure at the architecture (a) of the whole system and the communication medium (c) which can be the internet or wireless medium. The threats can be denoted by threats A (a, c) and include:

1. Disclosure, which corresponds to illicit reading and/or copying of information;
2. Distortion, any (fake) data insertion, spoofing or modification action (data, processes or configurations)
3. Disruption, that comprises the deleting or dropping of messages, processes or actions. Variants of this last threat can be those related to denial of service (DoS) such as gray hole (selectively forwarding packets to the next hop) or black holes (dropping all messages), reduction of functionality.

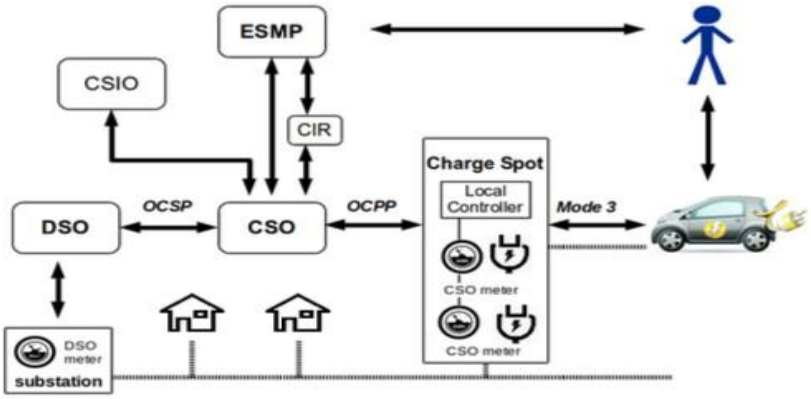


Fig. 1. Information flows for EV charging

The figure above gives a schematic of the EV charging set-up, where:

- The DSO (Distribution System Operator) manages a regional electricity grid, and isresponsible for a stable, reliable and well-functioning grid delivering electricity to consumers.

- The EMSP (E-Mobility Service Provider) (re)sells electricity to EV users for charging their car.So, the EMSP will set up contracts with EV users and takes care of billing.

- The CSO (Charge Spot Operator) operates and maintains charge spots. CSOs play animportant role in the EV market, as they interact with the DSO and the EMSPs.

- The CSIO (Charge Spot Infrastructure Operator) is typically a vendor of charge spots and will perform some maintenance, such as updating firmware, on behalf of the CSO. In some situations, such maintenance is only performed through the CSO, i.e., updates are sent to the CSO and the CSO takes care of them, but in other cases it is done directly by the CSIO.

Security Shortcomings:

1. Weak Authentication:

At public charge spots drivers authenticate themselves using an RFID card. Surprisingly, only the static ID (the so-called UID) of the card is used for authentication here. In essence, this means every customer is identified through a password that is transmitted plaintext through the air. This makes copying the cards extremely simple: on legitimate RFID cards the UID is fixed and cannot be changed, but counterfeit cards with a configurable UID and equipment that can spoof the RFID communication are readily available.

The UID can be eavesdropped if one has access to the card by simply using a standard NFC-enabled phone. With electronic equipment it is also possible to eavesdrop on the UID when it is used at a charge spot. This is possible at a distance of several meters [6, 7], but it would be simpler to stick eavesdropping equipment right on top of the RFID antenna of a charge spot. An attacker could also simply try out random UIDs until he finds one that the charge spot accepts, by reading out the UID of a few legitimate cards it will be easy to determine the approximate range of UIDs used for EV charging.

That cloning cards is so easy does not necessarily mean there is a viable criminal business model. Blacklisting cloned cards can frustrate fraudulent use of cloned cards, at the expense of also creating hassle for innocent victims who had their card cloned. The real deterrent to fraud would probably be the risk that users of the cloned cards run of being caught red-handed. Especially since charging electric cars still takes a significant amountof time.

2. Reliance on secure tunnels:

As a security measure, the OCPP specification suggest the use of TLS to secure communication links. In practice, this suggestion may not be followed because of bandwidth restrictions (charge spots generate very small messages, where introducing TLS increases the overhead significantly) and cost: charge spots often communicate over cellular networks, and the use of this communication link will be charged per transmitted byte, making the overhead extra costly. This means that these OCPP links then rely on the security offered by the underlying cellular technology.

Note that even if TLS is used to protect both the OCPP and the OSCP links, this still has some security shortcomings: it would not always provide true end- to-end security, and it would not provide a practical means for non-repudiation, as explained below:

- **Lack of end-to-end security:**

Some of the information for smart charging is forwarded across multiple links. For instance, measurement data generated at the charge spot meter should end up at the EMSP, so they can bill the customer accordingly. The CSO forwards the data received from the charge spot to the EMSP. Even if both the communication links are protected by TLS, this does not provide end-to-end security between the charge spot and the EMSP. The TLS tunnels will prevent against tampering at intermediate points between the charge spot and the CSO, and at intermediate points between the CSO and the EMSP, but the CSO will have to be trusted not to change the data. The same goes for metering data that goes from the charge spot to the DSO, or, conversely, for the charge plans that go from the DSO to charge points. To summaries: TLS does provide a secure tunnel, but only for one communication link, and not across multiple links.

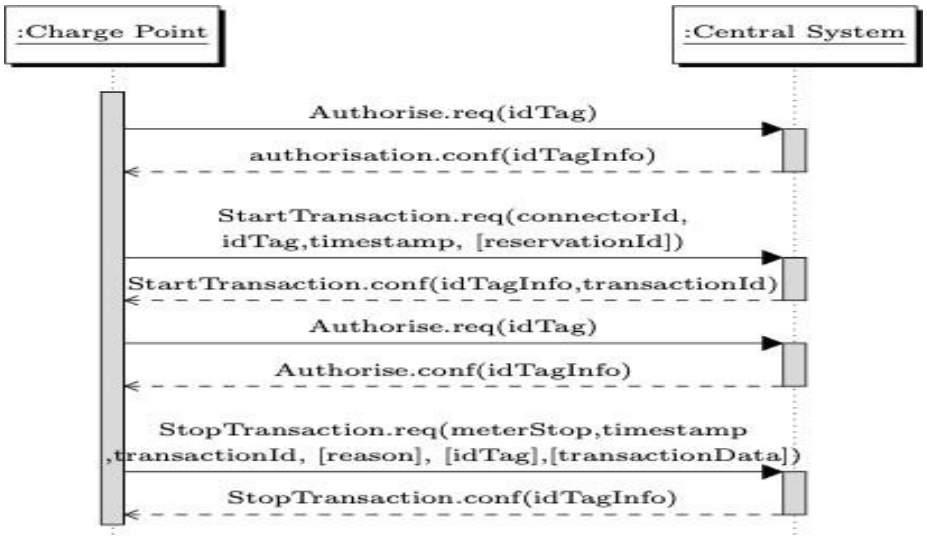
- **Lack of non-repudiation:**

TLS ensures the integrity of the data sent be- tween two parties: Message Authentication Codes (MACs) are added to any data sent and upon reception these are checked to rule out tampering with the data. As soon as data exits the TLS tunnel, all these integrity measures are stripped - what is left is the original data that was sent.

This has the advantage of making the data protection completely transparent. But a downside is that there is no easy way for the receiver to later prove the integrity of the message to a third party. The only way to do this would be to provide a log of the entire TLS session, including the TLS handshake, which is hardly practical.

MitM (Man-in-the-Middle) may also intercept the channel to lead on-path attacks of the kind threats A(c) ⊆ {distort, disrupt} such as: exhaustion of the channel, delays, replays by not being guaranteed the freshness of the OCPP messages, dropping or impersonation (e.g., sink- holes to attract traffic towards a malicious node, or wormholes to entail a sinkhole with several nodes in conjunction.

To illustrate the part of the information that we intend to protect, we must first look at the charge operation defined by the OCPP specification, which we described briefly in the introduction and is shown in the figure below. According to the sequence diagram in this type of operation, the user needs to be authenticated before the charge starts and before it ends. When the charge is provided, the charge point sends a Stop Transaction message that informs the central sys- tem of the quantity of energy charged through the Meter Stop value (specifically, computing the difference between that value and the Meter Start value received at the beginning of the transaction). Although more details about the trans- action can be provided to the CS with the optional transaction data element within the message, we accept that meter Stop is the one to be protected, hence its value has to be kept hidden from attackers



Transaction message flow between CP and CS

3. High level solution:

The solution to ensure data security in the EV charging processes has the following ensure thefollowing:

- Availability of electricity
- Integrity and non-repudiation for billing
- Privacy
- Business confidential data

4. Solution details:

We can now have a further look into the security requirements:

- **Availability of electricity:** Clearly availability of electricity is of paramount importance. Both theavailability and the integrity of information could affect the electricity supply, namely if the absence or incorrectness of information could hamper operation of the grid.

- **Integrity and non-repudiation for billing:** For billing integrity of the records of the charging is important. Some form of authentication of EVs or EV users will be needed for this. One may alsowant some form of non- repudiation, i.e.some evidence to settle disputes, say in case a customer of an EMSP disputes her bill. Non-repudiation is related to integrity, but, as we will seelater, some measures to ensure integrity (notably the use of secure tunnels) do not provide a practical means to support non-repudiation.

- **Privacy:** Confidentiality of information about an individual EV is important for the privacy of its user, as it for instance reveals the location where an EV was at a given time. Given that the userof an EV is typically a single person, such information will be personal information, and hencesubject to legal requirements on the handling of personal information.

- **Business confidential data:** Some of the companies involved may consider some of their data confidential for business reasons. For example, a CSO might not want its competitors to know how busy it's charge spots are, and an EMSP might not want its competitors to know customerinformation.

We need to address the security shortcomings of secure tunnels above, and to provide more flexibility and scalability in handling the information flows between the many parties involved in EVcharging. These directions are related in that they revolve around letting the data itself, rather thanthe communication links, play a central role.

5. Data-centric security:

By data-centric security we mean providing security at the level of data messages, rather than at the level of the communication links. We can take a look at the example of ISO 15118 in which the metering data can be digitally signed by both the car and the charge spot. This means that theultimate recipient of the data, say an EMSP, can verify that the data record comes from a particular customer and a particular charge spot.

In case of any disputes, the digital signatures provide evidence that a particular EV was involved in charging. So, this provides non-repudiation and end-to-end security, more specifically end-to-end integrity, between EMSP, charge spot and EV.

These guarantees do not rely on any secure tunnels for the communication, and that the CSO does not have to be trusted not to change the data. We hereby circumvent the threats the cometo data security in EV charging at the level of communication medium, which is also very helpfulsince we get rid of the need to separately design protocols set stringent standards to ensure thesecurity of the communication channel being used in EV charging. More generally, similar to the way that ISO 15118 provides integrity checks on certain messages,data integrity and confidentiality of data messages can be handled at the level of individual.

messages using the same standard crypto- graphic mechanism: integrity of messages can beguaranteed using either digital signatures or MACs, and confidentially of messages can be handled by encryption.
These solutions overcome the limitations of generic secure tunnels. They can provide end-to-end security, even for data forwarded between multiple parties, and provide non-repudiation, as messages come with their individual integrity checks.

6. Business benefits:

Data is a valuable asset that generates, acquires, saves, and exchanges for any company. Protecting it from internal or external corruption and illegal access protects a company fromfinancial loss, harm to reputation, consumer trust degradation, and brand erosion. Ensuring data security results in:

- Keeping your sensitive data out of the hands of competitors
- Retaining data integrity
- Enabling easy access to data wherever and whenever it’s required for business operations Customers generally expect that companies will safeguard their sensitive data, so any loss of thistrust can have huge ramifications for future custom, and ultimately a business’ bottom line. There’s the legal and moral obligation that companies have to protect their user and customer data from falling into the wrong hands.

For businesses, it is of paramount importance that the customer trusts them and is happy to accept products/services from them. This inevitably builds customer loyalty which is key for thebusinesses to achieve consistency in revenue and overall value, while also enabling growth.

References:

1. *Securing the information infrastructure for EV charging: Fabian van den Broek, Erik Poll, and B́ arbara Vieira*
2. *OCPP Protocol: Security Threats and Challenges: Cristina Alcaraz (Member, IEEE), Javier Lopez (Senior Member, IEEE), and Stephen Wolthusen (Senior Member, IEEE), 2017*
3. *Addressing Security in OCPP: Protection Against Man-in-the-Middle Attacks: Juan E. Rubio, Javier Lopez, Cristina Alcaraz*

telio EV

ONE STOP DESTINATION FOR

ELECTRIC VEHICLE

CHARGING MANAGEMENT SOLUTIONS

telio EV

TelioEV provides Complete Solutions for Electric Vehicle Charging Management

www.telioev.com

CONTACT DETAILS

91 Springboard Kondapur, 2nd Floor,Mytri Square,

2-41/11, 6/2, Gachibowli, Opp. Sharath Capital Mall / AMB Mall,

Prashanth Nagar Colony, Hyderabad, Telangana 500084.

support@telioev.com