Securing the information infrastructure for EV charging

Fabian van den Broek[1], Erik Poll[1], and Bárbara Vieira[2]

[1] Radboud University, the Netherlands
{f.vandenbroek,e.poll}@cs.ru.nl
[2] Software Improvement Group, the Netherlands
b.vieira@sig.eu

Abstract. We consider the functional and security requirements for the information exchanges in the infrastructure for EV charging being trialled in the Netherlands, which includes support for congestion management using the smart charging protocol OSCP. We note that current solutions do not provide true end-to-end security, even if all communication links are secured (for instance with TLS), as some data is forwarded between multiple parties. We argue that securing the data itself rather than just securing the communication links is the best way to address security needs and provide end-to-end security.
Moreover, because of the number of parties involved and the fact that the precise roles of these parties are still evolving, we argue that more data-centric communication solutions, using pub/sub (publish/subscribe) middleware, may be better suited than using point-to-point communication links between all parties, given the flexibility and scalability provided by pub/sub middleware.

Key words: EV charging, congestion management, end-to-end security, smart grids

1 Introduction

The introduction of electric vehicles (EVs) brings important new requirements on the information and control architecture of the electricity grid. Information needs to be exchanged for billing but possibly also for congestion management. Charging EVs consumes a lot of electricity, a single charge of an EV consumes roughly the same amount of energy as the daily demand of 2 to 3 houses, so controlling it is an important means to manage the grid's limited capacity. Furthermore, EV charging may become an important factor in balancing supply and demand. All this means that EV charging introduces a lot of information flows, adding a lot of complexity to the ICT infrastructure behind the electricity grid. Moreover, it involves many parties, and involves some data with high security requirements, especially for data which is used in actively managing the grid.

Looking at the solutions currently being used or trialled in the Netherlands, this paper considers the security requirements for data exchanged in the grid to support EV charging in Section 3. Here we note that there are many parties involved in exchanging or forwarding such data. This makes ensuring end-to-end security important, as otherwise the parties involved in EV charging have to put a great deal of trust in one another. The importance of end-to-end security is also stressed by standards such as IEC 62351 [15] and NIST guidelines for Smart Grid Cyber Security [14].

We then suggest possible directions to improve the situation, both when it comes to securing information and organising the new information flows. For securing information, Section 4.1 discusses the possibilities to introducing security measures at the level of the data being exchanged, and not the communications links. This seems the natural way to achieve end-to-end security in situations where data is exchanged and forwarded between multiple parties. For organising information exchanges, Section 4.2 discusses the use of pub/sub (publish/subscribe) middleware as a solution to exchange data between many parties that is more flexible and scalable than introducing direct communication links between all parties involved.

These two solutions form a natural combination. Indeed, the middleware solution developed in the C-DAX project (`http://cdax.eu`) combines them in a pub/sub solution that provides end-to-end security tailored to smart grid applications.

Concrete starting points for this paper are the solutions that are being rolled out and/or trialled in the Netherlands, which are described in detail in Section 2. These include the OCPP protocol for the communication between charge spots and operators, which is rolled out nationally, and the OSCP protocol for congestion management (using so-called smart charging), which is being trialled. The authors of this paper were involved in a security evaluation and resulting security design of smart charging, using OSCP. The security design focussed on achieving end-to-end integrity of data. This security design is currently being integrated within the EV charging system in the Netherlands. Anticipating on the roll-out of the security design, this paper aims to point out the more generic security problems at the heart of (smart) EV charging and present some generic solutions.

The use of EVs is still in its infancy: some solutions are still at the trial stage and, more importantly, the market models for EV charging, and the roles of the (many!) parties involved, are not yet clear and still evolving. However, this will not change the basic communication needs and associated security requirements. It is clear that EV charging will involve multiple parties, and some communication between these parties with high security requirements, as it involves information needed for billing, information that is privacy-sensitive, and information needed to actively control the grid. So money, privacy, and – most importantly – the stability of the grid are at stake. So even though we look at the concrete protocols currently being used or trialled in the Netherlands, we hope our conclusions will be relevant for any solution for EV charging.

Scope This paper looks at EV charging from the grid perspective rather than the EV perspective. By this we mean that the focus is on the communication needs in the grid – between grid operators, charge spot operators, and energy suppliers – to manage EV charging, and we largely ignore the communication with the EV or its user.

Also, we will not consider the underlying physical networking infrastructure in the field, which may include PLC (Power Line Communication), cellular networks such as GPRS or LTE, or CDMA[1], or optic fibers for parts of the communication network. This underlying networking infrastructure may provide some security. For example, cellular networks will provide authentication and security at the transport level. Still, we believe that security solutions for the communication and information architecture needed to support EV charging should be designed to be independent of the underlying networking technologies. The infrastructure continues to evolve and change rapidly, and different grid operators are choosing different technologies. So, ideally solutions should not be tied to a particular networking technology, beyond imposing minimum bandwidth and latency requirements, or rely on security guarantees these technologies provide. Of course, such security guarantees are useful additional layers of defence (following the principle of 'defence in depth').

2 EV charging

This section makes an inventory of the information and communication needs for managing EV charging, the various parties involved, and the associated security requirements. This includes communication for billing and for management of the grid, in particular for congestion management.

We consider the set-up and protocols that are being used or trialled in the Netherlands, where there are public EV-charge spots where customers with the right subscriptions can charge their EV. Still, the communication needs and security requirements are more general, and largely independent on the particular set-up and protocols used: Any solution for EV charging that involves billing and some form of congestion management will have similar requirements.

Fig. 1 gives a schematic overview of the smart charging set-up in the Netherlands. The different parties or roles involved are described below.

- The *DSO (Distribution System Operator)* manages a regional electricity grid, and is responsible 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 a important role in the EV market, as they interact with the DSO and the EMSPs.

[1] Alliander, one of the larger DSOs in the Netherlands, is rolling out its own CDMA cellular network, dedicated to communication with their equipment in the field and possibly other critical infrastructures.

- 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.

Fig. 1 also includes the *Central Interoperability Register (CIR)*, which is an online customer database provided by the joint EMSPs, which can be queried by a charge spot (via the CSO) to see if a customer is allowed to charge his/her car.

The precise market models for EV charging are still in flux, and it is not yet clear which parties will play which role or roles. For example, some companies in the Netherlands play the role of both EMSP and CSO. One can also imagine that a DSO also plays the role of CSO.

One factor here are government goals of market liberalisation and fostering free competition in the energy sector: DSOs are natural monopolists in the region where they manage the grid, so there will be government regulations on what they are supposed to do and on what they are not allowed to do. However, such concerns may be in conflict with government aims to stimulate the use of EVs and roll-out of charge spots: as an important and resourceful party, DSOs may have to take the lead in some domains to encourage the use of EVs.

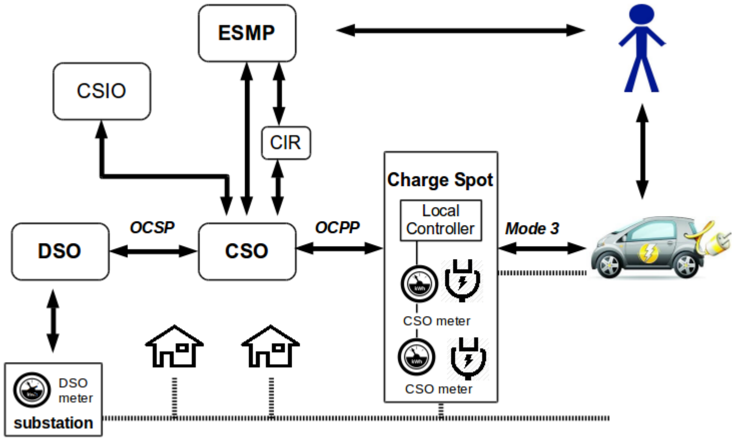

Fig. 1. Information flows for EV charging

We now turn to the physical infrastructure involved. The *charge spot (CS)* provides one or more sockets where EVs can be charged. A charge spot will include an electricity meter for each socket, which is owned by the DSO and controlled by the CSO. A charge spot or set of charge spots is managed by a *local controller* which has a communication link, for instance a GPRS connection, to the back-office of the CSO.

EV drivers with a subscription from an EMSP get an RFID card. A charge spot also contains an RFID reader, which is used to identify an EV-driver. When a charge starts, the charge cable is locked to the CS. The cable is only freed after identifying with the same RFID card that was used to start the charge.

Initially, charge spots in the Netherlands also contained a smart meter, similar to those placed in homes, which was under the direct control of the DSO, with its own GPRS connection. For cost reasons and size reasons (removing this additional meter allows for smaller charge spots) these smart meters are being phased out. New charge spots only have a traditional 'dumb' meter per socket, which communicates via a bus to the local controller. Even if the DSO no longer has a direct connection to a meter in a charge spot, it will have meters in the field, notably in the secondary sub-station that feeds a neighbourhood.

Each charging session is measured at the charge spot, and recorded at the CSO. The details (who charged how much, where and when) are then transmitted to the EMSP, who bills the customer. There are other billing chains, where energy providers bill the CSO for total consumption of its charge spots and the CSO bills the EMSP for charging of that EMSP's customers.

2.1 Protocols

EV charging in the Netherlands uses several internationally standardised protocols, incl. OCPP for communication with the charge spots by operators, and ISO 62196 Mode 3 for communication between EV and charge spot. A less standard solution being trialled in the Netherlands is the use of OSCP to dynamically control the capacity made available to charge spots for the purpose of congestion management. These protocols are discussed in more detail below.

Mode 3 ISO 62196 [9] standardises the charging of EVs, incl. the dimensions of different plugs and allowed current and voltage. It describes four possible modes for charging, of which the third describes EV charging at higher power stations. This specific connection is often referred to as Mode 3, and is supported by practically all currently available EVs.

There is a newer standard, ISO 15118 [10], that is essentially a successor of Mode 3. ISO 15118 still needs to see a wide roll-out, as hardly any EVs on the market support it. It includes several improvements, notably when it comes to security, as will be discussed later.

OCPP[2] The charge spot communicates with the CSO through the Open Charge Point Protocol (OCPP). OCPP standardises the communication between the charge spot and the party that operates the charge spot (i.e., the CSO), thereby allowing CSO back-ends and charge spots of different vendors to communicate (preventing vendor lock-in). As part of that, OCPP also allows for remote maintenance of charge spots by the CSO or CSIO through monitoring and firmware updates. It also offers features needed for congestion management, notably limiting the maximum capacity that a charge spot can deliver to an EV in a certain time slot.

[2] `http://www.ocppforum.net`.

OCPP is a SOAP-based protocol[3] originally designed by the E-Laad foundation (`http://www.e-laad.nl`), a foundation set up by the joint Dutch DSOs, but currently used by most countries that offer public charge stations. The current release is version 1.5; version 2.0 is under development.

OSCP[4] The large energy consumption of EVs poses a challenge for the electricity grid, given the limited capacity of the power lines at local level. OSCP (Open Smart Charging Protocol) allows a DSO to vary the capacity available to charge stations in time, given the varying predicted capacity needed for other consumers in an area.

This means that OSCP allows a DSO to do congestion management. Congestion management is about managing the limited capacity of the grid, given the physical infrastructure of transformers and cables, and sharing this capacity between charge spots, households, and commercial users in a neighbourhood.[5]

For congestion management, OSCP supports negotiation between a DSO and CSOs. The DSO creates a forecast, 24 hours in advance, for 15 minute intervals, on the power usage for each cable, based on historic measurement data and weather forecasts. The DSO then divides the forecast power usage among CSOs, again using historic data and contracted capacity. Using OSCP, each CSO is informed of its allotted capacity and the remaining spare capacity. The CSO can negotiate for more or less capacity, again using OSCP. The CSO then creates a charge plan for the charge spots, specifying the limit of the power they can supply per time slot, and transmits this to the charge spots using OCPP.

There is an important trust assumption here on the part of the DSO, that the CSO will not consume more energy than it negotiated, as there is no way for the DSO to limit the energy flow, other than a tripping safety breaker on the cable, which would stop the electricity supply to all consumers on this cable.

2.2 Security requirements

Any discussion of security is meaningless without considering the security requirements. A coarse classification in four overall security requirements can be made:

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

[3] A JSON over websockets version (version 1.6) of OCPP is currently being developed.

[4] `http://www.smartcharging.nl/smart-charging/open-smart-charging-protocol`

[5] Congestion management should not be confused which load balancing, which is about the more general issue of getting demand and supply in balance. The limited capacity of the grid is a (constant) factor here, but so is the variation in the supply of electricity – variation which will increase as there is more use of renewables (solar and wind power). So congestion management is always a local issue, and involves imposing limits on demand, whereas load balancing is also an issue on larger scale, and may involve influencing both demand and supply.

2. **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 also want 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 see later, some measures to ensure integrity (notably the use of secure tunnels) do not provide a practical means to support non-repudiation.
3. **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 user of an EV is typically a single person, such information will be personal information, and hence subject to legal requirements on the handling of personal information.
4. **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 customer information.

A more thorough evaluation of the security requirements, which would also involve the formulation of attacker models, is beyond the scope of the paper. Still, we do want to point out that EV charging introduces new players in the market, notably CSOs, that play an active part in congestion management and can affect the first security requirement above.

Here the introduction of smart EV charging seems to bring bigger risks than the introduction of smart metering. Smart meters also give new parties access to ICT infrastructure in the grid (for instance new service providers that read out metering data), but these are not meant to play an active part in managing the grid, as CSOs are expected to do in smart charging. Of course, this is not to say that smart meters are without risks to the availability of electricity, esp. if the smart meters allow consumers to be disconnected remotely [2]. A feature that was removed from smart meters in the Netherlands after a security evaluation.

Security risks can be mitigated at different levels: at the level of the ICT infrastructure, but also at the level of the application or service, as explained below.

1. At the level of the ICT infrastructure, risk to availability can be mitigated by redundancy, say by having back-up storage of critical data, or having a second communication link if a link fails. Risks to integrity and confidentially can be mitigated by various forms of access control, authentication, or the use of cryptographic checks, (i.e. digital signatures or message authentication codes (MACs) for integrity and encryption for confidentiality). Note that these are generic security measures, largely independent of the specific application. Of course, which measures and costs are reasonable will always depend of the specific application.
2. Independent of these more generic techniques at the level of the ICT infrastructure, it may also be possible to mitigate risk by more tailored measures at the level of the application. One such a measure is having fall-back scenarios. For example, when the management of the grid uses smart charging as a

way to do congestion management, there may be a fallback option on what to do if this system fails; a charge spot might have some default capacity that it will use in case it does not receive a dynamic capacity.

The security measures we discuss in the remainder of this paper will be of the former kind, but this does not mean one should overlook measures of the latter kind.

3 Security shortcomings

It appears that security considerations have not played a very prominent role in rolling out the public charge spots in the Netherlands, or indeed in the design of the OCPP protocol. The OSCP protocol is still under development and has had a security evaluation on an initial functional design. While not exactly security-by-design, the early inclusion of a security evaluation is already a marked improvement on the design of OSCP over OCPP. This security evaluation yielded several security issues, not just in the OSCP link, but in the whole EV-charging chain, as discussed in more detail below.

3.1 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 accept; 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 amount of time.

However, the weak authentication could be exploited to release the expensive charge cables, which in the Dutch setup are owned by the EV-driver.

3.2 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 summarise: TLS does provides 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 between 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.

4 More data-centric solutions

This section discusses directions 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 EV charging. These directions are related in that they revolve around letting the data itself, rather than the communication links, play a central role.

4.1 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. To illustrate the idea, we will first look at how integrity of meter readings in charging sessions is ensured in ISO 15118.

ISO 15118, the successor standard for Mode 3, provides built-in security measures that address some of the security concerns discussed in Section 3.2 above. In ISO 15118 metering data can be digitally signed by both the car and the charge spot. This means that the ultimate 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.

Note that 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. The fundamental difference is that the security is added to the data messages themselves, and not to the communication channels over which the data is transferred.

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 cryptographic mechanism: integrity of messages can be guaranteed using either digital signatures or MACs, and confidentially of messages can be handled by encryption.

These solutions overcome the limitations of generic secure tunnels discussed above in Section 3.2: 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.

4.2 More flexible architectures using pub/sub middleware

Adding security measures at the level of the data, as discussed above, rather than at the level of the communication links, opens up the possibility of using more flexible architectures to share data across multiple parties, as we will now discuss.

As shown in Fig. 1, the EV charging infrastructure requires a lot of communication links between various parties. In fact, the situation is more complex than Fig. 1 suggests: the figure only shows one DSO, CSO, EMSP, and one charge spot, whereas in reality there will be several DSOs, CSOs, and EMSPs, not to mention charge spots.

Organising communication links between all of these parties can be a challenge. One way to keep it manageable is to introduce some intermediaries or message brokers. Indeed, Fig. 1 already includes the CIR as a central intermediary acting on behalf of all EMSPs to allow a CSO to access client information irrespective of the EMSP.

A more structural way of organising information links between many parties is the use of a middleware solution such as pub/sub, short for publish/subscribe. This is a message-oriented middleware solution which provide a central 'data hub' that allows many parties to provide (aka publish) or receive (aka subscribe to) information.

Pub/sub middleware offers advantages of flexibility and scaling. It readily supports one-to-many communication as well as one-to-one communication. It does require a consistent data model to be shared between all parties, but in bilateral connections between individual parties data models have to be synchronised as well.

In the EU project C-DAX, a pub/sub information middleware solution [4] tailored to the smart grid has been developed. The solution has been inspired by and partially built on code of the earlier SeDAX system [11]. Although conceptually one can think of the C-DAX middleware as one central data cloud in which all the information is received and forwarded, as shown in Fig. 2, in reality this data cloud can be distributed over various geographical locations (for example to take into account bandwidth restrictions). Data may also be replicated across various locations to provide higher levels of resilience.

The C-DAX middleware also provides security mechanisms to provide confidentiality and/or integrity of messages, depending on the needs of the application, using either symmetric or asymmetric cryptography [8].

In using a pub/sub middleware solution to organise the information streams for EV charging there are still many configuration possibilities. For example, it may be useful to let EVs or their owners access data in the data cloud or provide data to the cloud. And instead of charge spots directly accessing the data cloud, one could also choose for a solution where they still only provide or obtain data via the responsible CSO.

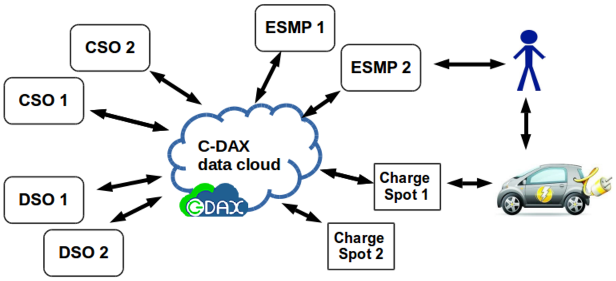

Fig. 2. C-DAX as pub/sub middleware for EV charging

5 Related work

Whereas we look at the communication infrastructure and associated security requirements from the grid perspective, most of the literature on the communication infrastructure for EV charging, such as [3], takes the EV perspective, and for instance considers ways in which EVs – or their drivers – could communicate with the grid and what information would then be exchanged.

The idea to use pub/sub middleware solutions for smart grid application is not new. An overview of middleware solutions for smart grid applications, including pub/sub solutions, is given in Section 6 of [1]. One of the pub/sub solutions discussed there, the SeDAX system [11], provided the starting point for the pub/sub solution developed in the C-DAX project.

This overview in [1] does not consider the specific scenario of EV charging. Rivera et al. do explore the use and advantages of pub/sub middleware for EV charging, for a more specific goal of optimising distributed EV charging [13].

6 Future work

The Dutch ElaadNL foundation is working on implementing a specific security design for smart charging, which focusses on end-to-end integrity of meter readings and stronger authentication of EV drivers.

We have not considered interaction with the user and/or the EV yet. This could be in the form of communication between the EV and the charge spot, to communicate wishes for charging, e.g. using ISO 15118 [10], but it could also involve communication between the user, e.g. using a smartphone app, and the EMSP.

One important aspect that we have not considered in this paper is privacy. How to take privacy into account in designing the overall information and communication infrastructure is an important issue. One interesting option to investigate is the use of privacy-friendly aggregation techniques as have been successfully applied for smart metering in homes [12, 5], where certain parties can then only see aggregate usage.

7 Conclusions

There were two observations that motivated us to write this paper. Firstly, we observed that the solutions that are being rolled out or trialled for EV charging do not provide true end-to-end security across the whole communication chain of the various parties involved. Given the small scale of EV charging, security may not be much of an issue yet, as the stakes involved are relatively small. But a danger is that retro-fitting security afterwards when these initiatives do grow to larger scales will be difficult. Indeed, it is widely recognised that it is best to practice Security by Design, and take security into account from the earliest stages of any design.

Secondly, we noted that when security is being considered, the security solutions largely relies on the use of secure communication tunnels. This is the case for both OCPP and OSCP. While using secure communication tunnels is a good step, and using standard solutions such as TLS is then the wise thing to do, it is important to realise that this may not take care of all security needs: as we argue in Section 3.2, TLS can secure a communication link between two parties, but it will not provide end-to-end security if data is forwarded between parties, and even when it is used between two parties it does not provide practical support for non-repudiation.

We considered two compatible directions for organising and securing the communication needs associated with EV charging: (i) adding security measures at the level of the data, and not just at the level of the communication links, discussed in Section 4.1, and (ii) using middleware solutions such as pub/sub that provide a more flexible way of connecting the many parties involved in EV charging, discussed in Section 4.2.

W.r.t. (i), given that the management of EV charging involves forwarding communication between multiple parties – including DSOs, CSOs and EMSPs – the right way to tackle security seems to be secure the data being exchanged, and not (just) secure the communication channels over which the data is communicated (e.g. using TLS). We were pleased to note that the newer ISO 15118 standard does provide security guarantees in this way, by having charging records digitally signed by both the charge spot and EV.

W.r.t. (ii), given the number of parties involved, and the fact their roles and business models are still evolving, solutions where all these parties have to bilaterally exchange data may not be practical. Having some central party to collect data and/or coordinate the exchange of data may be a more scalable approach. An interesting analogy here is the exchange of metering data. For this, the DSOs in the Netherlands have set up a joint organisation, called EDSN, to provide a central intermediary for exchanging metering data between DSOs and energy suppliers. EDSN was set up well before the introduction of smart meters, to facilitate billing by energy suppliers who have customers served by different DSOs. One can envisage a similar solution for the exchange of EV charging data. One way to realise this is through the use of pub/sub as a middleware solution. The pub/sub middleware solution developed in the EU FP7 project C-DAX demonstrates that such middleware solutions are feasible even in high-volume, low latency applications and with high guarantees for resilience [4].

Irrespective of whether the solutions we propose are ultimately the best or even feasible, a broader aim of this paper is to raise awareness and encourage debate about ICT and security issues surrounding EV charging. We have only discussed the way EV charging is organised in the Netherlands. Presumably there will be similar initiatives in other countries. By sharing information on how this is organised, there may be much that initiatives in different countries can learn from each other here.

Acknowledgements

The research of Fabian van den Broek and Bárbara Vieira has been supported by the European Community's Seventh Framework Programme FP7-ICT-2011-8 under grant agreement no. 318708 for the C-DAX project (`http://cdax.eu`). The authors alone are responsible for the content of this paper.

References

1. Ancillotti, E. and Bruno, R. and Conti, M.: The role of communication systems in smart grids: Architectures, technical solutions and research challenges. Computer Communications 36(17), 1665–1697 (2013)
2. Anderson, R. and Fuloria, S.: Who controls the off switch. In: International Conference on Smart Grid Communications (SmartGridComm). IEEE (2010)
3. Bayram, I. S. and Papapanagiotou, I.: A survey on communication technologies and requirements for internet of electric vehicles. EURASIP Journal on Wireless Communications and Networking 2014(1), 1–18 (2014)
4. Chai, W.K. and Wang, N. and Katsaros, K. V. and Kamel, G. and Melis, S. and Hoefling, M. and Vieira, B. and Romano, P. and Sarri, S. and Tsegay, T. and Yang, B. and Heimgaertner, F. and Pignati, M. and Paolone, M. and Develder, C. and Menth, M. and Pavlou, G. and Poll, E. and Mampaey, M and Bontius, H.: An information-centric communication infrastructure for real-time state estimation of active distribution networks. IEEE Transactions on Smart Grid (2015), to appear
5. Defend, B. and Kursawe, K.: Implementation of privacy-friendly aggregation for the smart grid. In: ACM workshop on Smart energy grid security. ACM (2013)
6. Engelhardt, M., Pfeiffer, F., Finkenzeller, K., Biebl, E.: Extending ISO/IEC 14443 Type A eavesdropping range using higher harmonics. In: SmartSysTech 2013. pp. 1–8. IEEE (2013)
7. Habraken, R. and Dolron, P. and Poll, E. and De Ruiter, J.: An RFID skimming gate using Higher Harmonics. In: RFIDsec 2015. Springer (2015)
8. Heimgaertner, F. and Hoefling, M. and Vieira, B. and Poll, E. and M. Menth, M. : A security architecture for the publish/subscribe C-DAX middleware. In: IoT/CPS-Security (IEEE ICC 2015). IEEE (2015), to appear
9. IEC 62196: Plugs, socket-outlets, vehicle couplers and vehicle inlets - conductive charging of electric vehicles (2003)
10. ISO/TC 22/SC 31 (Road Vehicles/Data communication): ISO 15118: Road vehicles - vehicle to grid communication interface. Tech. rep., ISO (2013)
11. Kim, Y.-J. and Lee, J. and Atkinson, G. and Kim, H. and Thottan, M.: SeDAX: A scalable, resilient, and secure platform for smart grid communications. Selected Areas in Communications, IEEE Journal on 30(6), 1119–1136 (2012)
12. Kursawe, K. and Danezis, G. and Kohlweiss, M.: Privacy-friendly aggregation for the smart-grid. In: Privacy Enhancing Technologies. pp. 175–191. Springer (2011)
13. Rivera, J. and Jergler, M. and Stoimenov, A. and Goebel, C. and Jacobsen, H.-A.: Using publish/subscribe middleware for distributed EV charging optimization. Computer Science-Research and Development pp. 1–8 (2014)
14. The Smart Grid Interoperability Panel Cyber Security Working Group: Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security (September 2010)
15. WG15 of IEC TC57: IEC 62351: Power systems management and associated information exchange data and communications security (2007)