EVS27
Barcelona, Spain, November 17 - 20, 2013

Impact of a Smart Grid to the Electric Vehicle Ecosystem From a Privacy and Security Perspective

Christophe Jouvray[1], Gloria Pellischek[2], and Mourad Tiguercha[1]
[1]*TRIALOG. 25 rue du Gnral Foy, 75008 Paris. France. christophe.jouvray@trialog.com*
[2]*ERPC.Beerengarten 14, 86938 Schondorf. Germany. g.pellischek@erpc-gmbh.com*

Abstract

In intelligent transport systems, connectivity of vehicle is the main feature for improving services to the driver and passengers. In Electric Vehicle domain, permanent connectivity is paramount in order to compensate both the limited range and to achieve an effective grid inclusion enabling the availability of electric energy everywhere anytime.

The objective of this paper is to present the risk on privacy due to the continuous connectivity between EVs and a smart grid. Privacy is composed of different viewpoints such as technical but also legal and socio-ethical.

Keywords: Smart Grids, Electric Vehicle, Security, Privacy, TVRA (Threat Vulnerability Risk Analysis), Common Criteria

1 Introduction

Due to environment concern, Electric Vehicles (EV) are becoming an increasingly important market. Permanent connectivity is paramount in order to compensate both the limited range and to achieve an effective grid inclusion. The energy domain is currently integrating this new market in their model. Indeed, EVs fundamentally change the current business model since charge and discharge feature is available.

From a technical point of view, data exchanges are needed between EVs and smart grids. Unfortunately, this new architecture raises security and privacy issues which, if left unaddressed, could jeopardise the wider deployment of ITS. For example, location-based services may in combining location information and personal data have possible implications for personal privacy. There may also be security vulnerabilities in electronics and communications systems. ITS technologies must ensure the integrity, confidentiality and secure handling of data, including personal and financial details, and show that citizens rights are fully protected. A second legal cornerstone to be taken into account in this paper is therefore the European legal framework for privacy and personal data protection. The main challenge of this paper is twofold: (i) presenting the key legal changes and (ii) identifying potential issues and attacks.

Performing a security analysis requires a suitable process. In the context of this paper, the TVRA (Threat Vulnerability Risk Analysis)method [9] has been selected. Different steps has to be done: (1) define the security environment (i.e., target of evaluation, the assets), (2) point out the security objectives and requirements (3) identification of the vulnerabilities (4) measure the likelihood (5) calculation of the likelihood (6) establishment of the risk and finally (7) define security countermeasures and evaluate their benefit.

The structure of this paper follows the TVRA method with one section which relates a status of current regulation. Section 3 presents the scope of the security analysis. For this purpose, a use case is defined. Security requirements related to the target of evaluation are detailed in Section 4. European Commission offers a legal framework in order to ensure privacy. Current regulations are detailed in Section 2. Finally, Section 5 points out security and privacy issues in the current situation.

2 Legal Framework for Privacy

European Union law and its application have always been inspired by the fundamental rights contained in international instruments, as repeatedly recognized by the Court of Justice of the European Union (the Court of Justice or ECJ).
The fundamental rights as laid down in the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR or the Convention) have in particular been a key source of inspiration for the general principles of EU law. Fundamental rights contained in international treaties, such as the rights of the Convention take in many countries precedence over national law.
Another and most important element to note is the incorporation of fundamental rights in Union law and the accession of the Union to the Convention since the 1st of December 2009.

2.1 ITS Legal Framework

On the 6th of August 2010 Directive 2010/40/EU was published in the Official Journal of the European Union. This Directive is entitled: Directive 2010/40/EU of the European Parliament and the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for the interface with other modes of transport. As is clear from the name, the Directive is a framework Directive for the deployment of ITS in Europe. ITS, for the purposes of the Directive, refers to the application of information and communication technologies in the field of road transport and its interfaces with other modes of transport. The Directive distinguishes between ITS applications and services. An ITS application is an operational instrument for the use of ITS. An ITS service is defined as the provision of an ITS application through a well-defined organizational and operational framework with the aim of contributing to user safety, efficiency, comfort and/or to facilitate or support transport and travel operations.

2.2 Art. 8 European Convention of Human Rights

The right to respect for ones private and family life is listed as one of the human rights and fundamental freedoms in the European Convention for the Protection of Human Rights and Fundamental Freedoms (”ECHR” or the ”Convention”) concluded in 1950 in the framework of the Council of Europe (”CoE”) in Article 8.
There is no doubt that the introduction of ITS in the Member States needs to fulfil the requirements of Article 8 ECHR. This means in particular that every individual EU citizen can potentially invoke this Article if he or she estimates that the introduction of a specific ITS (CS identification, navigation, e-roaming and -payment etc.) violates his/her privacy rights, for example, because the processing of personal information by the system goes further than what is necessary in a democratic society.

2.3 Charter of Fundamental Rights of the European Union

A new and most important step in the affirmation of the importance of the fundamental rights for the EU has been the adoption of the ”EU Charter of Fundamental Rights” (”EU Charter”).
The EU Charter sets out a whole range of civil, political and social rights enjoyed by the EUs citizens. It states in Article 7 that ”everyone has the right to respect for his or her private and family life, home and communications and codifies in Article 8a fundamental right to protection of personal data. The fundamental rights proclaimed in the EU Charter were, with a number of amendments, incorporated in EU law as primary law with full legal value by the Treaty of Lisbon (Article 6 (1) of the TEU).
The Treaty of Lisbon also amends two core treaties of the EU, i.e. the Treaty on European Union (TEU) (sometimes also referred to as the Maastricht Treaty) and the Treaty establishing the European Community (TEC) being presently renamed as the Treaty on the Functioning of the European Union (TFEU). The Treaty of Lisbon was signed on 13 December 2007 and took after the ratification by all Member States effect on the 1st of December 2009.

2.4 European Union Data Protection Framework

Directive 95/46/EC (the Data Protection Directive or ”Directive 95/46/EC”) is the basis for the data protection legislation of all the European Union countries. The Directive 2002/58/EC (the ”e-Communications Privacy Directive” or ”Directive 2002/58/EC”), as amended, is of importance as well, more in particular for data protection in the domain of publicly available electronic communications services.
In data protection law, crucial concepts are *personal data*, *controller* and *processor*.
Personal data is any information that relates to an identified or identifiable natural person. It is evident that this definition can lead to various interpretations. Therefore the Article 29 Data Protection Working Party has issued an opinion regarding the concept of personal Data.
The Article 29 Working Party explains in its opinion the notions of a person that is *identified* and of a person that is *identifiable*. The Working Party understands identified in general terms. It considers a person as identified if that person is distinguished within a group of persons from all the other members of the group.
Directive 95/46/EC says that we must take into account all means likely reasonably to be used to identify a person by the controller or a third party. The Article 29 Working Party gave in its Opinion a clarification on this aspect. For assessing *all the means likely reasonably to be used to identify a*

person, as it is worded in Recital 26 of the Directive 95/46/EC, the Article 29 Working Party stated that *all relevant factors shall be taken into account, including not only the cost of conducting identification, but also the intended purpose, the way the processing is structured, the advantages expected by the controller and the interests at stake of the data subjects, as well as the risks of organisational (breaches of confidentiality duties) and technical dysfunctions*.

In the terminology of Directive 95/46/EC the accountable entity (natural or legal person, or any other body) for processing personal data is called ***the controller***. The controller is the person deciding the goals and means of a particular data processing operation.

A ***processor*** is anybody that processes data on behalf of the controller. He is a subcontractor of the controller so to say, charged with executing the data processing operation as a whole or in part.

Very often it is difficult to distinguish between controllers and processors. Take the example of a car repair shop processing data in the context of a remote diagnosis system and therefore using a specialised service provider operating under a contract with the car manufacturer.

The problem is that the qualification of an entity as either a controller or a processor has significant implications. These implications are situated at mainly three levels: the allocation of responsibility and risk, the determination of applicable law, and compliance with the substantive provisions of the Directive.

Given these implications, it is essential to be able to determine which role an entity has assumed towards a particular processing operation. The distribution of responsibility and liability among controllers and processors results from a combination of several provisions. As far as the controllers obligations are concerned, the allocation of responsibility is in first instance the result of article 6(2) of the Directive.

The qualification of an actor as either a controller or a processor is also an essential element in determining which law(s) applies (apply) to a processing operation or set of processing operations. Article 4 (1) sets forth the various instances in which a Member State must apply the national laws it has adopted when implementing the Directive. Each of these instances hinges, to a greater or lesser extent, upon the location in which the controller is established.

However, the qualification of an actor as a processor can also be determinative in deciding which law to apply to a particular processing operation. Article 17 (3) provides that the scope of the security obligations (which shall be incumbent upon the processor by virtue of the contract which is to be concluded among controllers and processors) shall be determined by the national law of the Member State where the processor is established.

As a result, both concepts are pivotal in determining the scope of data protection legislation, not only by reason of the type of entity concerned but also when determining the applicability of national provisions.

Although the qualification of an actor as a processor or a (co)controller is consequently crucial, it will in particular in the context of examples as the one mentioned above related to a remote diagnosis system not be easy to establish. In the view of the WP29 each party taking in charge an essential contribution to the data processing chain should be considered as a (co)controller. Specifically, joint control shall arise whenever ”different parties determine with regard to specific processing operations either the purpose or those essential elements of the means which characterise a controller”.

2.5 Emerging Legislation

In the European Union the protection of personal data is a fundamental right and it is a political imperative, since Data Protection is part of EU’s constitutional Framework. Emerging new technologies call for the implementation of an enhanced data protection framework and the respective enforcement strategy in order to keep the leading edge in data protection and to remove bureaucratic obstacles.

In 2012, the Commission proposed a major reform of the EU legal framework on the protection of personal data along the baseline: (i) protecting your personal data and (ii) the free flow of personal data. The new proposals will strengthen individual rights and tackle the challenges of globalisation and new technologies.

The Commission proposes one, single, technologically neutral and future-proof set of rules across the EU. This means that regardless of how technology and the digital environment develop in the future, the personal information of individuals in the EU will be secure, and their fundamental right to data protection respected.

The Commission will also reinforce the right to be forgotten, so that if an individual no longer wants their personal data to be processed, and there is no legitimate reason for an organisation to keep it, it must be removed from their system. Citizens will also have a right to data portability, i.e. the right to obtain a copy of their data from one company (e.g. Internet Service Provider, etc.) and to transmit it to another one without hindrance from the first company. These proposals will help build trust in the online environment, which is good for individuals and businesses.

Key changes relative to the current situation are still needed:

- Guaranteeing easy access to ones own data and the freedom to transfer personal data from one service provider to another.

- Establishing the right to be forgotten to help people better manage data protection risks online.

- Ensuring that whenever the consent of the individual is required for the processing of their personal data, it is always given explicitly.

- Ensuring a single set of rules applicable across the EU and clear ruled applied to data controllers outside the EU

3 Target of Evaluation

A fleet of Electric Vehicle (EV) is the main stakeholder addressed by this paper. Indeed, modern automotive systems contain critical private information regarding the driver and/or the passengers (e.g., identities, banking information, address book, etc). This is accentuated since mobile phone can be connected to the vehicle. Private or sensible data can be shared with other parties. This section presents a use case with charging and reverse charging scenarios. For this purpose, EVs are grouped into fleets and interacts with the energy world. A use case presenting the main assets and the communication interfaces is specified in the following.

3.1 Use Case Definition

Figure 1 presents how a fleet of electric vehicles interacts with the smart grids and OEM servers. The V2G (Vehicle to Grid) link allows charging and reverse charging of the vehicle. In order to authorize energy transactions, electric vehicles have interactions with OEM servers which negotiate with the smart grid. All of these roles are more detailed in Section 3.2.

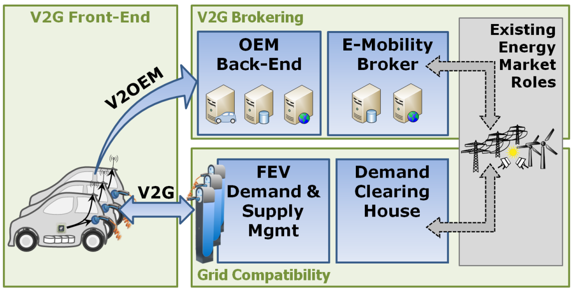

Figure 1: Required Infrastructure for Connecting a Smart Grid and a Fleet of Electric Vehicles

From the energy stakeholder, a broker is in charge of providing a charge profile for all the fleets.

3.2 Target of Evaluation and Assets

This analysis is build over three main assets:

- the fleet of EVs. The main characteristic of this use case is the flexibility provided by each electric vehicle. In particular, electric vehicle can (i) delay its own charging or (ii) provide its energy to the market (i.e., reverse charging). This asset corresponds to the target of evaluation. External parties will interact with this element. However, for privacy reasons, these third parties are considered in the analysis for measuring the privacy leakage.

- the OEM back-end. The energy flexibility offered by the fleet can be negotiated with a broker. This asset is in charge of this tradeoff. In order to have a bigger position, the OEM back-end aggregates all data of the full fleet. Indeed, in this paper, for simplification reason, the roles of OEM back-end and fleet manager are merged. The E-Mobility Broker is in charge of merging all power needs (several fleets) and to create a charge profile (i.e., agreement of energy transfert and prices). It is therefor possible to consider that merged data of all EVS are anonymized. Indeed, since it is impossible to find information specific to one vehicle, there is no data privacy issue.

- the charge spots. This kind of asset corresponds to the physical link between an EV and the energy market. Every charge spot is connected to a demand and supply manager (DSM). A DSM is in charge of providing the energy to each spot. Finally, the DSM gets orders from the demand clearing house which negotiates the prices and the charge profiles with the E-Mobility Broker.

The target of evaluation is the electric vehicle. Figure 2 explains the usual architecture of an electric vehicle which has to manage the energy and OEM back-end parts. Two different ECUs (Electronic Control Unit) are dedicated to these features. As any ECU inside a car, it is linked to the full electronic architecture by a CAN (Controller Area Network) bus. Over this connection, each ECU is abble to get vehicle properties (represented by the *Vehicle Control Manager* in Figure 2).

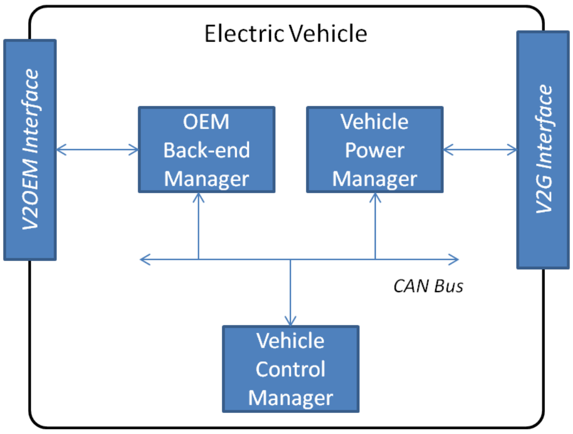

Figure 2: Overview of the Internal Architecture of an Electric Vehicle

3.3 Interfaces

As shown in Figure 2, an electric vehicle offers two different interfaces to external parties: V2G and V2OEM.

The communication between the electric car and charge spot (V2G Interface) is normalized by the ISO/IEC 15118 interface [4, 5]. Since private data are exchanged through this connexion, the security on transport layer used in the standard is provided by TLS [5]. The ISO/IEC 15118 uses power line based communications and the wireless module use 2G or 3G. Regarding the protocol between the EV and the OEM server, proprietary solutions are used. However, the ISO/IEC 15118 strongly recommends also using TLS [4].
The second interface is called V2OEM (Vehicle 2 OEM) which allows data exchange between a vehicle or fleet and an OEM back-end. There is no specific standard in this area. However, webservices based approach is an appropriate way.

4 Security and Privacy Requirements

According to [7], security can be considered with different viewpoints: confidentiality, integrity and authenticity. However, many security experts also consider availability and accountability for describing security. CIAAA (Confidentiality, Integrity, Authenticity, Availability and Accountability) corresponds to a technical vision which can be enforced by privacy aspect. **Privacy** [8] is the ability of an individual to be left alone, out of public view, and in control of information about oneself. One can distinguish the ability to prevent intrusion in ones physical space (”physical privacy”, for example with regard to the protection of the private home) and the ability to control the collection and sharing of information about oneself (”informational privacy”). The concept of privacy therefore overlaps, but does not coincide, with the concept of data protection.

Confidentiality is the ability to avoid the read of non-authorized parties. For instance, vehicle data pushed over the V2OEM interface has to be confidential. Similarly, when a vehicle is setting up a charge, bank account or contract number has to be protected. Since private data can be exchanged among the EV, the smart grid and the OEM servers, confidentiality has to be ensured. Moreover, for privacy reasons, data has to be annotated with policies for avoiding personal information to a tierce person.

Integrity aims at protecting the data exchange and data storage (including the operating system).

Authenticity is a main requirement in the use case presented in Figure 1. Indeed, charging and discharging features requires authenticity property for billing issues. Of course, authentication mechanisms have to be implemented in order to check the identity of the vehicle or driver. ***Non-repudiation*** is also a security property which is often associated to authenicity. The objective of non-repudiation is to avoid the risk of an asset composing the system which denies an action. For billing reason, non-repudiation is also a critical security property.

Availability has to be ensured in order to be able to send data through the V2OEM interface or to allow the charge of vehicle at any time.

Finally, ***accountability*** is a way to provide some evidences of security or privacy policies. In particular, non- repudiation mechanisms is a good way for identifying a sender. This property is crucial for billing aspects.

Through the two interfaces, data (private or not) are exchanged. According to the privacy policies, some mechanisms have to ensure the security properties associated to all data.

For the ISO/IEC 15118.X, the EV and the CS use a protocole. All functions sent by the EV finished by *req*, and, respectively, *res* for CS to EV messages.

In Table 1, all functions defined by the 15118 standard are listed. For all of them, we detail the security level. In this protocole, only few data are private (e.g., account number or EMAID). It means that confidentiality is not essential. However, data integrity and authenticity is crucial all along of data exchange.

List of all 15118 Services	**Confidentiality**	**Integrity**	**Authenticity**	**Non-repudiation**	**Availability**
supportedAppProtocolReq	L	M	M	L	L
supportedAppProtocolRes	L	M	M	L	L
sessionSetupReq	L	M	M	L	L
sessionSetupRes	L	M	M	L	L
serviceDiscoveryReq	L	M	M	L	L
serviceDiscoveryRes	L	M	M	L	L
serviceDetailReq	L	M	M	L	L
serviceDetailRes	L	M	M	L	L
servicePaymentSelectionReq	L	M	M	L	L
service PaymentSelectionRes	L	M	M	L	L
paymentDetailsReq	H	H	M	L	L
paymentDetailsRes	L	M	M	L	L
chargeAuthorizationReq	L	M	M	L	L
chargeAuthorizationRes	L	M	M	L	L
chargeParameterDiscoveryReq	L	M	M	L	L
chargeParameterDiscoveryRes	M	H	M	L	L
powerDeliveryReq	L	M	M	L	L
powerDeliveryRes	L	M	M	L	L
certificateUpdateReq	L	M	M	L	L
certificateUpdateRes	L	M	M	L	L
certificateInstallationReq	L	M	M	L	L
certificateInstallationRes	L	M	M	L	L
sessionStopReq	L	M	M	L	L
sessionStopRes	L	M	M	L	L
chargingStatusReq	L	H	H	H	L
chargingStatusRes	L	H	H	H	L
meteringReceiptReq	L	M	M	L	L
meteringReceiptRes	L	M	M	L	L
cableCheckReq	L	M	M	L	L
cableCheckRes	L	M	M	L	L
prechargeReq	L	M	M	L	L
prechargeRes	L	M	M	L	L
currentDemandReq	L	M	M	L	L
currentDemandRes	L	M	M	L	L
weldingDetectionReq	L	M	M	L	L
weldingDetectionRes	L	M	M	L	L

Table 1: Security Requirement Levels (Low, Medium, or High) for ISO/IEC 15118 services

Regarding the V2OEM interface, data exchanged are not standardized yet. In the context of the eDASH project, partners have identified some services in order to develop an OEM back-end server which provides some charge profile requirements to the broker. For this purpose, the OEM back-end server has to get at least vehicle identify, location and charge requests. As mentioned in Table 2, a failure inside the system can have an important impact regarding privacy issues.

Description	Possible Data Protection & Privacy Issues
Over-the-wire connection between FEV and CS, exchange of charging data	(i) Vehicle identity (ii) Sequential past, present and predicted future position/time data (iii) Exposure of any data held on vehicle
User CS Communication by entering personal/personizable data	(i) Credit Card or ID Card details revealed (ii) Tracking and Tracing of user
The Metering Operator is a natural or juristic person that accompanies the metering of electric energy at a give point on request of the concerned customer	(i) The Metering Operator gets hold of vehicle or personal ID numbers, which may lead to tracking and tracing
V2G over the air interface (Cellular) mobile communication of charge session independency: (i) Predetermination of individual demands, and (ii) Enriched set of OEM-specific information compared to V2G	(i) Received information only, but could perhaps be exploited by malicious users (ii) Sequential past, present and predicted future position/time data (iii) Vehicle identity (iv) Link between vehicle and mobile device that could be used to identify user (v) Personal information about the user
Consolidation of OEM related data provides new potentials for FEV fleets. Support of balancing power: Demand/Response & Charge schedule optimization based on predeterminations & fleet patterns.	(i) Vehicle identity (ii) Sequential past, present and predicted future position/time data
Brokering of tariffs and incentives for user awareness of charge optimization needs Authentication & Authorization, Financial balancing issues	(i) Payment contract identity (ii) Vehicle identity (iii) Sequential past and present position/time data

Table 2: Summary of Possible Data Protection and Privacy Issues Affecting EV/Smart Grid Architecture

5 Security and Privacy Risks

The goal of this section is to present privacy and security leakages. In order to achieve this goal, authors have used the TVRA (Threat, Vulnerability and Risk Analysis) method defined by ETSI [9]. Indeed, this method allows identifying security threats and their countermeasures.

Considering security threats is complex in large-scale systems such as presented in this paper. Understanding the goal of an attacker and the different ways to launch an attack seems crucial. In this context, we have followed the STRIDE threat model proposed by Microsoft [10]. STRIDE helps in classifying the threats with several vectors (spoofing, tampering, repudiation, denial of service, elevation of privilege).

5.1 Potential Privacy Leakage

Table 2 summarizes the private data which can be compromised if an attacker successfully makes an attack.

5.2 Threats and Vulnerabilities of the V2G Interface

As mentioned in Figure 1, VEs is connected to third parties by two different interfaces: V2OEM and V2G. Since only V2G interface is normalized, the following paragraphs highlights attacks for this interface. However, it is important to note that some usual attacks can be applied to the V2G interface. More information can be find in the related papers [1, 2, 3].

5.2.1 Formulas for measuring the risk

As defined in the TVRA method, the risk encountered by the system is measured by the likelihood and the impact. And, the likelihood is a composition of the material for mounting the attack (i.e., needed attacker knowledge, tooling, etc) and the motivation.

The vulnerability is the weakness of an asset or group of assets that can be exploited by one or more threats as presented:

$$\begin{aligned} Vulnerability &= Opportunity + Knowledge \\ &\quad + Expertise + Equipment \\ &\quad + Time \end{aligned}$$

In order to measure the weakness, some factors are taken into account:

- Opportunity: This parameter points out the time window needed to analyse the asset or the system under attack.
- Knowledge: It corresponds to the specific expertise on the asset which will be compromised needed for the attack.
- Expertise: This factor refers to the level of expertise required in order to mount an attack (i.e., laymen, proficient, expert).
- Equipment: Hardware or software can be required in order to exploit a vulnerability. Standard, specialized or bespoke equipment can be used.

- Time: This factor corresponds to the evaluation of the total amount of time taken by an attacker.

Each parameter composing the vulnerability formula is associated to some values. According to the total mount of the vulnerability, the likelihood is given (i.e., unlikely, possible, or likely). Finally, the risk is given by mixing the occurrence likelihood and the impact (i.e., combinaison of the asset impact and the attack intensity). $Risk = OccurenceLikelihood \times Impact$

5.2.2 Identification of the threats

In this section, all threat are described. An identifiant is setup for each threat and is used in the rest of the document.

TH1: Reuse a contract. This threat exploits the sleep mode. An EV can switch to a sleep mode (e.g., waiting for the charging). If the attacker unplugs the cable, it is able to reuse the contact of the slept EV. This attack relies on the SessionSetup service.

TH2: Malicious Services. The ServiceDiscovery function allows EVs to discover all services provided by the charging spots. Thanks to a man in the middle base attack it is possible to forecast malicious services like:

- DC charge only while the charging spot is in AC mode
- Update a malicious vehicle firmware (i.e., in particular by updating a FTP address)
- Update or install malicious certificate

Actually, this kind of attack due to the VAS (Value Added Service) principle is possible. If a vehicle detects a service with a better VAS level, it will select the malicious service.

TH3: Reinject Payment Details. The service PaymentDetailReq provides information regarding the body. By a replay attack it is possible to reuse the payment body. The ISO/IEC 15118 protocol has defined a process in order to check the identity. Indeed, a challenge can be requested by the charging spot requiring the EV private key. By consequence, an attacker without the private key can not realise the challenge. However, while this feature is not mandatory, this attack vector is still possible.

TH4: Certificate Management. The ISO/IEC 15118 standard has defined several services for managing certificates (in particular for updating or installing certificates. By using the threat TH2, it is already possible to use malicious services in order to break the certificate chain. Moreover, it is also to get private information through these services (in particular vehicle information). Thanks to information vehicle, it is then possible to launch car maker dependant attacks. This threat can be considered as an initial phase for a bigger attack.

TH5: Modification of Charge Parameters. The parameters of the charge exchanged between the EV and the CS are managed by the ChargeParameterDiscovery services. DOS (Denial Of Service) attack can damaged the quality of the service (e.g., delay a charge, destroy equipment due to bad values, etc). Moreover, due to man in the middle attack, it is possible to modify fees (i.e., modifying the receipt or avoiding a charge due to expensive rates).

TH6: Modification of the Charging Plan. The PowerDeliveryReq provides the charging plan. By a denial of service attack, it is possible to tamper the charging service (e.g., slow charging, avoid the charging).

TH7: Spoofing the Charging Status. When the electric vehicle switches to the charging mode, an infinite loop starts between the EV and the charging spot. By spoofing the data (i.e., meters), it is possible to reduce the quality of service.

TH8: Spoofing the Cable Check. A service is dedicated to the check of a cable. By spoofing data, it is possible to cancel the charge of a vehicle.

TH9: Key Exchange at MAC layer. The MAC layer is described in the standard ISO/IEC 15118-3 [6]. During the communication initialisation, a key exchange is done. If the attacker is present since the beginning, he is able to get all the keys since they are not encrypted. This thread is critical since this vulnerability highlights that all of the other attacks are possible.
The ISO/IEC 15118 standard relies on PLC protocol. For this reason, all threats based on this protocol can be applied to the system.

TH10: PLC Jamming. Electromagnetic field perturbations can damage the communications. It is a DOS (Denial Of Service) attack based technique.

TH11: PLC Radiation. PLC communications have a radiation radius. It is possible to wirelessly capture data. This threat can be coupled with the threat TH9 in order to get the MAC keys. Then, it is possible to launch all other attacks.
Some attacks are frequently used by the attackers. These attacks are fully generic and can be applied in this context.

TH12: Reuse of Material. The attacker can reuse material from one EV to another one. For instance, it can move the energy management system inside the professional vehicle to its own vehicle. In that case, the business contract will be use for charging an external vehicle.

TH13: Malicious Material. The attacker can use malicious material for launching an attack. For instance, he can use a customized ECU inside the electric vehicle, modify the cable, or replace some equipment inside the charging spot.

TH14: Retention of Compromised Asset. Relying on software, communication stacks, or compromised private keys, security issues can be discovered. For this reason, all software has to be updated to the last version. If updates are not applied, threats can be exploited by attackers.

ID	S	T	R	I	D	E
ISO/IEC 15118 related threats						
TH1	Y	N	N	N	N	Y
TH2	N	N	N	Y	Y	Y
TH3	Y	Y	N	N	N	N
TH4	Y	N	N	N	N	N
TH5	Y	Y	N	N	Y	Y
TH6	Y	N	N	Y	Y	Y
TH7	N	Y	N	Y	Y	N
TH8	N	Y	N	Y	Y	N
TH9	Y	Y	Y	Y	Y	Y
PLC related threats						
TH10	N	N	N	N	Y	N
TH11	N	N	N	Y	N	N
Traditional threats						
TH12	Y	N	Y	N	N	N
TH13	Y	N	Y	N	N	N
TH14	Y	Y	Y	Y	Y	Y

Table 3: Characterization of the treats with the STRIDE terminology

5.2.3 Measurement of the risk

Table 4 evaluates the risk encountered by the system for all identified threats.

5.3 Possible Countermeasures

In order to reduce the risk encountered by the system, it is possible to apply some countermeasures. The following list summarizes the main countermeasures:

C1: Check the identity. Spoofing the identity is an attack which can be applied to this use case. Controlling the identity by some challenges based on certificates seems critical.

C2: Use end to end communication. Security has to be applied at every level of the ISO communication stack. In particular, as defined in the ISO/DIS 15118.3 [6], the key exchange at the MAC level must no be done without protection.

C3: Use secure protected memory. Private keys, contract information, or all private data have to be stored a secure memory which avoids tampering attacks.

C4: Check the authenticity of all services. Fake services can be proposed by an attacker. EVs have to check the identity of the provided before selecting a service.

C5: Use cable with good level of protection against electromagnetic fields. PLC can be damaged by electromagnetic fields. For this reason, it is necessary to use cables which guarantee a good quality of service even if the environment is polluted.

C6: Use a secure boot. An attacker can replace equipment or software in the systems. This kind of attack can be avoided by using secure boot mechanisms.

C7: Update software with the last versions. Some new hacks and leaks are found everyday. For this reason, it is essential to install the last versions of all software elements.

In order to evaluate the benefit of a countermeasure, the risk is measured once again. The difference between the risk values gives the cost benefit (see Table 4).

5.4 Comments on V2OEM Interface

V2OEM interface is not standardized yet. However, it will be based on ITS (Intelligent Transport Systems) techniques like web services (e.g., in particular using REST protocol). In order to provide added value services, private data like location, vehicle identifiant has to be used. In the literature, [1, 2, 3] already made some security analysis of modern automotive or ITS systems. For instance, installation of malicious unit and or software, GPS spoofing are well-known possible attacks. As stated in Section 5.2, some of them can be applied to the V2G interface.
It is important to note that these attacks use the permanent connection of the car. Due to the lack of protection inside a vehicle, an attack can have an important consequence on the safety. Actually, the CAN bus can forward malicious data.

6 Conclusion

Electric cars is launching a new revolution in the automotive domain. These cars request a new suitable infrastructure. For this reason, it is mandatory to add new communication channels in the car in order to communicate with the infrastructure. However, privacy and security leakages has to be considered. This paper has presented a risk analysis in order to evaluate the potential attacks. 14 threats have been identified and some countermeasure has also be proposed in order to reduce the risk encountered by the system. Finally, current legal framework is not suitable with these new technologies. This paper has presented a status of the current situation. In particular, authors point out the emerging legislation.

Acknowledgments

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n 285586. Authors want to thanks all partner from the e-DASH Project.

References

[1] K. Koscher, A. Czeskis, F. Roesner, S. Patel, and T. Kohno. Experimental Security Analysis of a Modern Automobile. SP '10 Proceedings of the 2010 IEEE Symposium on Security and Privacy. pp 447-462. Washington, DC, USA. 2010.

[2] S. Checkoway, D. McCoy, B. Kantor, K. Koscher, A. Czeskis, F. Roesner, T. Kohno. Comprehensive Experimental Analyses of Automotive Attack Surfaces. SEC'11 Proceedings of the 20th USENIX conference on Security. CA, USA. 2011

[3] R. Moalla, B. Lonc, H. Labiod, and N. Simoni. Risk Analysis of ITS Communication Architecture. Third International Conference on the Network of the Future (NOF). pp 1-5. 21-23 Nov. 2012. Tunis, Tunisia. 2012.

[4] International Organization for Standardization, Road Vehicles Vehicle-to-Grid Communication Interface Part 1: General Information and Use-Case Definition, ISO/IEC DIS 15118-1: 2012-06

[5] International Organization for Standardization, Road Vehicles Vehicle-to-Grid Communication Interface Part 2: Technical Protocol Description and Open Systems Interconnections (OSI) Layer Requirements, ISO/IEC DIS 15118-2: 2011-09-14

[6] International Organization for Standardization, Road Vehicles - Vehicle-to-Grid Communication Interface - Part 3: Physical and Data Link Layer Requirements, ISO/DIS 15118-3:2013-02-04

[7] A. Avizienis, J-C. Laprie, B. Randell, and C. Landwehr. Basic Concepts and Taxonomy of Dependable and Secure Computing, IEEE Transactions on Dependable and Secure Computing. Vol.1 N1, Jan-March 2004. ISBN: 1545-5971/04

[8] PRECIOSA Project. Models and Privacy Ontology for V2X, PRECIOSA Project Deliverable D6. Nov. 2010

[9] ETSI. Intelligent Transport Systems (ITS) Security Threat, Vulnerability and Risk Analysis (TVRA) ,ETSI TR 102893 V1.1.1. March 2010.

[10] Microsoft. STRIDE Threat Model, http://msdn.microsoft.com/en-us/library/ee823878%28v=cs.20%29.aspx

Authors

Christophe Jouvray has more than 10 year experience on embedded systems and the engineering process for embedded systems. He is currently involved in the development of security, trust and privacy metamodels for embedded systems. Prior to joining Trialog, he was with CEA List (French laboratory specialized on real-time embedded system modelling) and at the IEF (Fundamental Electronic Institute at Orsay University) where he worked on (i) real-time embedded modellin (ii) software component approaches (iii) middleware and execution platform. He holds a PhD from University of Orsay. His PhD thesis was on the support of model driven engineering for intelligent sensors.

Gloria Pellischek is the Managing Director of ERPC GmbH. ERPCs core business is the co-ordination of multi-national activities in Research and Technology Development (RTD) on European level and consultancy to all stakeholder who take initiative in this area. The encompassing background of ERPC in engineering sciences, primarily in aerospace and automotive engineering, enables ERPC to provide qualified advice on RTD matters regarding strategy and operations. In close cooperation with a legal expert ERPC was able to extended its technological consultancy into the domain of data protection security and privacy in context with emerging technologies.

Mourad Tiguercha is a software engineer specialized on communication technologies for embedded systems. He is representing Renault in the Joined Working Group ISO/IEC 15118 PT2. He is involved in research and industrial projects around electrical vehicle recharging. Moreover, he has a significant experience on automotive and home automation systems.

ID	Asset Involved	Countermeasures	Resistance	Likelihood	Impact	Risk	Risk Value	Benefit
TH1	Network	C1, C2	Moderate	Possible	High	Critical	6	4
			Beyond High	Unlikely	Medium	Minor	2	
TH2	Network	C1, C2	Moderate	Possible	High	Critical	6	4
			Beyond High	Unlikely	Medium	Minor	2	
TH3	Network, ECU	C2, C3	Moderate	Possible	High	Critical	6	4
			Beyond High	Unlikely	Medium	Minor	2	
TH4	Network	C2, C3	Moderate	Possible	Medium	High	4	2
			Beyond High	Unlikely	Medium	Minor	2	
TH5	Network	C2, C4	Moderate	Possible	High	Critical	6	4
			Beyond High	Unlikely	Medium	Minor	2	
TH6	Network	C2	Moderate	Possible	High	Critical	6	4
			Beyond High	Unlikely	Medium	Minor	2	
TH7	Network	C2	High	Unlikely	Low	Minor	2	1
			Beyond High	Unlikely	Medium	Minor	1	
TH8	Network	C2	Beyond High	Unlikely	High	Major	3	1
			Beyond High	Unlikely	Low	Minor	2	
TH9	Network	C2	Basic	Likely	High	Critical	9	7
			Beyond High	Unlikely	Medium	Minor	2	
TH10	Network	C5	No rating	Likely	Low	Major	3	1
			Beyond High	Unlikely	Medium	Minor	1	
TH11	Network	C2, C3	No rating	Likely	Medium	Critical	6	5
			Beyond High	Unlikely	Low	Minor	1	
TH12	ECU	C3, C6	High	Unlikely	Medium	Minor	2	1
			Beyond High	Unlikely	Medium	Minor	1	
TH13	ECU	C6	High	Unlikely	Medium	Minor	2	1
			Beyond High	Unlikely	Medium	Minor	1	
TH14	Network, ECU	C7	Basic	Likely	Medium	Critical	6	5
			Beyond High	Unlikely	Medium	Minor	1	

Table 4: Possible Attacks over the V2G Interface