FABRIC

Feasibility analysis and development of on-road charging solutions for future electric vehicles

Report on Security for upscaling

Deliverable No.		D5.4.3	
Workpackage No.	WP54	Workpackage Title	Integrating EV with ICT, transfer and grids
Authors		Mohammad Khodaei, Panagiotis Papadimitratos, (KTH), Andrew Winder (ERTICO)	
Status		Final	
Dissemination level		Public	
Project start date and duration		01 January 2014, 54 Months	
Revision date		2018-03-26	
Submission date		2018-03-30	

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 605405

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

ABBREVIATION	DESCRIPTION
AAA	Authentication, Authorisation, Accounting
AC	Alternating Current
ANPR	Automatic Number Plate Recognition
CA	Certification Authority
CAM	Cooperative Awareness Message
CI	Charging Infrastructure
CIO	Charging Infrastructure Operator
DC	Direct Current
DDoS	Distributed Denial of Service
DENM	Decentralized Environmental Notification Message
DSO	Distribution System Operator
DoS	Denial of Service
DoW	Description of Work
Dx.x.x	Deliverable x.x.x (of FABRIC project unless otherwise stated)
ECDSA	Elliptic Curve Digital Signature Algorithm
ER	Energy Retailer
ERS	Electric Road System
EU	European Union
EV	Electric Vehicle
EVB	Electric Vehicle Backend

ABBREVIATION	DESCRIPTION
EVSE	Electric Vehicle Supply Equipment
FABRIC	Feasibility analysis and development of on-road charging solutions for future electric vehicles
FEMP	FABRIC Electric-Mobility Platform
GNSS	Global Navigation Satellite Systems
GPS	Global Positioning System
HMI	Human Machine Interface
HSM	Hardware Security Module
HW	Hardware
I2I	Infrastructure to Infrastructure
ICE (ICEV)	Internal Combustion Engine (ICE Vehicle)
ICT	Information and Communication Technology
ID	Identity
ITS	Intelligent Transport System
km/h	Kilometres per hour
LBS	Location-based Service
MITM	Man-In-The-Middle
ms	Milliseconds
OBU	On Board Unit
OEM	Original Equipment Manufacturer
RSU	Roadside Unit

ABBREVIATION	DESCRIPTION
SVD	Selective Vehicle Detection
TTP	Trusted Third Party
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
VANET	Vehicular Ad hoc Network
VC	Vehicular Communication
VPKI	Vehicular Public Key Infrastructure
VSN	Vehicular Social Network
WP	Work Package (of FABRIC project)
WPT	Wireless Power Transfer

REVISION CHART AND HISTORY LOG

REV	DATE	REASON
0.1	2017-08-31	Draft template
0.2	2017-11-09	Input from KTH
0.3	2018-01-04	First stable version
0.4	2018-02-05	Second stable version
0.5	2018-02-13	Pre-final version for peer review
0.6	2018-03-28	Author update following peer review
1.0	2018-03-30	Final quality check for submission

EXECUTIVE SUMMARY

This deliverable looks at security threats and requirements for mitigating them with respect to Electric Road Systems (ERS). For the purposes of this study, ERS constitutes one or more of the on-road charging solutions developed and tested by FABRIC, focusing on Wireless Power Transfer (WPT) technology but also considering conductive systems (overhead wires or in-road conductive charging).

If such systems were to be rolled out on public roads, they would most likely be connected to many other systems, possibly over the internet or particular shielded and protected networks. This gives rise to vulnerability to interference or attacks with consequent risks to the system's availability and smooth operation, the privacy and safety of users and to the security of financial transactions. This report therefore identifies these risks and recommends steps to avoid or mitigate them.

As ERS solutions as demonstrated by FABRIC do not yet exist on public roads, the nature and likelihood of different types of illicit activity against such systems can only be estimated, although the work also draws on experience and counter-measures in other domains.

The main groups of threat identified are as follows:

- Location spoofing: affecting the operation of Charging Infrastructure Operator (CIO) entities;
- Man-in-the-Middle (MITM) attacks: affecting the operation of CIO;
- Replay attacks: affecting the operation of CIO, Distribution System Operators (DSO), and Energy Retailers (ER);
- Exploiting accounting uncertainty: affecting the operation of Electric Vehicle Supply Equipment (EVSE), CIO, DSO, and ER;
- Breaching user privacy;
- Clogging Denial of Service (DoS), affecting the operation of EVs, DSO, ER, and CI;
- Theft, or damage of physical equipment: affecting the operation of Electric Vehicles (EV), and the reputation of DSO, ER, and CI.

1. INTRODUCTION

Electromobility is expected to be an essential component in the pursuit of the decarbonisation of road transport and mobility. One of the main issues hindering the uptake of electric vehicles (EVs) is the need to stop to charge regularly. As a potential solution, the FABRIC project is investigating on-road power transfer solutions. The project has developed ICT and charging prototypes and has demonstrated different solutions at test sites in France and Italy (wireless induction solutions) and at associated test sites in Sweden (conductive solutions).

Sup-Project 5 (SP5) of FABRIC covers the feasibility assessment of on-road charging solutions, including their technological feasibility, socio-economic viability and environmental sustainability. This includes assessment of societal perspectives, technical specifications for Electric Road Systems (ERS, or e-roads), deployment scenarios, traffic operations, life-cycle assessment, supply chain issues, security, and costs and benefits.

1.1 Work Package description

The aim of WP54 “Integrating EV with ICT, transfer & grids” is to assess the combinatory complexity when electric vehicles will be charged using on-road charging with large-scale deployed ICT, transfer and grid systems. This extends the work done on other Sub-Projects of FABRIC and synthesises on it by taking the technical requirements and optimisations of each of the technologies and the charging solutions tested to the scale of regional, national and Europe-wide deployment.

Other parts of WP54 have used simulation approaches to project the impact of different FABRIC solutions, providing insight in the requirements that large-scale deployment of the on-road charging solutions will have for system-level implementation.

1.2 Task description

The description of the task leading to this deliverable, from the FABRIC Description of Work (DoW), is as follows:

“When the ICT in SP2 and SP4 gets to a demonstrable level, the next step is to connect it to many other systems, possibly over the internet or particular shielded and protected networks. With the increasing amount of cyber criminality, the charging solution, and with that the transport system as a whole, can become vulnerable for attacks on the networks. Building on

the ICT security work in SP2 and 4 for the specific solutions, this task assesses the vulnerabilities due to connected infrastructures and recommends future steps to cater for any identified issues."

1.3 Scope of task

The scope of this task and deliverable focuses on assessing risks of different types of malicious attacks on large-scale ERS operations and what counter-measures can be taken. It does not deal with benign failures (non-malicious equipment failure, accident, weather, etc.) or with safety of the systems, as these depend on the specific equipment installed and such issues were part of the demonstration in SP4 of FABRIC. This deliverable rather focuses on security needs for future ERS deployment, independent of the power transfer technology used.

2. APPROACH

FABRIC has developed and tested different prototype ERS solutions, but in all cases these have been on private test tracks only. Since such systems do not yet exist on public roads, security issues need to be approached with a certain level of abstraction, as the risks and requirements may vary according to the type and scale of system(s) deployed.

This task takes the results on architecture and data security and privacy from WP2.4 as its main starting point, in particular Deliverable D2.4.1 “ICT functional architecture and specifications” (January 2015), Chapter 3 “Data Security and Privacy”. This chapter began by benchmarking relevant research projects, then provided a security analysis for the ICT part of FABRIC. It included attacker profiles, a threat analysis, counter-measures and security requirements. An analysis of requirements was also carried out.

The present task also draws on work done on interoperability (WP2.2) and technical feasibility (WP4.2).

The approach takes account of the elements of FABRIC architecture, in particular as described in the above D2.4.1 and describes the general security and privacy requirements. It works on an adversarial model whereby different types of adversaries (hackers, fraudsters, attackers, etc.) are identified along with their motivation (stealing money, electricity or data, disruption, sabotage, etc.) and what they would need in order to carry out their aims. It then goes on to propose appropriate measures based on the likelihood of each type of malicious activity and the severity of its potential consequences.

3. SYSTEM MODEL, ASSUMPTIONS AND REQUIREMENTS

In this section, we discuss the FABRIC system model and assumptions, and outline adversarial model as well as security and privacy requirements towards the deployment of on-road Electric Vehicle (EV) charging infrastructure.

3.1 FABRIC System Model and assumptions

FABRIC charging infrastructure entities, as defined in other deliverables, are as follows:

Distribution System Operator (DSO): This concerns the provision of energy and its pricing, managed by the DSO, which interfaces with the FEMP and the CIO.

FABRIC Electric-Mobility Platform (FEMP): This comprises the FABRIC backend system; it includes at least a middleware platform for infrastructure data collection and potentially data aggregation functionalities, and one service provider platform that provides EV services to customers. Additionally and according to the business strategy, other backend systems may be included such as an Identity (ID) provider that manages the ID and contract information of customers.

Energy Retailer (ER): It supplies the power via the DSO, using the CI. Also interfaces with the FEMP regarding energy pricing/payment.

Charging Infrastructure (CI): It comprises the primary power transfer coil and its electronics and software that communicates with the CIO and the OBU and monitors and controls the charging process based on the information received by the CIO and the EV.

Charging Infrastructure Operator (CIO): This is a backend system that manages the operation of the EVSE. It should handle authentication and authorization tasks before the EV charging, monitors the charging process and collects energy consumption data for billing purposes. CIO is the communications hub with the FABRIC platform. It hosts a load balancing module that controls the energy supply to the EVSE based on high level grid restrictions. CIO also provides EVSE status and operating characteristics information to the FABRIC platform.

Electric Vehicle Supply Equipment (EVSE): The EVSE is composed of the Hardware (HW) components for the electric power transfer, and works in resonance with the compatible secondary coil device that is installed under the EV. One of the components of the EVSE is the charging station control unit which manages the V2G data exchange between the OBU and the

charging infrastructure operator. EVSE is connected with charging infrastructure operator within a specific charging infrastructure operator network using IP communication.

EV Backend (EVB): Electric vehicles from different vehicle manufacturers have their own protocol, communication technology and services; in the FABRIC scenario different OEMs are foreseen therefore the EV OEM backend is the interface with the FABRIC platform.

Road Side Unit (RSU): It transmits information to EVs in the vicinity. It can also gather information from EVs and forward it to the CI.

On Board Unit (OBU): It is integrated into the EV. It includes communication hardware (e.g. Wi-Fi, UMTS, G5...), application unit hardware, vehicle gateway to interface with EV electronic system, at least one Human Machine Interface (HMI) device and the in vehicle charging system.

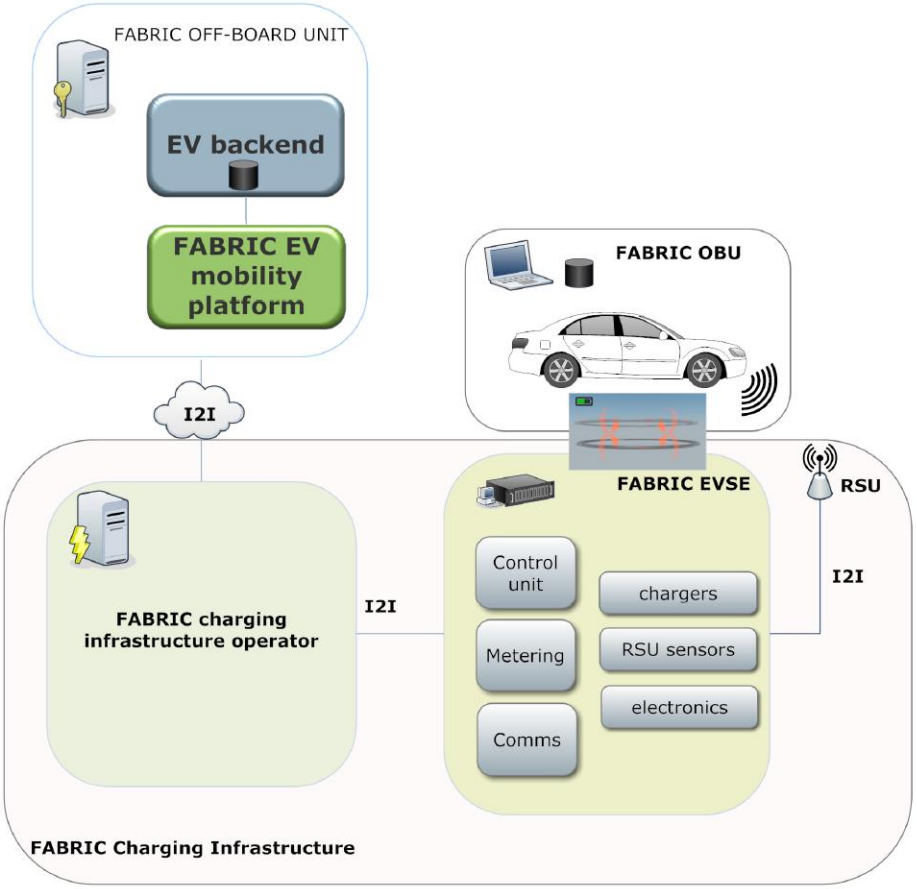

Figure 1: FABRIC charging infrastructure: high level architectural view

We assume that each legitimate EV is registered in the system and there is a Vehicular Public Key Infrastructure (VPKI), e.g., [3][26], that provides short-lived anonymized certificates, termed *pseudonyms*, to EVs; this facilitates secure and privacy-preserving communications/interactions with other entities, e.g., vehicles or RSUs. We further assume that each EV is able to be serviced, i.e., charged in this case, by any charging provider in its domain [6]. To facilitate cross-domain operation, a trust association should be established between the two domains [6].

3.2 Adversarial Model

We adhere to the adversarial model defined in the literature [10][31]: adversaries could be internal, i.e., faulty, compromised, or malicious, or external, i.e., unauthorized entities. The internal adversaries are provided with credentials and cryptographic keys and they are legitimate part of the system; however, they might deviate from system protocols and policies for various reasons, e.g., their sensors become faulty/malfunction, or a module is reprogrammed by its respective owner towards his own benefit. Alternatively, they might be compromised by external adversaries for malicious intent, e.g., installing a malware to set a packet field to an inappropriate value [31]. External adversaries do not possess cryptographic keys and credentials; but they can affect the system operation, e.g., replaying old charging messages that were transmitted by legitimate entities.

From a different perspective, adversaries could be active, i.e., capable of injecting or modifying exchanged messages, or passive, i.e., capable of collecting information by eavesdropping the communication. The behaviour of an adversary can vary based on the implemented protocols and the capabilities of the adversary whose incentive can be his own benefit or malice. An active adversary, either internal or external, could omit, delay, modify, or retransmit early messages from other entities, e.g., forging a charging request in order to masquerade a legitimate EV to mislead the charging service provider to be charged without being invoiced. Alternatively, he could jam the communication and erase one or more messages selectively. A passive adversary, internal or external, could eavesdrop the communication in a region-of-interest towards extracting or inferring information from those messages. From the security point of view, this could target sensitive information about the system, i.e., compromising data confidentiality. From a different perspective, this could harm user privacy if the content reveals user sensitive information. This is further discussed Section 4.2.

Possession of credentials and cryptographic materials does not necessarily guarantee the correct execution of operation or actions. An adversary might not be able to deviate from system security protocols, but he could alter the local inputs to the protocols [31]. More so, entities can be infected, thus the cryptographic materials are compromised and sent to illegitimate nodes. Thus, adversaries could craft a network of *"legitimate-looking"* nodes, namely performing Sybil-based [39] misbehaviour, and affect the output of voting-based protocols by sending out redundant, yet authenticated, information, e.g., real-time reporting of EV traffic flow and density for optimizing the load on the power grid. This implies that not only the protection of the cryptographic materials and other data is imperative, but also a restriction on the number of cryptographic keys/tokens, provided to each entity at any point in time, is demanding.

Due to the nature of Vehicular Communication (VC) system, an adversary could disrupt the operations of location-aware applications relying on the position of a node and its neighbours, e.g., disrupting vehicular traffic monitoring application by relaying counterfeit positions for an accident. In case of on-road EV charging operation, an adversary could bypass the charging authentication phase by replaying counterfeit positions. Even though cryptographic operations would ensure the authenticity of origin, there is no guarantee about the physical layer of communication [1][2].

Without loss of generality, we consider compromising entities in three layers of communication: on-board EV equipment, road-side equipment, and the back-end infrastructure. In the on-road EV charging system, an on-board unit could be compromised; an active malicious OBU could potentially steal electricity, e.g., by tampering with the OBU charging controller, or replaying an old message or spoofing location. Alternatively, it might try to compromise the availability of the charging system, e.g., by clogging a Denial of Service (DoS) attack. Moreover, a local passive adversary could also eavesdrop the communication towards harming user privacy, possibly by collusion with other entities.

Road-side equipment, e.g., Road-side Units (RSUs) and charging pads, could be compromised; an active malicious entity can perform a Man-In-The-Middle (MITM) attack to bypass or subvert the authentication process, thus charging an "external" vehicle without being invoiced. Moreover, a passive adversary could observe the wireless communication to extract users' sensitive information towards harming user privacy.

Similar to any networked system, adversarial behaviour is not limited to the front-end entities; the back-end infrastructure components could “misbehave” too. Typically, we assume the backend infrastructure entities to be fully-trustworthy, widely referred to as Trusted Third Parties (TTPs). However, due to the recent experience in other mobile applications, e.g., [18][19] and recent stream of disclosures on mass surveillance, e.g., [15][16], it is essential to consider the infrastructure entities to be *honest-but-curious* rather than being fully-trustworthy. *Honest-but-curious* entities fully comply with the system security policies and protocols and they never attack the system to affect users operation. However, due to the fact that they interact with many users, they might be “tempted” to collect user sensitive information, possibly combined with extra information derived from VC systems, e.g., the transcript of pseudonymously signed messages, and profile users based solely on the prescribed functionality. In case of EV charging operation, a charging service provider entity might be tempted to identify the actual identity of an EV, e.g., if it knows the mapping between pseudonyms and actual identities of EVs [5]. As a result, they could harm user privacy and attempt to monetize this by offering customized services to the users. In the context of this report, we consider the charging service provider entities (as discussed in Sec. 3.1) and the Vehicular Public Key Infrastructure (VPKI) entities, i.e., the central building block of secure and privacy-preserving VC systems, to be honest-but-curious.

We also consider the risk of compromising back-end security infrastructure entities, even though the risk is lower in comparison with the risk of compromising other system entities. VPKI entities provide credentials to legitimate EVs: each vehicle is equipped with a set of short-lived anonymized certificates, termed *pseudonyms*, along with the corresponding short-term private keys. The system maintains a mapping of these short-term identities to the vehicle long-term identity for accountability purposes. Vehicles disseminate their mobility information, e.g., Cooperative Awareness Message (CAMs) and Decentralized Environmental Notification Message (DENMs), time- and geo-stamped, periodically. Such mobility information is digitally signed with a private key, corresponding to the currently valid pseudonym and vehicles switch from one pseudonym to another to protect user privacy. However, VPKI entities might be “tempted” to identify the real identity of a vehicle, or link successive messages based on the pseudonymous credentials properties, e.g., timing information of the credentials [3]. In fact, they have extra information about the users, e.g., during registration phase and credential acquisition process. As a result, they might try to extract sensitive information, e.g., location, from transcript of pseudonymously signed messages in order to de-anonymize users by cross-referencing with

other source of data, or diminish their anonymity set [9][12][13], thus tracking them for a long period.

We assume that the external adversaries are unable to successfully “crack” the employed cryptosystems and cryptographic primitives since they are computationally limited. However, the adversarial model considers multiple entities collude, i.e., share information that each of them individually infers with the others, to harm user privacy. The nature of collusion can vary, e.g., depending on who is the owner or administrator of any two or more colluding entities. In the context of this report, we do not consider benign failures on the side of the infrastructure entities, e.g., system/server faults or crashes, or network/electricity outages.

3.3 Requirements

The security and privacy requirements for V2X communications have been extensively specified in the literature [10][31][32] with further requirements specifically for VPKI entities in [3]. Next, we compile security and privacy, as well as functional and performance requirements related to communication between any two or more entities, e.g., on-board equipment, road-side equipment, or backend infrastructure entities.

Authentication and communication integrity: All EV-CI communication/interaction should be mutually authenticated, i.e., both interacting entities should confirm the sender of a message as well as the liveness of the sender. The authentication mechanism should be lightweight due to the ephemeral nature of contact between an EV and a charging pad. Communication integrity is necessary so that all exchanged messages are protected from any alternation. More precisely, replay and Man-In-The-Middle (MITM) attacks should be mitigated; replay attacks could enable an adversary to impersonate a legitimate node, e.g., becoming a free-rider towards electricity theft. Furthermore, an attacker should not be able to conduct MITM attacks by tampering with the key establishment between the EV and the CIO entities.

Beyond the conventional entity authentication, it is imperative to identify neighbours securely, i.e., discovering of devices located in “close” (physical) proximity in a way that they can directly communicate with each other. Even though cryptographic operations would ensure the authenticity of origin, there is no guarantee about the physical layer of communication [1][2].

Authorization and access control: Only registered and legitimate EVs should be able to interact with the charging infrastructure and access services, i.e., being charged. The charging infrastructure should authorize EVs to control what each EV is allowed to do, e.g., commencing

charging process from a particular charging pad at a specific time, or if an EV has booked a time-slot.

Fine-grained accounting: The total amount of energy provided to each EV should be properly calculated; an EV could be charged by different charging service providers under dynamic pricing/tariffs, or it could potentially roam from a domain to a “foreign” domain and be charged by a foreign charging provider in that domain. Moreover, having provided energy to an EV, the DSO and ER should not be able to over-claim, thus invoicing the EV with a different price than the genuine one. By the same token, an EV should not be able to under-claim the amount of received energy.

Non-repudiation and accountability: All operations of the charging infrastructure entities and EVs should be non-repudiable, i.e., a sender cannot deny having sent a message.

Message confidentiality: The content of sensitive information, either exchanged messages between two interacting entities or messages stored in local repositories, should only be disclosed to the authorized entities. Moreover, the system should not disclose or allow inferences on the personal and user private information towards harming user privacy, e.g., an unauthorized entity should not be able to infer/identify the actual identity of an EV during charging process.

Misbehaviour detection: A misbehaviour detection mechanism should be in place to observe the actions, operation and activities in the system in order to detect abnormal behaviour and possibly identify the misbehaving node. For example, in case of over-claiming by the charging infrastructure, or under-claiming by the EVs, the misbehaviour detection entity should audit/monitor the charging process, identify any deviation, and resolve any dispute if happened. Depending on the misbehaviour and the situation, appropriate reaction should be taken, e.g., de-anonymising the misbehaving entity and imposing a fine, or revocation of its cryptographic materials and evicting it from further accessing the system.

Eviction/revocation: In case of deviation from system policies, the infrastructure should be able to evict the malicious (compromised, misbehaving, or malfunctioning) entity from the system. For example, a compromised EV should be evicted from further accessing the system, i.e., not be able to be charged. Alternatively, a compromised RSU or charging infrastructure entity, e.g., a charging pad, should be excluded from the system. The revocation information should be timely distributed among the entities to ensure proper system operations and

functions, i.e., preventing malicious or compromised nodes from harming the system. Revocation can be useful for other operational and administrative reasons [40][41]; for example, a specific attribute (e.g., battery type) of a whole class of EVs can be revoked.

Availability: The charging infrastructure should be resilient against resource depletion attacks, e.g., jamming, DoS, and Distributed DoS (DDoS). Such attacks could compromise the availability of the charging infrastructure, thus preventing legitimate EVs from being charged.

Efficiency and scalability: Entity authentication and message validation should be efficient (lightweight), i.e., incurring low computation and communication overhead. This requirement stems from the fact that the length of charging pads is small, e.g., 1 meter, and EVs move at high speeds; thus, the contact time between the EVs and the charging pads might be in the order of tens of milliseconds. At the same time, the system design should be scalable to support a large number of EVs being charged in short periods. The scalability results from efficient and lightweight operations, supporting high-level concurrency for dense vehicular mobility scenarios, and fault-tolerant design to ensure that the system remains operational in the presence of benign failures or resource depletion attacks, e.g., clogging DoS attacks. Ideally, the system should be able to dynamically scale down/up based on its load metrics, e.g., the number of requesting nodes, in order to efficiently and cost-effectively utilize the allocated resources.

Privacy: EV charging systems should ensure confidentiality, anonymity, and unlinkability [47] of all actions ranging from data sharing to system-specific transactions. More precisely, EV charging systems should not disclose any user sensitive information, or allow an adversary to infer user private information towards de-anonymizing users and their actions, e.g., linking anonymous participants. At the same time, the backend (charging or security) infrastructure should be designed by separating processes and functions across entities according to the separation of duties principle [45][46]: each entity should be given minimum information required to execute its desired tasks. This results in enhancing user privacy in the presence of “honest-but-curious” infrastructure entities, i.e., preventing a single entity from accessing all user-sensitive pieces of information towards harming user privacy. In what follows, we elaborate these three pillars of privacy in the EV charging system.

- **Data confidentiality:** Collection, processing, usage, and storage of user sensitive information should be compliance with the General Data Protection Regulation (GDPR) [45]. Clearly, keeping data confidential contributes to protecting user privacy.

- **Anonymity (conditional):** EVs should be able to participate in the system and interact with the charging infrastructure anonymously, i.e., without disclosing their actual identity. However, anonymity should be conditional in the sense that the infrastructure should be able to de-anonymize a wrong-doer, and possibly evict it from the system, if it deviates from the system policies (security or operational), e.g., being charged without successfully conducting the payment, or under-claiming the amount of received energy.
- **Unlinkability:** Dynamic charging for EVs should not enable an internal or external adversary to link/correlate two or more items of interest, e.g., linking successive anonymous charging requests (in fact credentials or tokens used for authentication and authorization) of the same user. Moreover, an adversary should not be able to retrieve the long term identity of an anonymous user from the anonymized token (along with extra information that can be captured). For instance, honest-but-curious charging infrastructure entities, e.g., the Distribution System Operator (DSO), could collect sensitive user information and they might be tempted to profile users in order to predict their trajectory, thus, monetizing it by offering customized services. In order to achieve full unlinkability, which results in perfect-forward-privacy, no single charging infrastructure entity should be able to link a set of anonymous charging requests to an individual EV. More so, upon a revocation event, all anonymous credentials/tokens, corresponding to a “misbehaving” EV, should remain unlinkable, i.e., no backward-trackable or backward-linkable. In other words, user privacy should be protected for a period, during which the user was not compromised/evicted. To this end, the design and deployment of the charging infrastructure should render such inferences hard.

The level of anonymity and unlinkability is highly dependent on the anonymity set, i.e., the number of active participants and the resultant number of charging requests to the charging infrastructure. For example, revisiting the charging infrastructure at a specific location on a regular basis could disclose user sensitive information as the charging request could be unique, or one of few requests.

4. THREAT ANALYSIS

In this section, we provide potential threats towards the deployment of on-road EV charging infrastructure. Essentially, there are two types of authentication path, either through the controller or RSU (vehicle-to-controller), or through the pads (vehicle-to-pad). We address the potential vulnerabilities for both types with emphasis on authentication via vehicle-to-controller communication as this is the design choice in the FABRIC project.

4.1 Electricity theft (free rider) and financial fraud

4.1.1 Location spoofing

An adversary could disrupt the operations of location-aware applications relying on the position of a node and its neighbours by spoofing and/or replaying/relaying navigation messages of Global Navigation Satellite Systems (GNSS) [1][30][33][37][38]. For example, an active adversary could subvert/bypass EV authentication phase before the charging process starts, thus masquerading an internal legitimate EV. To this end, an adversary could either provide counterfeit positions by spoofing its location to the RSU/controller/pad, or he could remotely manipulate the location of another legitimate EV by relaying an authentic position to the RSU/controller/pad. Regardless of type of authentication path, i.e., vehicle-to-controller or vehicle-to-pad, an adversary could successfully conduct such an attack. As a result, an adversary could be charged for free. The main challenge is to identify neighbours securely, i.e., the discovery of devices located in the ‘physical location’ that they claim to be. Even though cryptographic operations would ensure the authenticity of messages and origin, there is no guarantee about the physical layer of communication [2]. These attacks affect the operation of CIO entities in FABRIC architecture.

Implications and recommendations

The security of the charging infrastructure highly relies on an accurate prediction/detection of an EV location exactly because the controller could be misled if an attacker spoofs the location of a legitimate EV. The need for secure ranging and localization is paramount; a fully distributed lightweight framework for discovery and verification of neighbour positions is proposed [2]: any node can anonymously identify and verify its neighbours without an omnipresent trusted infrastructure or a priori established trust.

4.1.2 Man-in-the-Middle (MITM) attacks

A MITM attack is a potential threat during charging authentication process or key establishment phases[1]: an active adversary could 'deploy' a fake RSU or a bogus controller to mislead legitimate vehicles. Alternatively, depending on the authentication process, an active attacker could impersonate another legitimate entity by tampering the key establishment messages, e.g., obtaining a token or an authenticator during charging process of a legitimate EV. Upon stealing a valid token, an external malicious EV could impersonate a legitimate EV, thus presenting the token to the charging infrastructure to be charged for free. This attack affects the operation of CIO in FABRIC architecture.

Implications and recommendations

Mutual authentication eradicates this attack; however, a proper mechanism to mitigate such an attack should be lightweight. For example, digital signature and certificates might not be good candidates for such an authentication process due to their processing overhead [8]. A hash-chain based authentication by leveraging pseudonymous credentials can be a computationally lightweight solution to facilitate EV-pad mutual authentication process [4]: each EV establishes a symmetric session key with every pad. However, each charging pad should interact with the backend charging infrastructure entities, which might be not efficient (in terms of communication delay) as the EV-pad contact time is very short.

4.1.3 Replay attacks

An active attacker could replay old EV messages to the controller (or to another pad, depending on the type of charging infrastructure deployment) in order to bypass the authentication process, or confuse the billing system to invoice an internal legitimate EV multiple times; an active adversary could also replay old pricing/tariff information to the neighbouring EVs to mislead them about the actual pricing/tariff. This attack affects the operation of CIO, DSO, and ER in FABRIC architecture.

[1] Note that establishing a new session key for each interaction is necessary to achieve perfect-forward-secrecy.

Implications and recommendations

Replay attacks can be mitigated by ensuring the authenticity of origin and ensuring clock synchronization[2] to include a timestamp or a nonce in every message to ensure the freshness of messages and liveness of the sender and the receiver. By the same token, nonces should be stored for a specific security association in order to identify replay attacks, e.g., validating the freshness of a nonce if not seen before.

4.1.4 Exploiting accounting uncertainty

Depending on the business model of the charging service providers (DSO/ER), vehicles could choose to pay for the amount of energy that they receive, or pay for a flat monthly charging fee. For the former, drivers could tamper with the OBU charging controllers that store the amount of energy received by the EVs, i.e., under-claiming the amount of received energy. By the same token, the DSO might be tempted to bypass or subvert system mechanisms for its own profit, e.g., invoicing a user more than an agreed tariff or dispensed energy. Alternatively, the DSO might be tempted to steal money repeatedly in extremely small quantities (Salami slicing attack [11]). Stealing money in such small quantities from each EV per charging pad would result in financial fraud. DSO “could” claim for such extremely small increments as the dispensed energy to EVs can be wasted during wireless charging. This attack affects the operation of EVSE, CIO, DSO, and ER in FABRIC architecture.

Flat monthly charging fee is vulnerable to *masquerading* attacks: by stealing a legitimate EV’s authenticator/token, or intentionally sharing an authenticator with the rest, malicious EVs could be freely charged. Since the charging service fee is chosen to be flat, the charging service provider would dispense energy to the requesting *“legitimate-looking”* EV upon receiving a valid token. In other words, the authentication phase can be subverted and any EV with a valid token is to be charged. Even if an upper-bound threshold for the flat fee is determined, a potential abuse of accounting can be taken place: “compromised EVs” could share their quota in order to maximally benefit from it. This attack affects the operation of EVSE, CIO, DSO, and ER in FABRIC architecture.

[2] In some schemes, e.g., [5], full synchronization among EVs, charging pads, and charging service provider entities is crucial to mitigate replay attacks; in other words, loosely synchronized clock cannot prevent from replay attacks as an adversary could capture a charging request sent by a legitimate EV to a charging pad ‘p’ and replay it to the next charging pads, closely located to the charging pad ‘p’.

Similar to any networked system, attackers could hack into the billing system (clearing house), compromising the integrity, confidentiality, and accounting of the system. This attack affects the operation of CIO, DSO, and ER in FABRIC architecture.

Implications and recommendations

In order to mitigate this class of attacks when the charging infrastructure levies invoices based on the amount of dispensed energy to each EV, the payment process should be based on the reports by the DSO/ER and the EVs. The reports on the amount of energy should be non-repudiable and should be compared for any deviation to detect over-claiming by the charging service provider or under-claiming by the EVs. The charging infrastructure could possibly levy a fine providing that an intentional deviation is detected, e.g., [5]. However, it is not straightforward how to define a threshold to detect a deviation between the two reported values due to potential energy loss during the charging process. More precisely, to maximize the power transfer, vehicles should strictly follow the charging lane; otherwise, energy cannot be properly dispensed to the EV. Therefore, defining a threshold to detect any deviation from the reported values is challenging.

Charging vehicles for a flat monthly fee seems to be the most straightforward solution as EVs will not be charged for any energy loss during the charging process. Still, the charging infrastructure needs to authenticate EVs and mitigate masquerading attacks, i.e., preventing multiple “compromised” EVs from being charged with the same token. Clearly, appropriate mechanisms should be employed on both sides, i.e., on the side of the infrastructure and the EVs. On the side of the infrastructure, each EV should be given a short-lived authenticator, bound to a specific region of operation, i.e., limiting the usage of the tokens in time and space. Multiple charging requests with the same token from totally distinct locations should be rejected, and/or reported to misbehaviour detection authority for further investigation. On the side of the EV, they should be provided with Hardware Security Modules (HSMs) to ensure that these tokens never leave the HSM. Any suspicious deviation from such policies should be reported to the misbehaviour detection authority for further investigation. In case of detecting abnormal behaviour, the misbehaving or compromised node should be evicted from the system.

Application-layer and network-layer firewalls, Intrusion Detection Systems (IDSs) and Honey Pots could potentially mitigate networked systems vulnerabilities.

4.2 Breaching user privacy

User privacy can be violated in different ways and by various system infrastructure entities: a global passive observer capable of eavesdropping messages, charging infrastructure entities, and identity and credential providers (VPKI), or some combination thereof, i.e., collusion by different entities.

Charging infrastructure entities: User privacy can be compromised by different charging infrastructure entities. According to D.2.4.1, during EV registration phase, all user sensitive information, e.g., name, address, bank account number, EV model, and parking slot reservation, are provided to the EV backend entity. It is not clear why all these information are necessary, why the registration cannot be anonymous (in fact conditionally anonymous), and how these data are stored, protected, and processed. Furthermore, it is not clear how EVs could anonymously communicate with the charging infrastructure entities.

According to D.2.4.1, during end-user registration phase, EV model and its technical information need to be bound to a token (a payment tag) to ensure vehicle identification while preventing from transferring the payment tag to a different EV. These information suffice to track a specific EV since one can simply filter out EVs based on the information in the charging requests or tokens, e.g., a specific battery type of a Polestar Volvo car could be unique, or one of few, in a region, and thus linkable by the charging service provider, or even an external observer.

According to D.2.4.1, during EV identification and access control, an EV is required to transmit "*EV identification data*" to the charging infrastructure, considered as the default identification method; alternatively, an EV can be identified using Automatic Number Plate Recognition (ANPR) camera-based system. ANPR is proposed as a solution for access control to the charging lane in order to differentiate a real OBU from a fake one (possibly in combination with the default method). However, such approaches obviously violate user privacy: not only the "*EV identification data*" needs to be anonymized, but also conducting access control using ANPR is a realistic threat to user privacy, considering the recent stream of disclosure on mass surveillance, e.g., [15][16].

User privacy can be compromised during the billing process; for example, the charging infrastructure operator (CIO) submits charging session data to the EVB, including the amount of energy transferred to an EV, the identity of an EV, and the timestamp of the session. Thus, an EVB, operated by different vehicle manufacturers, could infer the actual identity of an EV, the

interacting charging service provider (thus estimating the region of operation), and the time of charging operation.

External observers: An eavesdropper could collect user-identifying information to identify users and track vehicles, thus harming user privacy: by cross-referencing the time, location, and other external information [9][50][53][55], e.g., driving patterns [12][13], it would be feasible to track and identify a vehicle. The experience from mobile applications and Location-based Services (LBSs) [18][19][20] hints that this is a realistic threat to user privacy, aggravated, of course, by the recent stream of disclosures on mass surveillance, e.g., [15][16]. For example, revisiting the charging infrastructure at a specific location on a regular basis could disclose user sensitive information as the charging request could be unique, or one of few requests. Thus, vehicles should participate in the VC systems (and other closely-related environment, e.g., LBSs [24], and Vehicular Social Networks (VSNs) [61]) and communicate with each other (ideally) anonymously and the content of the exchanged messages should not disclose user identifiable information.

VPKI Entities: Identity and credential management infrastructure could potentially violate user privacy during pseudonym acquisition process: a single VPKI entity could try to identify the actual identities of the vehicles, or link successive pseudonym requests to a single vehicle. Moreover, pseudonyms carry distinguishable attributes, e.g., issuer identity, and lifetime and expiry time. These information could breach user privacy if one collects them and filter out the pseudonyms based on these uniquely identifiable information [3][27]. More so, colluding between a single VPKI entity and an external observer could allow a single VPKI entity (pseudonym provider) to link the pseudonyms of the same vehicle, or potentially de-anonymize a user (by the identity provider), based on the content of the digitally signed and transmitted messages, i.e., CAMs and DENMs, time- and geo-stamped [9][13][18][19][54].

Pseudonyms can be leveraged to authenticate EVs to the charging infrastructure entities [4], or for real-time reporting of EVs' future trip start time and battery state-of-charge, necessary for optimizing the load on the power grid [29]. Furthermore, pseudonyms can be highly beneficial in other application domains; for example, secure and privacy-preserving LBS provision, e.g., [34][35][36][24], can be leveraged for energy pricing and tariff, or localizing the closest charging stations. Thus, it is imperative to provide *"anonymous credentials"* so that they do not contribute to breach user privacy based on their properties or attributes.

Implications and recommendations

Charging infrastructure entities: Anonymous user registration and operation can be achieved by leveraging pseudonymous authentication and group signatures, e.g., [25]: one can design a comprehensive secure and privacy-preserving architecture to achieve all key aspects of charging process, i.e., accountability, accounting, efficiency, scalability, and strong privacy protection.

In order to prevent from linking (or binding) a payment tag to "*a specific identified vehicle*", one can employ attribute-based credential [23] that allows to flexibly and selectively authenticating different *attributes* about an entity without revealing additional information about the entity (zero-knowledge-property). Moreover, double spending of a payment tag can be prevented by leveraging a credential management scheme that restricts credential usages up to a certain level, e.g., [14].

Beyond the communication in EV charging, there are all sort of cryptocurrencies, e.g., [42][43][44][48][64], that can be employed to protect user privacy in electronic commerce. For example, anonymous coins can be employed to protect user privacy during charging process and payment [62]: each EV requests to purchase anonymous coins from a bank using partial blind signature scheme. Thus, the bank cannot link the coins to the real identity of an EV. In order to initiate the charging request, the EV communicates with the corresponding charging service provider and presents its anonymous coins. The charging service provider interacts with the bank to validate the coin (and prevent from double spending). It then delivers two tokens to each authenticated EV, used to interact and mutually authenticate the corresponding RSUs. Upon receiving the tokens, each EV can derive the corresponding secret key for each RSU using a hash chain and XOR operations. In order to commence the charging process, an EV interacts with an RSU; the RSU mutually authenticates the EV employing the tokens provided by charging service provider. Upon a successful authentication, a new token is transported to the EV, used to interact with the charging pads, which are controlled and operated by that RSU. Moreover, a challenge/response protocol ensures the authentication between an EV and the charging pads. Once the authentication is successful, the charging pad dispenses energy to the authenticated EV. Inspired by [62], one can deploy an entity in FABRIC architecture to issue anonymous coins to legitimate EVs; one anonymous coin can be sufficient for an EV to be charged by a certain number of charging pads.

VPKI Entities: Pseudonymous authentication is a promising solution to achieve accountability and user privacy at the same time [7][10][17][31][32][49]. It has been elaborated by several projects and proposals, notably in VC systems, and there are special-purpose identity and credential management systems, namely Vehicular Public-Key Infrastructure (VPKI), e.g., [3][26][27], that facilitates multi-domain operations in the VC systems and enhances user privacy in the presence of *honest-but-curious* system entities. Moreover, the separation of duty among different VPKI entities would prevent a single entity from de-anonymizing a user: each entity should be given minimum amount of information required to execute its desired tasks. In this case, the identity provider should not know which pseudonym provider is targeted and which pseudonyms are obtained by which vehicles and for which period. By the same token, the pseudonym provider should not be able to identify the real identity of the vehicles, or even link successive pseudonym requests to a single vehicle.

External observers: Timing and location information of pseudonymously authenticated messages could help an external adversary, who eavesdrops all traffic through an area, to link pseudonyms based on these information [9]. Even if vehicles switch from one pseudonym to another, one can still link them during pseudonyms transition, i.e., changing the currently used (or expired) pseudonym to a new one. Some proposals [51][52][55] suggest changing pseudonyms at appropriate places, e.g., at an intersection or a parking lot, to make it more difficult for an observer to link two successive pseudonyms belonging to the same vehicle. To enhance user privacy, i.e., to increase the probability of unlinkability between two pseudonyms, [56] suggests that each vehicle should be silent, i.e., not beaconing, for a quiet-time interval, or if the speed is below a threshold [57]. However, vehicle transceivers cannot be simply switched off [50] as they could cause fatal accidents, thus seriously jeopardizing human safety. A cooperative pseudonym changing process was proposed [58][59]: multiple OBUs cooperate with each other to determine the exact time of pseudonym transition so that they simultaneously change their pseudonyms. Alternatively, all vehicles operating in a domain could switch their pseudonyms at the same time to eliminate any distinction among pseudonym sets [3][21][26][27]. Timely-aligned pseudonyms are issued for all vehicles to essentially eliminate any distinction among pseudonym sets and at the same time, upon pseudonym transition process (as all vehicles change their pseudonyms simultaneously). Even if a fraction of vehicles run out of pseudonyms and cannot refill their pseudonym pool, user privacy still can be protected by leveraging other anonymous credentials [14][21][22].

4.3 Clogging DoS

Due to the lack of symmetry in some operations/actions, an active adversary could compromise the availability of an entity simply by clogging a DoS attack. This can be conducted on the charging infrastructure entities/facilities, e.g., a controller, an RSU, the charging pad or the backend charging infrastructure entities. Alternatively, an attacker could compromise the availability of a VPKI entity by sending fake certificate requests, or bogus authenticators [3][26]. Depending on the authentication method, one can also perform a signature flooding attack [28] on the charging controller, e.g., fake ECDSA signatures or fake reports.

Alternatively, an active attacker could deliberately disrupt communication by tampering the clock synchronization. This could affect any operation based on timestamp. Thus, a precise and secure synchronization is indeed necessary.

Attacks on physical layer communication could also disturb the communication, thus the operation, of the on-road charging services. An attacker could launch a DoS attack by jamming the communication over small or wider geographical areas. Such attacks overwhelm the infrastructure entities/facilities so that the correct operation of the system would be at stake. The goal of an attacker could be compromising the reputation of a given charging service provider, thus motivating EVs to switch to another charging provider. Alternatively, an adversary might be tempted to prevent the charging service provider from receiving an authentic charging request so that he can replay the message to be charged for free. This attack affects the operation of EVs, DSO, ER, and CI in FABRIC architecture.

Implications and recommendations

A proper design choice, e.g., a lightweight mutual authentication, and an appropriate DoS mitigation technique, e.g., puzzle for DoS prevention [60], can be employed to prevent external adversaries from overflowing the servers with spurious requests. For example, DDoS attacks were mitigated in a VPKI system [3][26], thus preventing the external adversaries from overflowing the servers with spurious requests. A proper mitigation technique could degrade the power of an active adversary to the power of a legitimate client.

An EV could synchronize its clock either through Global Navigation Satellite Systems (GNSS) providing that it has on-board GPS device, or utilizing other network timing protocols. Depending on the accuracy of Real Time Clocks (RTCs) in electronic devices and the maximum deviation, each EV should synchronize its clock frequently. For example, if the accuracy of an

RTC is 50 parts-per-million (ppm), i.e., 50×10^{-6}, and the maximum accepted error in timestamp is 50 milliseconds (ms), then the EV (and other entities, e.g., charging pads) should synchronize its clock every 16 minutes ($\frac{50\times10^{-3}\ sec}{50\times10^{-6}\ ppm}$).

Various techniques to mitigate jamming in wireless networks are available, e.g., frequency hopping spread spectrum. The essence is that if an adversary overwhelms a channel, then legitimate users/devices should switch to a jammer-free channel. The challenge is to make it hard for the jammer to follow or predict which channel to jam. If this is impossible to achieve, e.g., the jammer is too powerful, then the solution is eventually to localize the jammer and remove the jamming devices (sources of offending signals) physically, e.g., [63]. Moreover, one can prevent an adversary from replaying other EVs' charging request by ensuring the authenticity of origin and ensuring clock synchronization.

4.4 Theft, or damage of physical equipment

The charging infrastructure could be physically damaged, e.g., theft, vandalism, sabotage or terrorism activities, in order to bring the charging system down or threaten to do so possibly for a ransom or political reasons. Disturbing the function and operation of the charging infrastructure, e.g., by stealing in-road equipment (copper) for profit or damaging the charging pads, would compromise the availability of the charging system. This type of attack can affect the operation of EVs, DSO, ER, and CI in FABRIC architecture.

Note that the threat description in Sec. 4.3 could stem from a sophisticated and well-organised attack, e.g., terrorism and sabotage, whereas this threat, disabling the system, is a lower level crime, e.g., theft and vandalism, which might disable parts of the service but not bring down the entire charging system.

Implications and recommendations

Note the parallel with theft of copper signalling cables of railways which is a regular problem in many areas. Stricter laws on scrap metal dealers accepting metal one solution that has been implemented in some countries (i.e., no longer allowed to accept metal from anonymous persons or to pay them in cash). Another solution is invisible marking on metal (e.g. copper wire) to trace its origin.

5. KEY RECOMMENDATIONS

The security of the charging infrastructure highly relies on an accurate prediction/detection of an EV location exactly because the controller could be misled if an attacker spoofs the location of a legitimate EV. The need for secure ranging and localization is paramount; a fully distributed lightweight framework for discovery and verification of neighbour positions is proposed [2]: any node can anonymously identify and verify its neighbours without an omnipresent trusted infrastructure or a priori established trust.

A proper design choice, e.g., a lightweight mutual authentication, and an appropriate DoS mitigation technique, e.g., puzzle for DoS prevention [60], can be employed to prevent external adversaries from overflowing the servers with spurious requests. For example, DDoS attacks were mitigated in a VPKI system [3][26], thus preventing the external adversaries from overflowing the servers with spurious requests. A proper mitigation technique could degrade the power of an active adversary to the power of a legitimate client.

Replay attacks can be simply mitigated by ensuring the authenticity of origin and including a timestamp or a nonce in every message to ensure the freshness of messages and liveness of the sender and the receiver. By the same token, nonces should be stored for a specific security association in order to identify replay attacks, e.g., validating the freshness of a nonce if not seen before. Furthermore, a mutual authentication eradicates MITM attacks; however, such a mechanism should be lightweight due to the nature of interactions during the charging process.

User privacy should be protected not only by relying on legal frameworks (EU Data Protection Regulation (GDPR) [45]), but also by leveraging Privacy Enhancing Technologies (PETs), led to privacy-by-design concept. According to the GDPR [45], all entities, which collect user information, are responsible and accountable for protecting personal data by applying "*privacy by design*" and mandating "*pseudonymization"* in the development of business processes. Furthermore, PETs provide a set of mechanisms, methods, tools and protocols to enhance user privacy, ranging from "*communication anonymizers*" (thus achieving unlinkabilitry, untraceability, anonymity and pseudonymity) to "*accessing to personal data*" by minimizing the amount of personal information that service providers could collect. They further enable users to gain control over their personal data (self-determination of information).

Security and privacy-preserving solutions in closely related domains, e.g., VC systems [7][10], LBSs [24], and VSNs [61], can be leveraged in the design and deployment of an on-road

charging infrastructure. For example, SECMACE [3] is a highly scalable and robust identity and credential management that facilitates multi-domain operations in the VC systems and enhances user privacy. This architecture can be used as the central building block of a secure and privacy-preserving charging infrastructure. A secure and privacy-preserving accountable Participatory Sensing system [25] can be utilized in order to aggregate real-time reporting of EV information, e.g., trip duration and battery state-of-charge, for optimization purposes, e.g., load management and charging scheduling. Furthermore, a decentralized secure and privacy-preserving Location Based Service (LBS) architecture [24] can be leveraged for energy pricing and tariff. To mitigate the effect of location spoofing attacks, one can leverage a fully distributed lightweight framework for discovery and verification of neighbour positions [2]: any node can anonymously identify and verify its neighbours without an omnipresent trusted infrastructure or a priori established trust.

Last but not least, we need to emphasise that the effect of providing security (and safeguarding user privacy) should not undermine the functionality and operation of the system. More precisely, implementing a security countermeasure should not increase the complexity of an application, or result in decreasing the performance and efficiency of the system operations. The security and privacy mechanisms should be designed so that their integration into the system design has limited effects on the system performance [22].

6. CONCLUSIONS

In this report, we considered the FABRIC system model and assumptions towards the deployment of a secure and privacy-preserving EV on-road charging infrastructure. We further pointed out adversarial model, and security and privacy as well as functional and performance requirements related to all communication between any two or more entities. We surveyed the literature and identified potential attacks for EV on-road charging and we provided a set of recommendations for the identified vulnerabilities towards mitigating them. We further highlighted a set of key recommendations towards the deployment of an efficient, effective, resilient, secure and privacy-preserving EV on-road charging infrastructure. A summary of the key recommendation is shown in Table 1.

Table 1: Summary of key recommendations

Threat	***Recommendation***
Location spoofing: affecting the operation of CIO entities.	Ensuring the initiator of a protocol and physical presence of a node and direct communication with its neighbours. A fully distributed lightweight framework for discovery and verification of neighbour positions can be leveraged: any node can anonymously identify and verify its neighbours without an omnipresent trusted infrastructure or a priori established trust. Detailed analysis and recommendation in Sec. 4.1.1.
Man-in-the-Middle (MITM) attacks: affecting the operation of CIO.	Computationally lightweight mutual authentication, e.g., a hash-chain based authentication by leveraging pseudonymous credentials, and establishing symmetric session keys with every pad. Detailed analysis and recommendation in Sec. 4.1.2.

Replay attacks: affecting the operation of CIO, DSO, and ER.	Ensuring authenticity of origin and ensuring clock synchronization to include timestamps and nonce on the exchanged messages; nonces should be stored for a specific security association and the freshness should be validated, e.g., accepted if not seen before. Detailed analysis and recommendation in Sec. 4.1.3.
Exploiting accounting uncertainty: affecting the operation of EVSE, CIO, DSO, and ER.	In case of levying invoices based on the amount of dispensed energy to each EV: the payment process should be based on the reports by the DSO/ER and the EVs. The reports on the amount of energy should be non-repudiable and should be compared for any deviation to detect over-claiming by the charging service provider or under-claiming by the EVs. In case of a flat monthly fee, the charging infrastructure still needs to authenticate EVs by providing legitimate ones with a short-lived authenticator, bound to a specific region of operation, i.e., limiting the usage of the tokens in time and space. Multiple charging requests with the same token from totally distinct locations should be rejected, and/or reported to misbehaviour detection authority for further investigation. For both business models, any suspicious deviation from such policies should be reported to the misbehaviour detection authority for further investigation; in case of detecting abnormal behaviour, the misbehaving or compromised nodes should be evicted from the system. Detailed analysis and recommendation in Sec. 4.1.4.

Breaching user privacy	Extending the adversarial model from fully-trusted entities to honest-but-curious, i.e., those entities that fully comply with system security policies and protocols, but tempted to collect as much as information towards harming user privacy. User privacy should be protected not only by relying on legal frameworks (EU GDPR), but also by leveraging Privacy Enhancing Technologies (PETs), led to privacy-by-design concept: all entities, which collect user information, are responsible and accountable for protecting personal data by applying *"privacy by design"* and mandating "pseudonymization" in the development of business processes. Separation of duty among different (charging or security) infrastructure entities would prevent a single entity from de-anonymizing a user: each entity should be given minimum amount of information required to execute its desired tasks. Anonymous user registration and operation can be utilized by charging infrastructure entities by leveraging pseudonymous authentication and group signatures. Moreover, one can employ attribute-based credential that allows to flexibly and selectively authenticating different attributes about an entity without revealing additional information about the entity (zero-knowledge-property). Timely-aligned pseudonyms should be issued for all vehicles to essentially eliminate any distinction among pseudonym sets and at the same time, upon pseudonym transition process (as all vehicles change their pseudonyms simultaneously). There are privacy-preserving solutions in closely related domains that can be leveraged in the design and development of an on-road charging infrastructure, e.g., SECMACE, and SPPEAR. Detailed analysis in Sec. 4.2.

Clogging DoS: affecting the operation of EVs, DSO, ER, and CI.	Computationally lightweight operations and an appropriate DoS mitigation technique to compensate the work of asymmetry and degrade the power of an active adversary to the power of a legitimate client. Frequently synchronizing EV clock either through Global Navigation Satellite Systems (GNSS) providing that it has on-board GPS device, or utilizing other network timing protocols. Depending on the type of jamming attack, employing appropriate mechanism, e.g., frequently switching to a jammer-free channel. Detailed analysis and recommendation in Sec. 4.3.
Theft, or damage of physical equipment: affecting the operation of EVs, and the reputation of DSO, ER, and CI.	Stricter laws on scrap metal dealers, (i.e., no longer allowed to accept metal from anonymous persons or to pay them in cash); another solution is invisible marking on metal (e.g. copper wire) to trace its origin. Alternative solution is invisible marking on materials to trace its origin. Detailed analysis and recommendation in Sec. 4.4.

REFERENCES

[1] P. Papadimitratos, M. Poturalski, P. Schaller, P. Lafourcade, D. Basin, S. Capkun, and J.-P. Hubaux, "*Secure Neighborhood Discovery: A Fundamental Element for Mobile Ad Hoc Networking,"* IEEE Communications Magazine , vol. 46, no. 2, pp. 132–139, February 2008.

[2] M. Fiore, C. Casetti, C. Chiasserini, and P. Papadimitratos, "*Discovery and Verification of Neighbor Positions in Mobile Ad Hoc Networks,"* IEEE Transactions on Mobile Computing, vol. 12, no. 2, pp. 289–303, February 2013.

[3] M. Khodaei, H. Jin, and P. Papadimitratos, "*SECMACE: Scalable and Robust Identity and Credential Management Infrastructure in Vehicular Communication Systems,"* in the IEEE Transactions on Intelligent Transportation Systems (TITS), April 2018, Accessed Date: 30-Nov-2017. [Online]. Available: https://arxiv.org/abs/1707.05518.

[4] R. Hussain, D. Kim, M. Nogueira, J. Son, A. Tokuta, and H. Oh, "*A New Privacy-aware Mutual Authentication Mechanism for Charging-on-the-Move in Online Electric Vehicles,"* in 11th International Conference on Mobile Ad-hoc and Sensor Networks (MSN), Shenzhen, China, pp. 108–115, December 2015.

[5] L., Hongyang, G. Dán, and K. Nahrstedt, "*Portunes: Privacy-Preserving Fast Authentication for Dynamic Electric Vehicle Charging,"* in IEEE International Conference on Smart Grid Communications, Venice, Italy, November 2014.

[6] M. Khodaei and P. Papadimitratos, "*The Key to Intelligent Transportation: Identity and Credential Management in Vehicular Communication Systems,"* IEEE Vehicular Technology Magazine (VT-mag), vol. 10, no. 4, pp. 63–69, December 2015.

[7] T. Leinmüller, L. Buttyan, J.-P. Hubaux, F. Kargl, R. Kroh, P. Papadimitratos, M. Raya, and E. Schoch, "*SEVECOM – Secure Vehicle Communication*". In IST Mobile and Wireless Communication Summit, Mykonos, Greece, June 2006.

[8] H.-C. Hsiao, A. Studer, C. Chen, A. Perrig, F. Bai, B. Bellur, and A. Iyer, "*Flooding-resilient Broadcast Authentication for VANETs,"* in Proceedings of the 17th annual international ACM conference on Mobile computing and networking, Las Vegas, Nevada, pp. 193–204, September 2011.

[9] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos, "*Privacy in Inter-Vehicular Networks: Why Simple Pseudonym Change is not Enough,"* in IEEE International Conference on Wireless On-demand Network Systems and Services, Kranjska Gora, Slovenia, February 2010.

[10] P. Papadimitratos, V. Gligor, and J.-P. Hubaux, "*Securing Vehicular Communications-Assumptions, Requirements, and Principles,*" in ESCAR, Berlin, Germany, pp. 5–14, November 2006.

[11] Kabay, M. E. "*Salami fraud," Network World Security Newsletter* 24, July 2002.

[12] E. Sampson, "*The future looks bright for ITS,"* June 2015. Accessed date: February 2018. [Online]. Available: http://www.itsinternational.com/sections/comment-interview/interviews/the-future-looks-bright-for-its/

[13] J. Krumm, "*Inference Attacks on Location Tracks,"* in International Conference on Pervasive Computing, Toronto, Canada, pp. 127–143, May 2007.

[14] J. Camenisch, S. Hohenberger, M. Kohlweiss, A. Lysyanskaya, and M. Meyerovich, "*How to Win the Clonewars: Efficient Periodic n-Times Anonymous Authentication,"* in ACM CCS, NY, USA, pp. 201–210, October 2006.

[15] G. Greenwald, "*NSA Prism Program Taps in to User Data of Apple, Google and Others,"* June 2013. Accessed date: February 2018. [Online]. Available: http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

[16] S. Era and B. Preneel, "*Cryptography and Information Security in the Post-Snowden era,"* in IEEE/ACM 1st International Workshop on Technical and Legal aspects of Data Privacy and Security, Florence, Italy, pp. 1–1.May 2015.

[17] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "*Efficient and Robust Pseudonymous Authentication in VANET,*" in Proceedings of the ACM International Workshop on Vehicular Ad hoc Networks (VANET), Montreal, Quebec, Canada, pp. 19–28, September 2007.

[18] M. van Rijmenam, *"The Re-Identification of Anonymous People with Big Data."* Accessed date: February 2018. [Online]. Available: https://dataflog.com/read/re-identifying-anonymous-people-with-big-data/228

[19] Y.-A. De Montjoye, C. A. Hidalgo, M. Verleysen, and V. D. Blondel, *"Unique in the Crowd: The Privacy Bounds of Human Mobility,"* Scientific reports, vol. 3, no. 1376, February 2013.

[20] P. LeBeau, "Ford exec backpedals after saying it tracks drivers," January 2014. [Online]. Available at: http://www.cnbc.com/2014/01/09/ford-exec-backpedals-after-saying-it-tracks-drivers.html.

[21] M. Khodaei, A. Messing, P. Papadimitratos, "*RHyTHM: A Randomized Hybrid Scheme To Hide in the Mobile Crowd,*" in IEEE Vehicular Networking Conference (VNC), Torino, Italy, November 2017.

[22] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "*On the Performance of Secure Vehicular Communication Systems,"* IEEE Transactions on Dependable and Secure Computing (IEEE TDSC), vol. 8, no. 6, pp. 898–912, November 2011.

[23] J. Camenisch, M. Dubovitskaya, A. Lehmann, G. Neven, C. Paquin, F-S. Preiss, *"Concepts and Languages for Privacy-preserving Attribute-based Authentication"*, in IFIP Working Conference on Policies and Research in Identity Management (Springer), Berlin, Heidelberg, pp. 34–52, April 2013.

[24] H. Jin and P. Papadimitratos, "*Resilient Privacy Protection for Location-Based Services Through Decentralization,"* in ACM WiSec, Boston, MA, USA, July 2017.

[25] S. Gisdakis, T. Giannetsos, and P. Papadimitratos, "*SPPEAR: Security and Privacy-preserving Architecture for Participatory-sensing Applications,*" in ACM Conference on Security & Privacy in Wireless and Mobile Networks (ACM WiSec), Oxford, United Kingdom, July, 2014.

[26] M. Khodaei, H. Jin, and P. Papadimitratos, "*Towards Deploying a Scalable & Robust Vehicular Identity and Credential Management Infrastructure*," in IEEE Vehicular Networking Conference (VNC), Paderborn, Germany, December 2014.

[27] M. Khodaei and P. Papadimitratos, "*Evaluating On-demand Pseudonym Acquisition Policies in Vehicular Communication Systems*," in Proceedings of the First International Workshop on Internet of Vehicles and Vehicles of Internet (IoV-VoI), Paderborn, Germany, pp. 7–12, July 2016.

[28] HC. Hsiao, A. Studer, C. Chen, A. Perrig, F. Bai, B. Bellur, A. Iyer. "*Flooding-resilient Broadcast Authentication for VANETs,*" In Proceedings of the 17th annual international ACM

conference on Mobile computing and networking, Las Vegas, Nevada, USA, pp. 193–204, September 2011.

[29] H. Li, G. Dán, and K. Nahrstedt, "*Lynx: Authenticated Anonymous Real-time Reporting of Electric Vehicle Information,*" In: IEEE International Conference on Smart Grid Communications (SmartGridComm), Miami, FL, USA, p. 599–604, November 2015.

[30] K. Zhang, R. A. Tuhin, and P. Papadimitratos, "*Detection and Exclusion RAIM Algorithm against Spoofing/Replaying Attacks,*" in International Symposium on GNSS, Kyoto, Japan, November 2015.

[31] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, *"Secure Vehicular Communication Systems: Design and Architecture,"* in IEEE Communications Magazine, vol. 46, no. 11, pp. 100–109, November 2008.

[32] F. Kargl, P. Papadimitratos, L. Buttyan, M. Müter, E. Schoch, B. Wiedersheim, T. V. Thong, G. Calandriello, A. Held, A. Kung, and J.-P. Hubaux, *"Secure Vehicular Communication Systems: Implementation, Performance, and Research Challenges,"* in IEEE Communications Magazine, vol. 46, no. 11, pp. 110–118, November 2008.

[33] K. Zhang and P. Papadimitratos, *"GNSS Receiver Tracking Performance Analysis under Distance-decreasing Attacks,"* in International Conference on Location and GNSS (ICL-GNSS), Gothenburg, Sweden, pp. 1–6, June 2015.

[34] R. Shokri, P. Papadimitratos, and J.-P. Hubaux, *"MobiCrowd: A Collaborative Location-Privacy Preserving Mobile Proxy,"* in ACM International Conference on Mobile Systems, Applications and Services (ACM MobiSys), San Francisco, CA, USA, June 2010.

[35] R. Shokri, P. Papadimitratos, G. Theodorakopoulos, and J.-P. Hubaux, *"Collaborative Location Privacy,"* in IEEE International Conference on Mobile Ad-hoc and Sensor Systems (IEEE MASS), Los Alamitos, CA, USA, pp. 500–509, October 2011.

[36] R. Shokri, G. Theodorakopoulos, P. Papadimitratos, E. Kazemi, and J.-P. Hubaux, *"Hiding in the Mobile Crowd: Location Privacy through Collaboration,"* in IEEE Transactions on Dependable and Secure Computing, vol. 11, no. 3, pp. 266–279, May 2014.

[37] P. Papadimitratos and A. Jovanovic, *"GNSS-based Positioning: Attacks and Countermeasures,"* in IEEE Military Communications Conference (IEEE MILCOM), San Diego, CA, USA, pp. 1–7, November 2008.

[38] P. Papadimitratos and A. Jovanovic*, "Protection and Fundamental Vulnerability of GNSS,"* in IEEE International Workshop on Satellite and Space Communications (IEEE IWSSC), Toulouse, France, pp. 167–171, October 2008.

[39] J. R. Douceur, "The Sybil Attack," in ACM Peer-to-peer Systems, London, UK, Mar. 2002.

[40] P. Papadimitratos, ""On the road" – Reflections on the Security of Vehicular Communication Systems," in IEEE ICVES, Columbus, OH, USA, pp. 359–363, September 2008.

[41] M. Raya, D. Jungels, P. Papadimitratos, I. Aad, and J.-P. Hubaux, "Certificate Revocation in Vehicular Networks," Technical Report, EPFL, Switzerland, 2006.

[42] Nakamoto, Satoshi. "Bitcoin: A Peer-to-peer Electronic Cash System," 2008.

[43] Antonopoulos, A. M. *"Mastering Bitcoin: Unlocking Digital Cryptocurrencies,"* O'Reilly Media, Inc., December 2014.

[44] Cryptocurrency Market Capitalizations, [Online]. Accessed date: February 2018. Available at: https://coinmarketcap.com/all/views/all/.

[45] The EU General Data Protection Regulation (GDPR) Portal, https://www.eugdpr.org/the-regulation.html. Accessed date: February 2018.

[46] J. H. Saltzer and M. D. Schroeder. *"The Protection of Information in Computer Systems,"* in Proceedings of the IEEE 63.9, pp. 1278–1308, September 1975.

[47] A. Pfitzmann, and M. Hansen. *"A Terminology for Talking about Privacy by Data Minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management,"* PETs Lecture Notes in Computer Science, August 2010. Available at: http://www.maroki.de/pub/dphistory/2010_Anon_Terminology_v0.34.pdf.

[48] Liu, J. K., Au, M. H., Susilo, W., and Zhou, J. *"Enhancing Location Privacy for Electric Vehicles (at the right time),"* In European Symposium on Research in Computer Security, Springer, Berlin, Heidelberg, pp. 397–414, September 2012.

[49] J. Petit, F. Schaub, M. Feiri, and F. Kargl, *"Pseudonym Schemes in Vehicular Networks: A Survey,"* IEEE communications surveys & tutorials, vol. 17, no. 1, pp. 228–255, March 2015.

[50] P. Papadimitratos, A. Kung, J.-P. Hubaux, and F. Kargl, *"Privacy and Identity Management for Vehicular Communication Systems: a Position Paper,"* in Workshop on standards for privacy in user-centric identity management, no. LCA-CONF-2006-020, July 2006.

[51] A. R. Beresford and F. Stajano, *"Mix-zones: User Privacy in Location-aware Services,"* In Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops, Orlando, FL, USA, pp. 127–131, March 2004.

[52] J. Freudiger, M. Raya, M. Félegyházi, P. Papadimitratos, J.-P. Hubaux, *"Mix-zones for Location Privacy in Vehicular Networks,"* in Win-ITS, Vancouver, BC, Canada, August 2007.

[53] Z. Ma, F. Kargl, and M. Weber, *"Measuring Location Privacy in V2X Communication Systems with Accumulated Information,"* in IEEE 6th International Conference on Mobile Adhoc and Sensor Systems (MASS'09), Macau, China, pp. 322–331, November 2009.

[54] P. Golle and K. Partridge, *"On the Anonymity of Home/Work Location Pairs,"* in Pervasive computing, Springer, pp. 390–397, May 2009.

[55] R. Lu, X. Li, T. H. Luan, X. Liang, and X. Shen, *"Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in VANETs,"* in IEEE Transactions on Vehicular Technology, vol. 61, no. 1, pp. 86–96, January 2012.

[56] S. Eichler, *"Strategies for Pseudonym Changes in Vehicular Ad Hoc Networks Depending on Node Mobility,"* in IEEE Intelligent Vehicles Symposium, Istanbul, Turkey, pp. 541–546, June 2007.

[57] L. Buttyán, T. Holczer, A. Weimerskirch, and W. Whyte, *"SLOW: A Practical Pseudonym Changing Scheme for Location Privacy in VANETs,"* in IEEE Vehicular Networking Conference (VNC), Tokyo, Japan, pp. 1–8, October 2009.

[58] M. Gerlach, *"Assessing and Improving Privacy in VANETs,"* in ESCAR, Embedded Security in Cars, Berlin, Germany, November 2006.

[59] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, *"CARAVAN: Providing Location Privacy for VANET,"* in ESCAR, Embedded Security in Cars, Cologne, Germany, November 2005.

[60] S. T., Zargar, J., Joshi, and D., Tipper, “A Survey of Defense Mechanisms against Distributed Denial of Service (DDoS) Flooding Attacks,” in IEEE Communications Surveys & Tutorials, 15(4), pp. 2046–2069, March 2013.

[61] H. Jin, M. Khodaei, and P. Papadimitratos, *‘‘Security and Privacy in Vehicular Social Networks,”* in Vehicular Social Networks. CRC Press, Taylor & Francis Group, March 2017.

[62] S. Gunukula, A. Sherif, M. Pazos-Revilla, B. Ausby, M. Mahmoud, and X. S. Shen, *“Efficient Scheme for Secure and Privacy-Preserving Electric Vehicle Dynamic Charging System,”* in IEEE International Conference on Communications (ICC), Paris, France, pp. 1–6, May 2017.

[63] G. Kanika, A. Lim, and Q. Yang, *“Jamming and Anti-jamming Techniques in Wireless Networks: A Survey,”* International Journal of Ad Hoc and Ubiquitous Computing, Vol. 17, No. 4, 197–215, December 2014.

[64] M. Ian, C. Garman, M. Green, and A-D. Rubin, *“Zerocoin: Anonymous Distributed E-cash from Bitcoin,”* In IEEE Symposium on Security and Privacy (SP), Berkeley, CA, USA, pp. 397–411, May 2013.