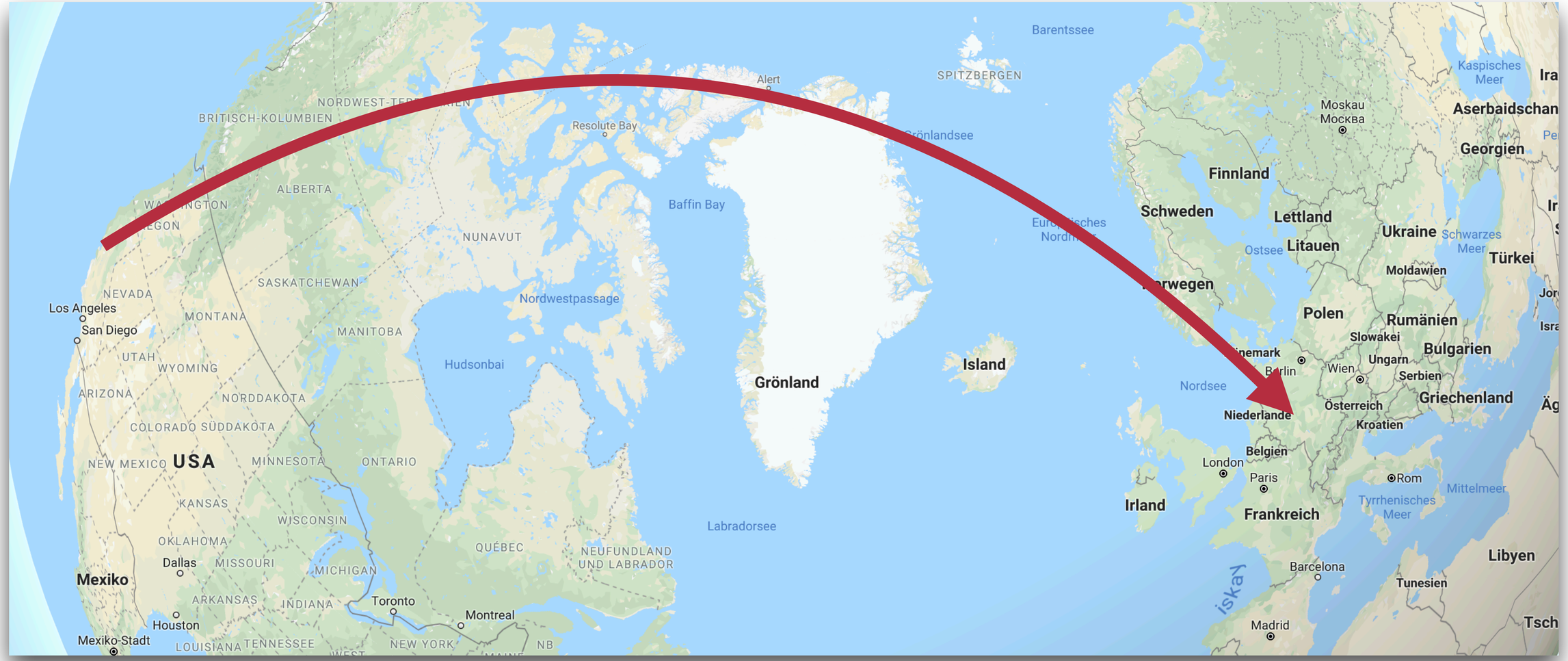
Institut für Verteilte Systeme
Institute of Distributed Systems

ulm university universität
uulm



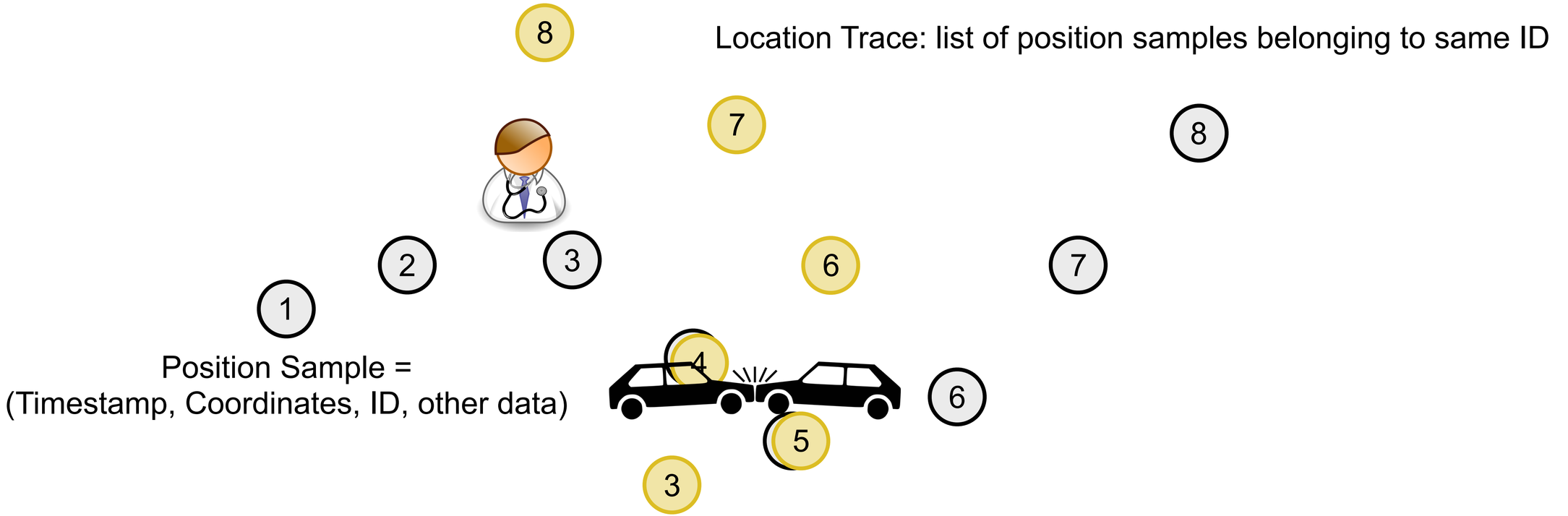
Privacy Engineering in the Automotive Domain

Frank Kargl | PEPR'19 | 2019-08-12


Barentssee
SPITZBERGEN
Alert
Resolute Bay
Grönlandsee
Baffin Bay
NUNAVUT
Nordwestpassage
Hudsonbai
Grönland
Island
Labradorsee
BRITISCH-KOLUMBIEN
ALBERTA
SASKATCHEWAN
MANITOBA
NEVADA
MONTANA
UTAH
WYOMING
ARIZONA
NORDDAKOTA
COLORADO
SÜDDAKOTA
NEW MEXICO
USA
MINNESOTA
ONTARIO
KANSAS
WISCONSIN
OKLAHOMA
MISSOURI
MICHIGAN
ARKANSAS
INDIANA
QUÉBEC
NEUFUNDLAND UND LABRADOR
Los Angeles
San Diego
Dallas
Mexiko
Houston
Mexiko-Stadt
Toronto
Montreal
LOUISIANA
TENNESSEE
NEW YORK
NB
Nordsee
Ostsee
Schwarzes Meer
Kaspisches Meer
Moskau
Москва
Finnland
Schweden
Lettland
Litauen
Ukraine
Georgien
Aserbaidschan
Türkei
Moldawien
Polen
Rumänien
Slowakei
Bulgarien
Ungarn
Serbien
Griechenland
Österreich
Kroatien
Niederlande
Belgien
London
Paris
Irland
Frankreich
Rom
Tyrrhenisches Meer
Mittelmeer
Barcelona
Madrid
Tunesien
Libyen
Wien


Kiel
Rostock
Hamburg
Stettin
Bremen
Continental
Amsterdam
Berlin
Niederlande
Magdeburg
Dortmund
Leipzig
Dresden
Brüssel
Köln
Deutschland
Belgien
Frankfurt
am Main
Prag
Luxemburg
Tschechien
Mannheim
Nürnberg
Audi
BOSCH
Salzburg
Österreich
Zürich
ZF
Graz
Liechtenstein

Why is Privacy in Automotive and Mobility Systems relevant?



Contextual information:
any data that allows to correlate positions or facts with position samples

"Privacy in Inter-Vehicular Networks: Why simple pseudonym change is not enough", WONS 2010

Do Vehicle Positions Identify Users?

Hoh and Gruteser showed that k-means clustering is an effective way to reconstruct home-addresses from vehicle position data



(a) Well clustered destinations

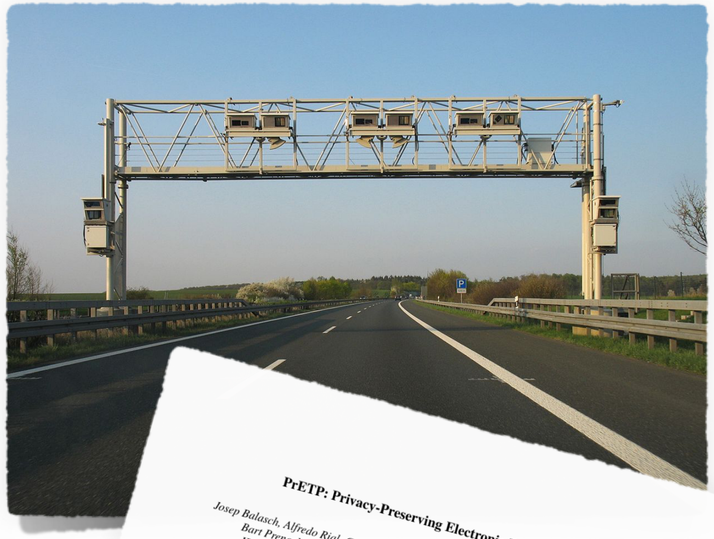
(b) Noisy originations due to GPS signal acquisition delay

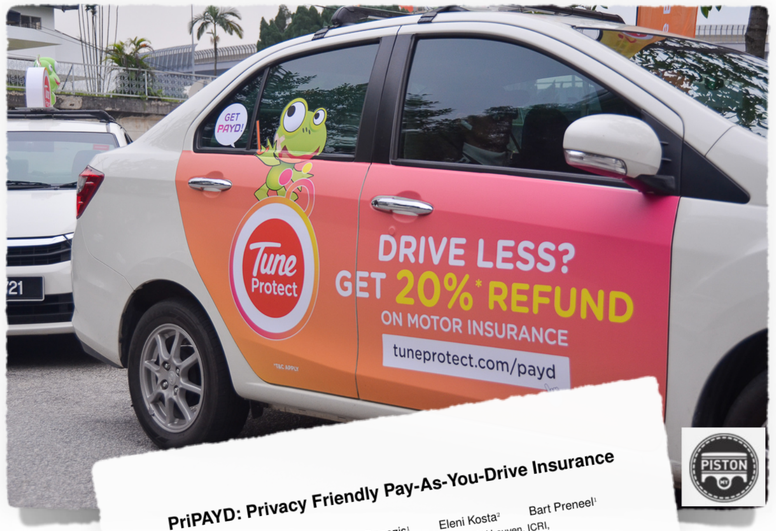
Figure 4.1: Place identification example. Determining which building a driver visited is possible in left scenario because trip endpoints (shown by the markers) cluster denser than nearby homes.

You are where you travel!

Baik Hoh, "Achieving Guaranteed Anonymity in Time-Series Location Data", PhD. Thesis, Rutgers University 2008

Various Stakeholders Interested in Your (Cars) Whereabouts







PrETP: Privacy-Preserving Electronic Toll Pricing

Josep Balasch, Alfredo Rial, Carmela Troncoso, Bart Preneel, Ingrid Verbauwhede
IBBT-K.U.Leuven, ESAT/COSIC.
Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium.
firstname.lastname@esat.kuleuven.be

Christophe Geuens
K.U.Leuven, ICRI.
Sint-Michielsstraat 6, B-3000 Leuven, Belgium.
christophe.geuens@law.kuleuven.be

Abstract

Current Electronic Toll Pricing (ETP) implementations rely on on-board units sending fine-grained location data to the service provider. We present PrETP, a privacy-preserving ETP system in which on-board units can prove that they use genuine data and perform correct operations while disclosing the minimum amount of location data. PrETP employs a cryptographic protocol, Optimistic Payment, which we define in the ideal-world/real-world paradigm, construct, and prove secure under standard assumptions. We provide an efficient implementation of this construction and build an on-board unit on an embedded microcontroller which is, to the best of our knowledge, the first self-contained prototype that supports remote auditing. We thoroughly analyze our system from a security, legal and performance perspective and demonstrate that PrETP is suitable for low-cost commercial applications.

1 Introduction

Vehicular location-based technologies [36, 42] are viewed by governments as a perfect tool to support applications such as electronic toll collection, automated law enforcement, or collection of traffic statistics. In October 2009, the European Commission announced that the current flat road tax system existing in the Member States will be substituted by an European Electronic Toll Service (EETS) [13, 20]. In the United States, there are also ongoing initiatives to introduce *Electronic Toll Pricing* (ETP), as for instance the Regional High Occupancy Toll Network of the California Metropolitan Transportation Commission [1].

ETP allows road taxes to be calculated depending on parameters such as the distance covered by a driver, the kind of road used, or the time of usage. This is beneficial both for citizens and governments. The former pay only for their actual road use, while the latter can improve road mobility by applying "congestion pricing". This strategy assigns prices to roads depending on their traffic density such that driving in congested roads implies a higher cost. This in turn will encourage users to change their route (or even avoid using their vehicles) thus reducing congestion. Moreover, ETP has also environmental benefits as it discourages driving hence reduces pollution.

ETP architectures proposed so far [1, 13, 20] require that vehicles are equipped with an on-board unit necessary for collecting location data. At the end of each tax period, the fee corresponding to those data is computed either remotely [36, 42] or locally [44], and relayed to the service provider. In both cases the service provider needs to be convinced that the fees correspond to the actual road usage of the driver, and that they have been correctly calculated. The verification is straightforward in implementations in which all the location data is sent to the service provider, but this constitutes an inherent threat to users' privacy.

We propose PrETP, a privacy-preserving ETP system in which, without making impractical assumptions, on-board units i) compute the fee locally, and ii) prove to the service provider that they carry out correct computations while revealing the minimum amount of location data. PrETP employs a cryptographic protocol, Optimistic Payment (OP), in which on-board units send along with the final fee commitments to the locations and prices used in the fee computation. These commitments do not reveal information on the locations or prices to the service provider. Moreover, they ensure that drivers cannot claim that they were at any other position, nor used different prices, from the ones used to create the commitments. In order to check the veracity of the committed values, we rely on the service provider having access to a toll gate) that a car was at a specific point at a particular time as previously suggested in [17, 39]. Upon being challenged with this proof, the on-board unit must respond with some information proving that the location

PriPAYD: Privacy Friendly Pay-As-You-Drive Insurance

Carmela Troncoso[1] George Danezis[1] Eleni Kosta[2] Bart Preneel[1]
[1]K.U.Leuven, ESAT/COSIC, Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium.
firstname.secondname@esat.kuleuven.be
[2]K.U.Leuven, ICRI, Sint-Michielsstraat 6, B-3000 Leuven, Belgium.
eleni.kosta@law.kuleuven.be

ABSTRACT

Pay-As-You-Drive insurance systems are establishing themselves as the future of car insurance. However, their current implementations entail a serious privacy invasion. We present PriPAYD where the premium calculations are performed locally in the vehicle, and only aggregate data arrives to the insurance company, without leaking location information. Our system is built on top of well understood security techniques that ensure its correct functioning. We discuss the viability of PriPAYD in terms of cost, security and ease of certification.

Categories and Subject Descriptors

C.3 [**Computer Systems Organization**]: Special-purpose and application-based systems—*Real-time and embedded systems*; J.1 [**Computer Applications**]: Computers in other systems—*Consumer products*

General Terms

Design, Security, Legal Aspects

Keywords

Privacy, Car Insurance, Pay-as-you-drive

1. INTRODUCTION

Insurance is a large percentage of the cost of owning a car. In order to decrease costs for both owners and insurers, insurance companies have developed Pay-As-You-Drive (PAYD) (or Pay-Per-Mile) models. In contrast to the current pay-by-the-year policy, customers are charged depending on where and when they drive, instead of a fixed amount per year. For each kilometer that a car is driven the statistical risk of accident, depending on the road and the time of the day, is calculated and translated to personalized insurance fees. To make possible the estimation of the monthly premium by the client, the fares applied for the billing are made public beforehand. Depending on the policy followed by the insurer these fares can be: price per type of road, price per time of driving, . . .

Pay-As-You-Drive insurance models are hailed as the future of car insurance due to their advantages for users and companies [22, 42]. First, the insurance fees applied to each user are fairer than the ones in the pay-by-the-year scheme, as customers are only charged for the actual kilometers they travel. Customers can also reduce their monthly bill by choosing cheap itineraries or by just not using their car. This makes vehicle insurance affordable for lower-income car users (e.g. young people) or for people who wish to have a second vehicle. Second, PAYD policies are socially beneficial, as they encourage responsible driving, decreasing the risk of accidents, which in turn saves money for users and insurers (aside from saving lives). Finally, PAYD has an environmental benefit, as it discourages driving, hence reduces energy consumption and pollution emissions. Due to all these advantages, PAYD insurance companies all by motorist associations like the National Motorist Association [9] and the American Automobile Association [8]; and they are being widely developed by insurance companies all over the world like Norwich Union [38] (UK), Aioi [1], Toyota [12] (Japan), Hollard Insurance [19] (South Africa), etc.

Although PAYD insurance seems to have many advantages, its current implementations involve an inherent threat to user's privacy. The full information used for billing (the time and position where the car was) is gathered by a black box in the car, and transferred to the insurance company (and, in some of the cases, to a third company providing the location infrastructure). In this model, the insurance company has the ability to track any of its users with ease and precision.

We propose PriPAYD a privacy friendly scheme, where the premium computation is done in the car's black box, and only the minimum information necessary to bill the client is received by the insurance company. We provide an overview of our architecture, where well understood techniques are combined to give assurance to the user that the insurance company does not get more information than necessary, while granting him (or a judge in case of dispute) access to all the data. Our techniques also permit easy management and enforcement of the policies by the insurer. A similar case has been pointed by LeMay et al. in [18] in the field of electric metering, where a remote billing system that preserves user privacy against the electric company and cavesdroppers is proposed.

The rest of the paper is organised as follows: Sect. 2 presents a survey on the current implementations of PAYD

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.
WPES'07, October 29, 2007, Alexandria, Virginia, USA.
Copyright 2007 ACM 978-1-59593-883-1/07/0010 ...$5.00.

POPCORN: Privacy-Preserving Charging for eMobility

Christina Höfer
University of Twente, The Netherlands
c.n.hofer@alumnus.utwente.nl

Jonathan Petit
University of Twente, The Netherlands
j.petit@utwente.nl

Robert K. Schmidt
DENSO AUTOMOTIVE Deutschland GmbH
r.schmidt@denso-auto.de

Frank Kargl
University of Ulm, Germany & University of Twente, NL
frank.kargl@uni-ulm.de

ABSTRACT

Upcoming years will see a massive deployment of electric vehicles and, combined with this, of charging infrastructure. This will require protocols and standards that will control authentication, authorization, and billing of electric-vehicle charging. The ISO/IEC 15118 protocol that addresses the communication between the charging station and the vehicle is going to play an important role, at least in Europe. While it foresees security protection, it does not specify any measures for privacy protection, if there are no significant mechanisms for privacy protection in place. In this paper, we investigate the privacy protection of ISO/IEC 15118 and the surrounding charging and payment infrastructure by means of a Privacy Impact Assessment (PIA). Based on this we propose modular extensions of the protocol applying state-of-the-art Privacy Enhancing Technologies like anonymous credentials to come to a system with maximum privacy protection. We conducted a second PIA to show the benefits compared to the original ISO/IEC 15118. We also describe a proof-of-concept implementation of our system based on a model of electric vehicle and charging station that shows the feasibility of our approach and allows a first preliminary analysis of performance and other issues.

Categories and Subject Descriptors

C.2.0 [**COMPUTER-COMMUNICATION NETWORKS**]: General—*Security and protection*

General Terms

Design, Security

Keywords

Electric vehicle charging, ISO/IEC 15118, security, privacy, privacy enhancing technologies

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or to publish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
e-Energy'13, November 4, 2013, Berlin, Germany.
Copyright 2013 ACM 978-1-4503-2407-8/13/11 ...$15.00.
http://dx.doi.org/10.1145/2517968.2517971.

1. INTRODUCTION

Mobility in the future has to become more eco-friendly. Especially, in urban scenarios the move towards electric mobility is already starting to become visible. This will bring along a fundamental transformation of the way how our transportation systems work, especially as electric vehicles will have to recharge much more often compared to the refueling of traditional cars. Charging of *Electric Vehicles (EVs)* is a central aspect of the electric vehicle infrastructure and a lot of attention is given to fast and widely available charging opportunities. Ideally, fast and widely available charging will be as simple as parking – just park, plugin, and charging begins. Still, for charging control, authorization, and billing purposes a lot of information has to be exchanged automatically between the EV and the *Electric Vehicle Supply Equipment (EVSE)* also simply known as *charging station/spot (CS)*. Especially the simple interaction for the payment requires a thorough setup of the EVSE. Moreover, frequent charging will also include frequent payments. The payment should be done without user-interaction for convenience. In the context of ongoing standardization efforts like ISO TC 22/IEC TC 69, it is manifesting that in the future certain roles of actors in the backend system will be concerned with security and privacy-related processes. Particularly, for the charging management related protocols to perform load management, billing and clearing, as well as certification and payment, standards are defined or in the standards. While security is already considered so far, privacy protection has never been considered analysis of ISO/IEC 15118 and proposes modular privacy enhancements that lead to a fully privacy-preserving charging protocol for electric vehicles.

Next, we first briefly summarize the charging scenario and outline the relation between the different actors as follows. The ISO/IEC 15118 standard already defines a number of different payment options. Assuming the user wants to benefit from the most user-friendly charging management defined by ISO/IEC 15118, a contract with a so-called *Mobility Operator (MO)* has to be concluded in advance. In this simplest form, the MO can be the utility provider of the user that will collect charging fees together with the monthly energy bill. However, the MO can also be a separate entity that

Images: Klaus Foehl & Brbbl, Wikicommons, CC BY-SA 3.0 / piston.my

Solutions in Reality?

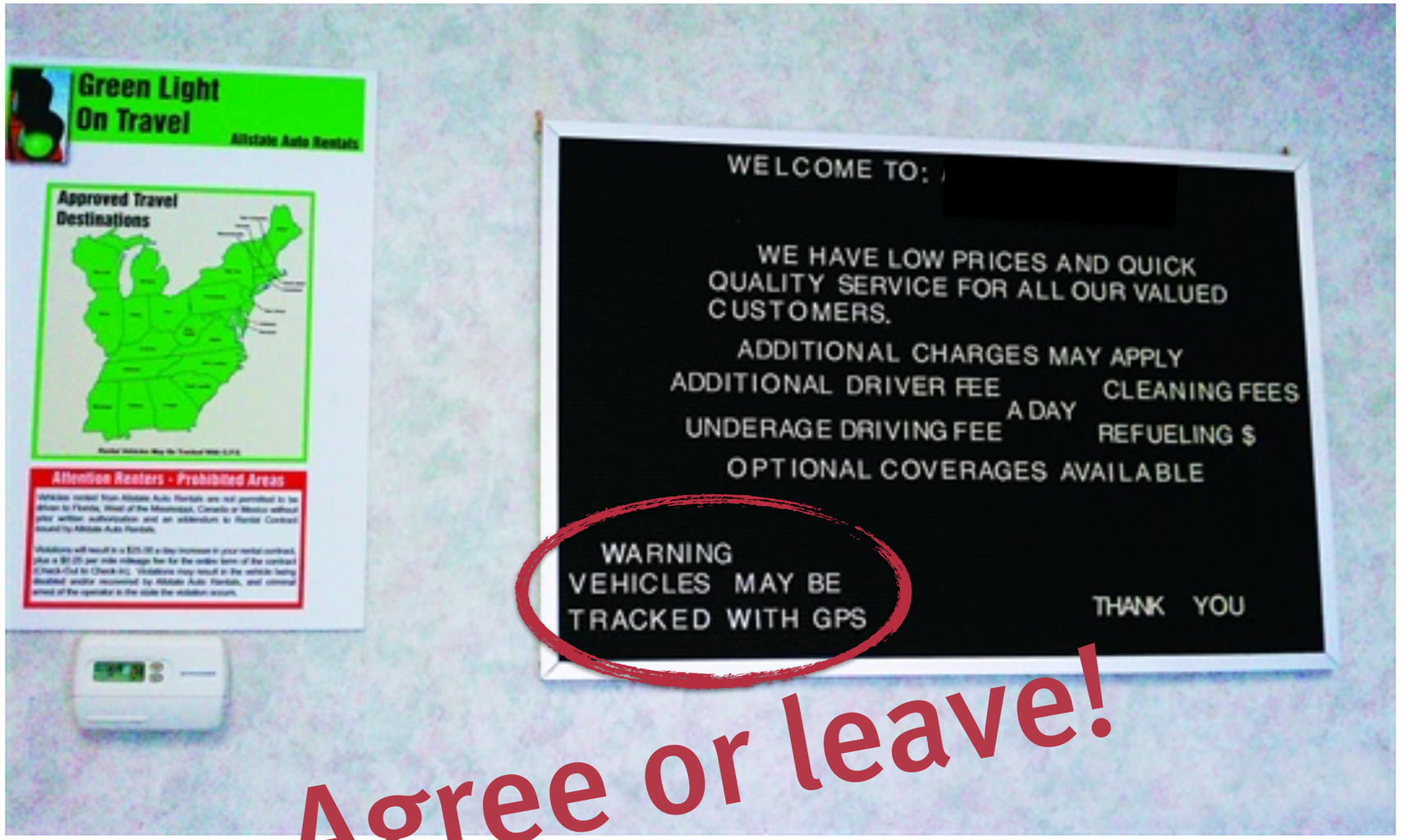


Image: https://www.autorentalnews.com/147811/gps-tracking-the-right-way-disclosure-fees-and-recovery

Drivers and Industry are Both Concerned

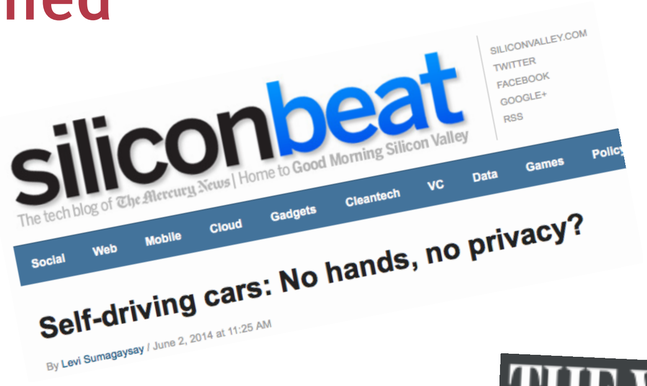
"Self-driving cars are a privacy nightmare. And it's totally worth it."
Washington Post (May 21, 2013)

75% concerned that automated cars may collect personal data,

70% concerned that their data is forwarded to government,

81% very concerned that hackers my take control of self-driving car
(Survey by Alliance of Automobile Manufacturers)


Los Angeles Times
Consumer group says self-driving cars pose privacy risk
May 30, 2012 | By Jerry Hirsch
A consumer group says a bill that would allow self-driving cars on California's roads does not do enough to protect privacy.
The bill, SB 1298, sponsored by Sen. Alex Padilla (D-Pacoima), has passed the California Senate and is awaiting Assembly consideration in June. It establishes guidelines for "autonomous vehicles" to be tested and operated in California.
State Sen. Alex Padilla drives Google's autonomous car. A consumer... (California State Senate...)


siliconbeat
The tech blog of The Mercury News | Home to Good Morning Silicon Valley
Self-driving cars: No hands, no privacy?
By Levi Sumagaysay / June 2, 2014 at 11:25 AM


THE WALL STREET JOURNAL.
June 3, 2013, 1:46 PM ET
The Big Worry About Driverless Cars? Losing Privacy


SPIEGEL ONLINE NETZWELT
VW-Chef zur Cebit-Eröffnung: "Das Auto darf nicht zur Datenkrake werden"


TITELTHEMA
BIG BROTHER AN BORD
Nichts bleibt geheim. Wo Sie fahren, wie schnell Sie sind, wo Sie stehen bleiben – alles wird registriert. Viele Überwachungsgeräte zeichnen es auf. Vor allem Ihr Auto, das die Infos nur allzu gern weitergibt.



Institut für Verteilte Systeme
Institute of Distributed Systems



ulm university universität ulm







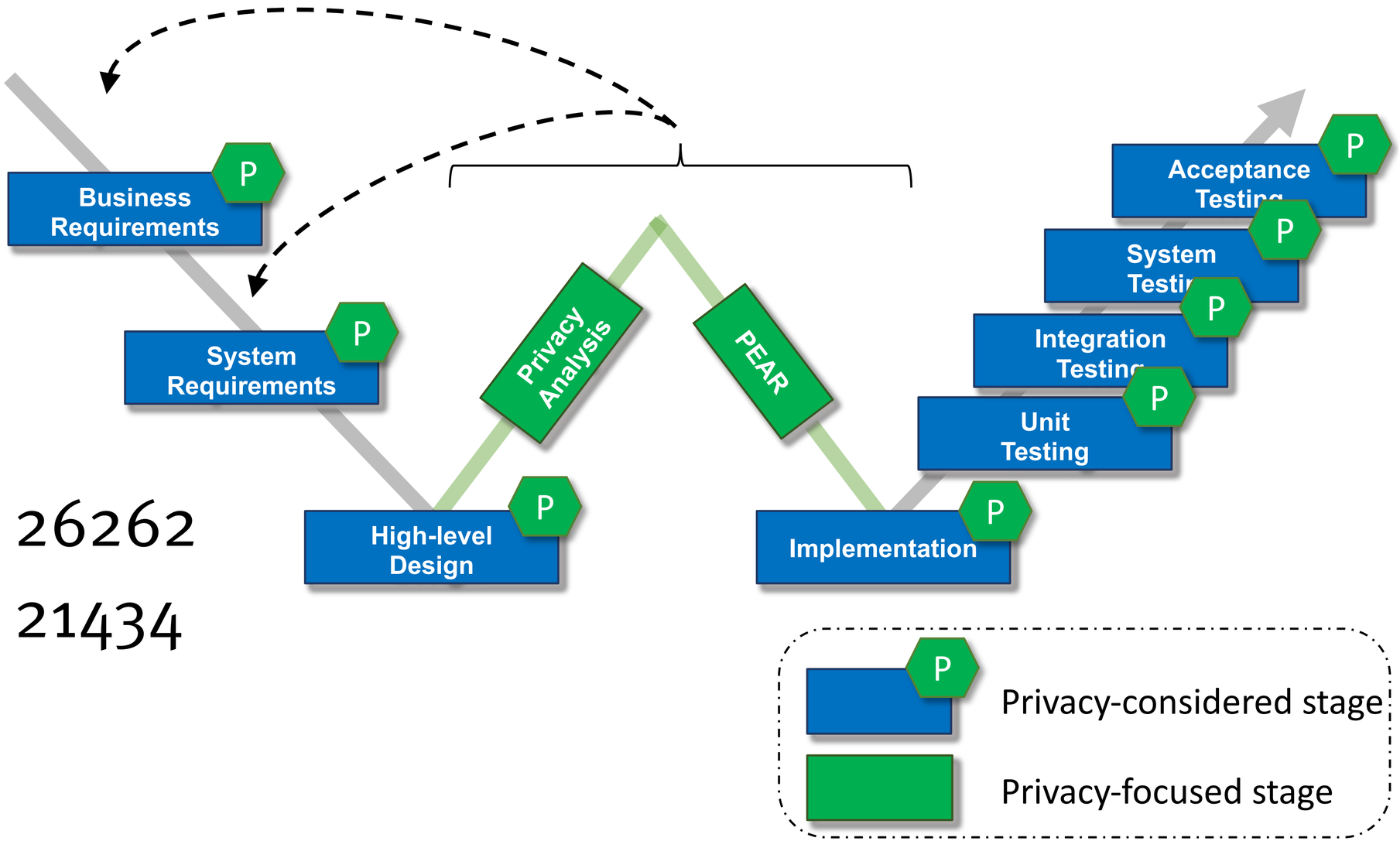




2005

Why are none of our nice academic solutions used out there?

Observation 1: Privacy Engineering Needs to Integrate into Overall Processes



+ ISO 26262

+ ISO 21434

+ ...

A Privacy-Aware V-Model for Software Development, IWPE 2019

Observation 2: Agile Development May Complicate Things Further

Privacy technologies need to go to the gym

on the challenges of privacy engineering in an AGILE world



Carmela Troncoso

SPRING
SECURITY AND PRIVACY ENGINEERING LABORATORY

EPFL

Joint work with Seda Güerses (TU Delft) and Blagovesta Pirelli (EPFL)

C. Troncoso, „Privacy technologies need to go to the gym - on the challenges of privacy engineering in an Agile World, IWPE 2019 Keynote

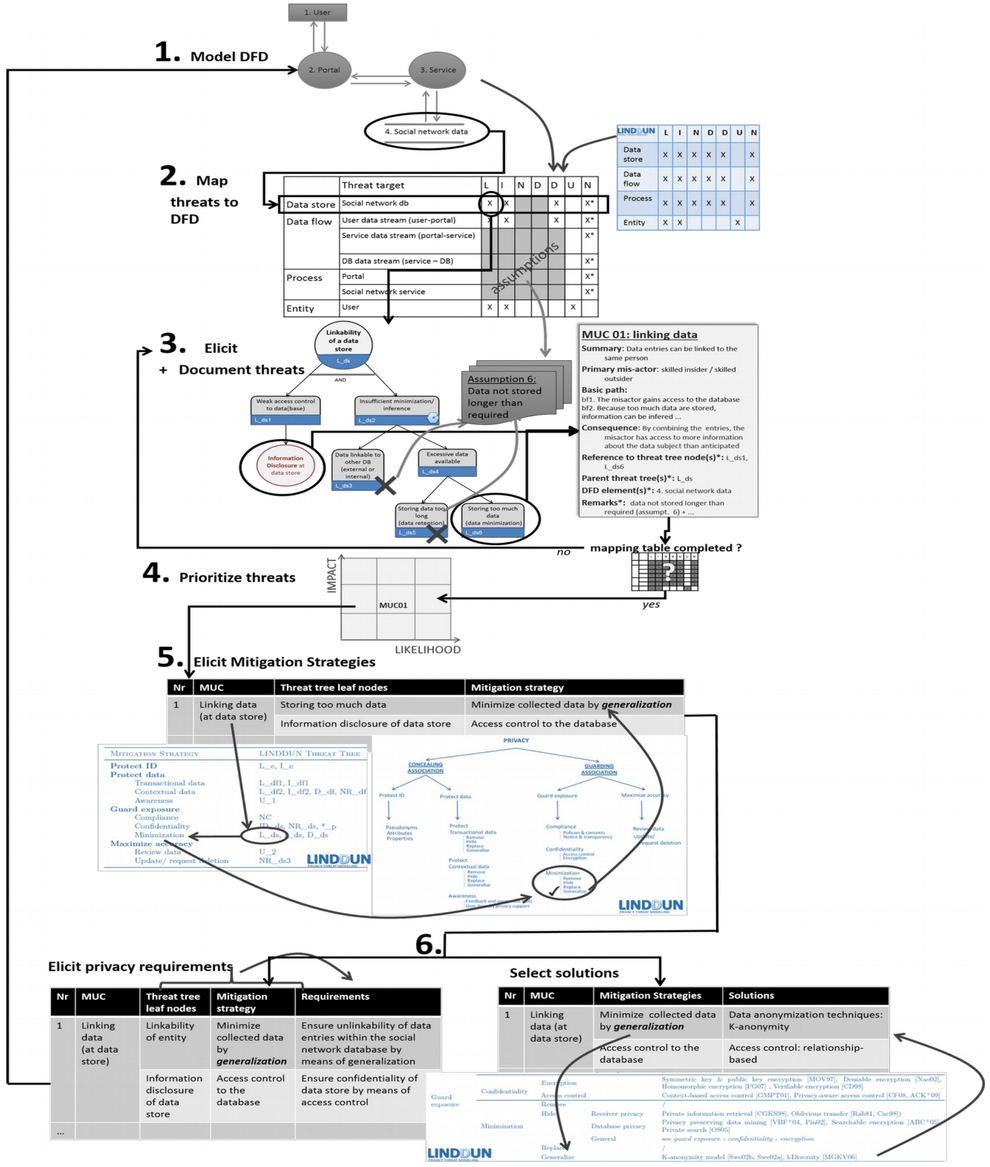
Observation 3: Aligning Security and Privacy Helps Integration

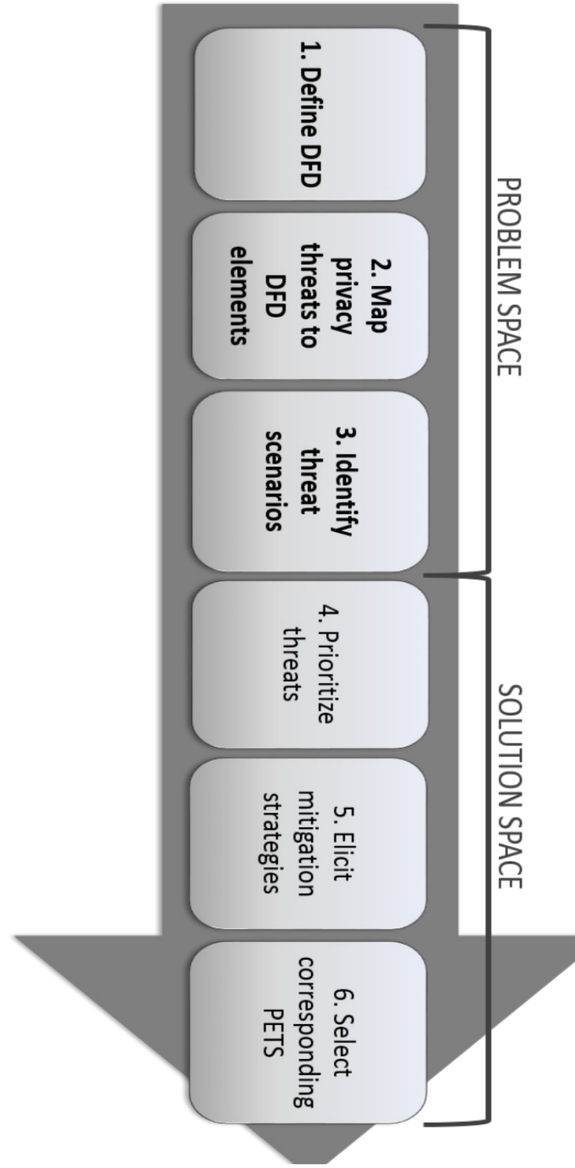
Security Risk Analysis



Risk-based Privacy Engineering Approach (e.g., LINDDUN)

avoids duplicate work





Observation 4: Limited Privacy Knowledge in Car Companies

Anonymization

PETs

GDPR

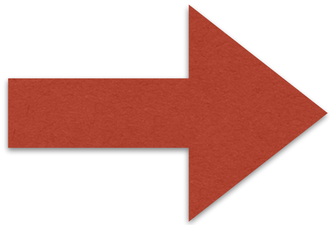
Anonymous Credentials

Privacy

DPIA

Differential Privacy

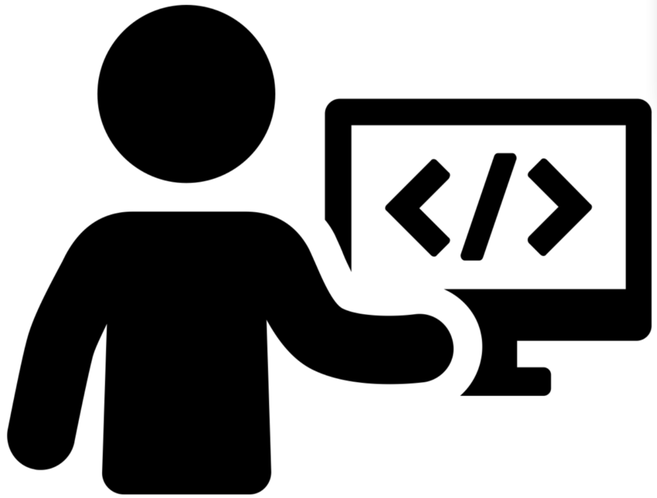


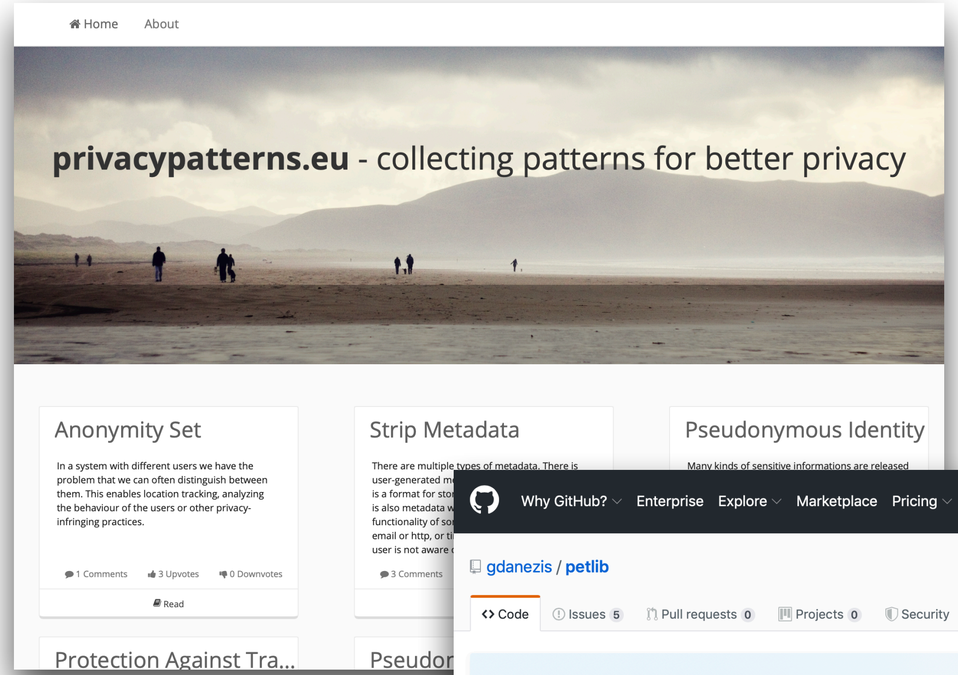


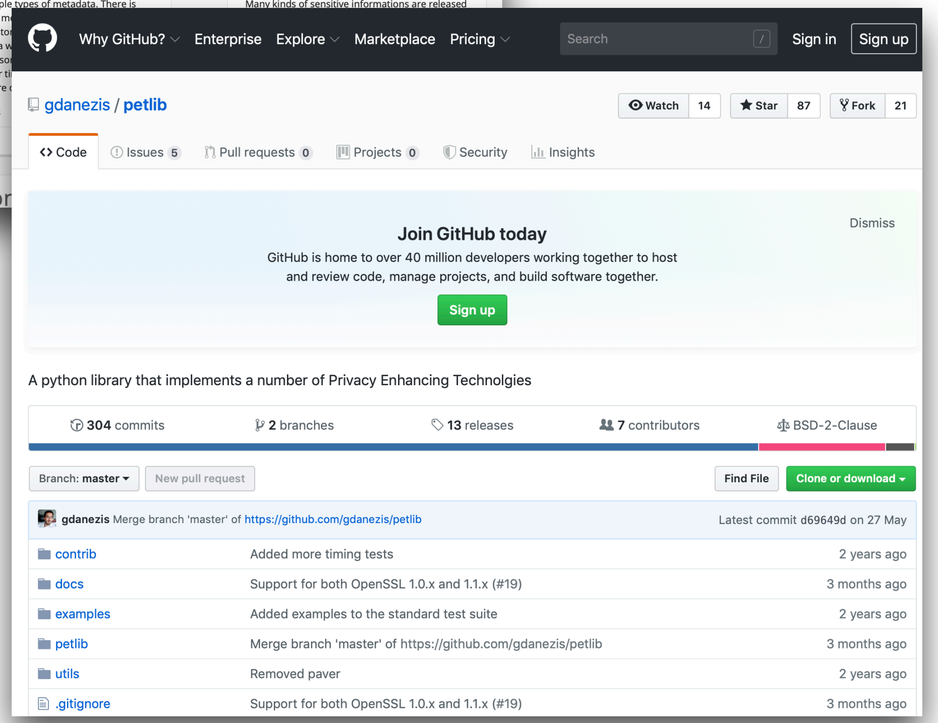
Training

Simplifying Solutions

Observation 4: Limited Privacy Knowledge in Car Companies

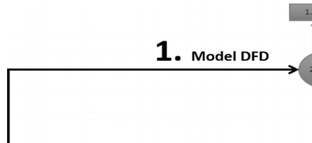






Observation 4: Limited Privacy Knowledge in Companies

Solution Trees simplify PETs selection



1. Model DFD

2. Map threats to DFD

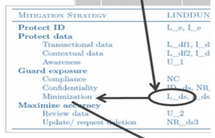
Protect ID

3. Elicit + Document threats

4. Prioritize threats

5. Elicit Mitigation

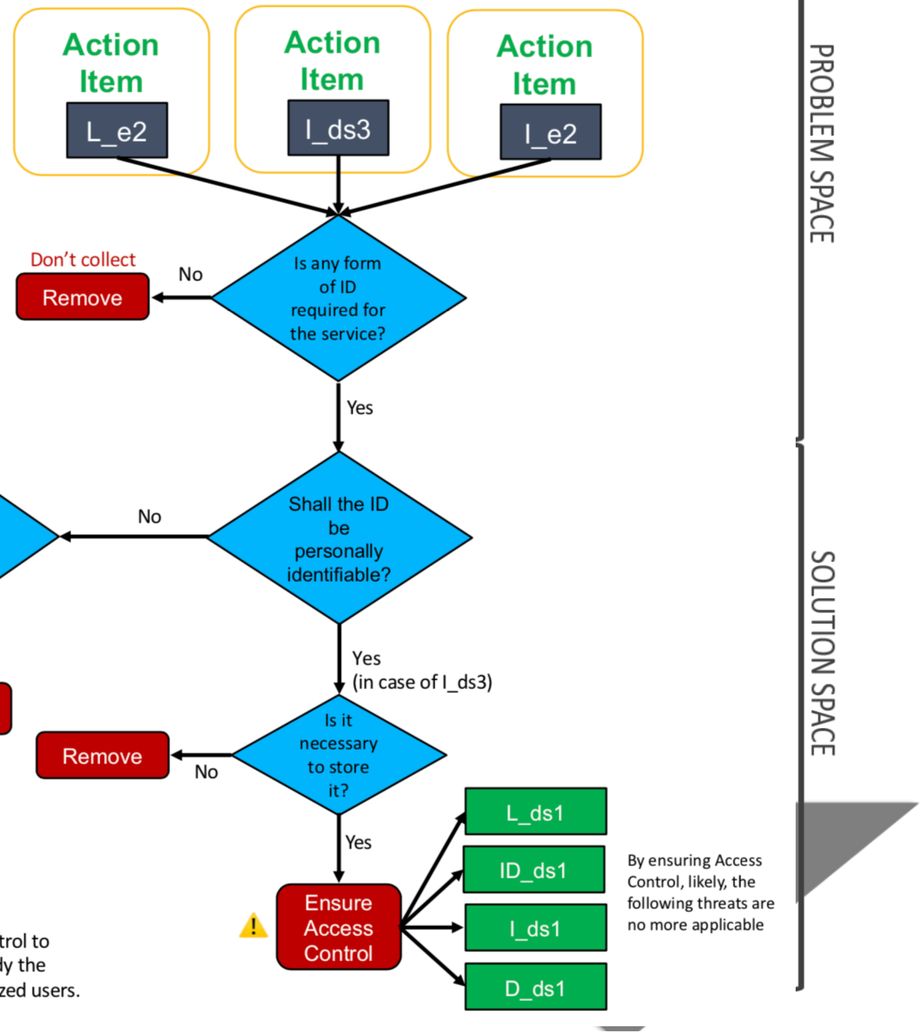
Nr	MUC	Thre
1	Linking data (at data store)	Stori
		Infor



Elicit privacy requirements

Nr	MUC	Threat tree leaf nodes	Mitigation strategy
1	Linking data (at data store)	Linkability of entity	Minimize collected data by ***generalization***
		Information disclosure of data store	Access control to the database
...			





⚠ The access control here refers to the classical security access control to achieve authorization. This kind of access control does not remedy the privacy threats but limits the exposure of data to specific authorized users.

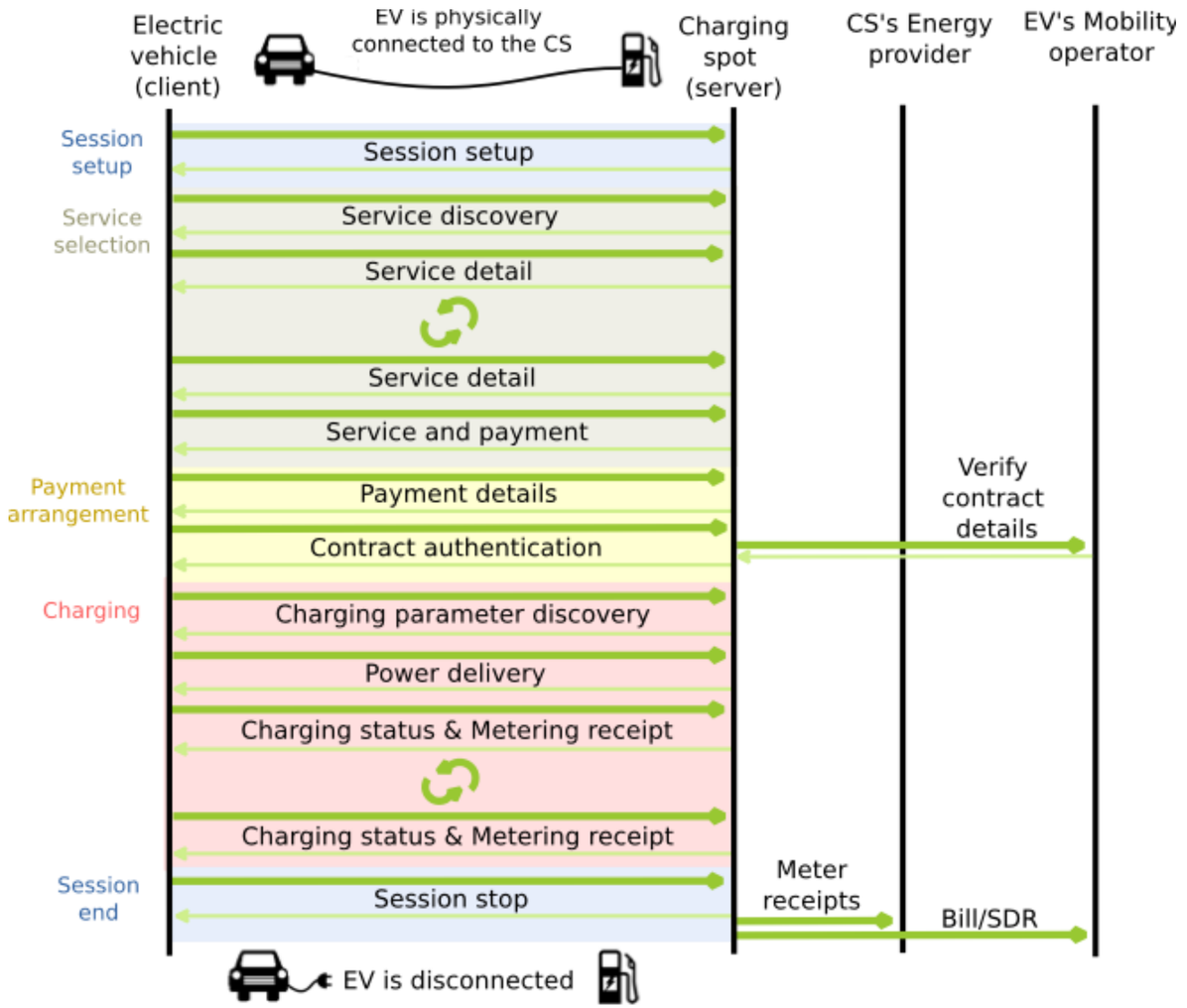
Case-Study: Electric Vehicle Charing and ISO/IEC 15118



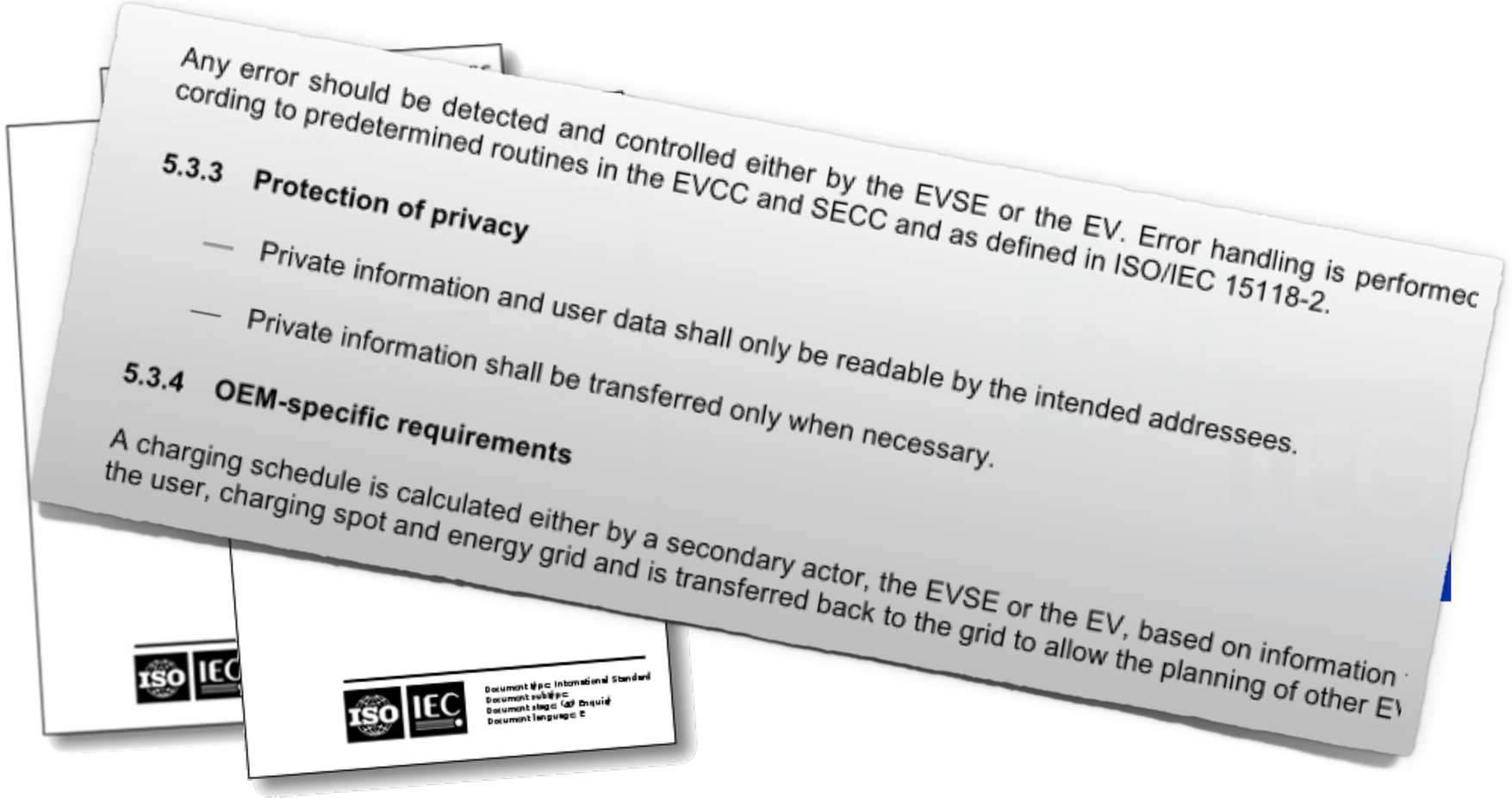
Image: Wikicommons, Author Brbbl, CC BY-SA 3.0

ISO/IEC 15118 - Voting Draft 2011/12

ISO/IEC 15118 for Electric Vehicle Charging AAA & billing



ISO/IEC 15118 - Voting Draft 2011/12



Any error should be detected and controlled either by the EVSE or the EV. Error handling is performec
cording to predetermined routines in the EVCC and SECC and as defined in ISO/IEC 15118-2.

5.3.3 Protection of privacy

— Private information and user data shall only be readable by the intended addressees.

— Private information shall be transferred only when necessary.

5.3.4 OEM-specific requirements

A charging schedule is calculated either by a secondary actor, the EVSE or the EV, based on information
the user, charging spot and energy grid and is transferred back to the grid to allow the planning of other EV

POPCORN

Privacy-Preserving ChaRgiNg for e-mobility

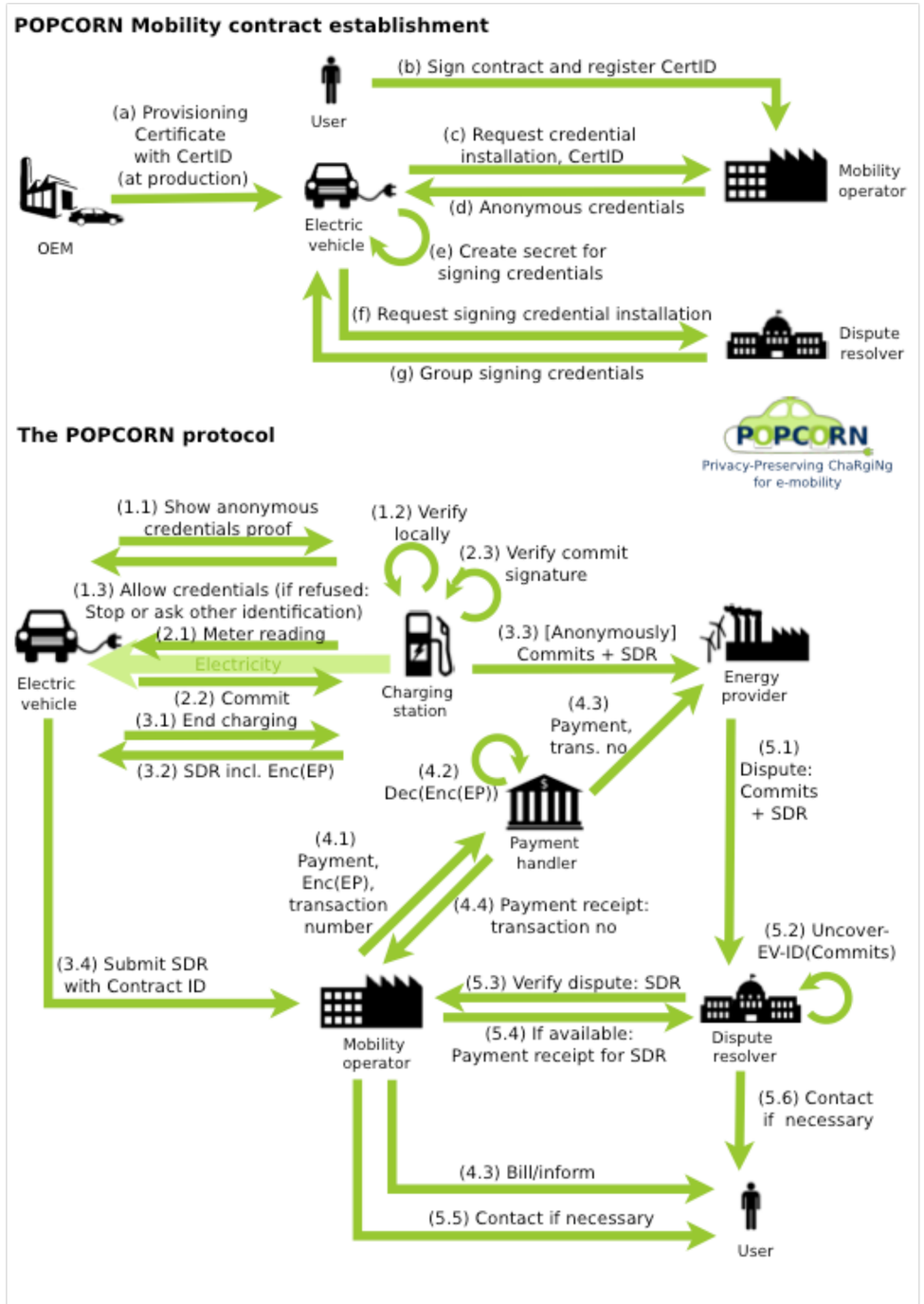
Minimization

Anonymous Credentials

Group Signatures

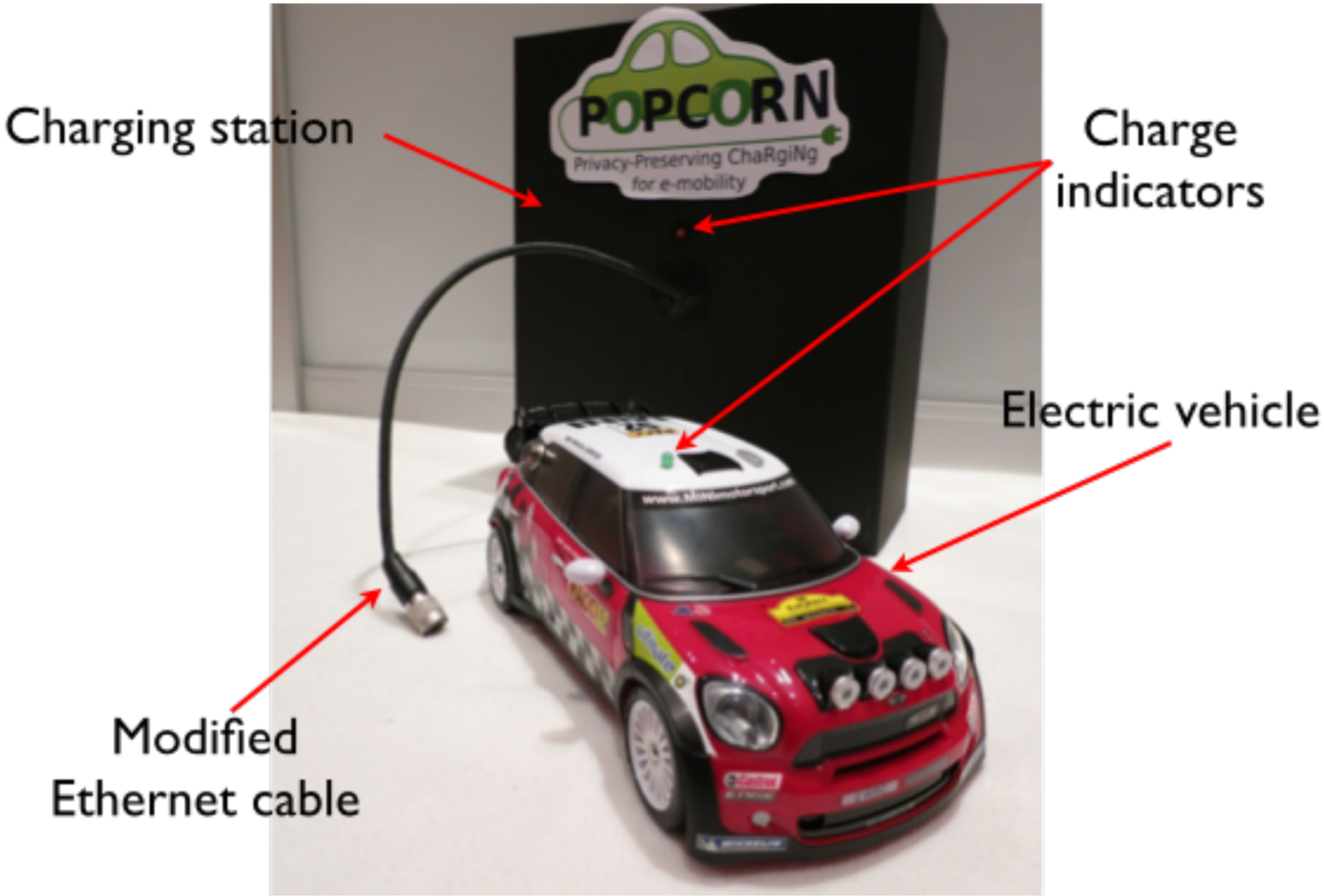
…

POPCORN provides step-wise privacy enhancements for ISO/IEC 15118 using state-of-the-art PETs

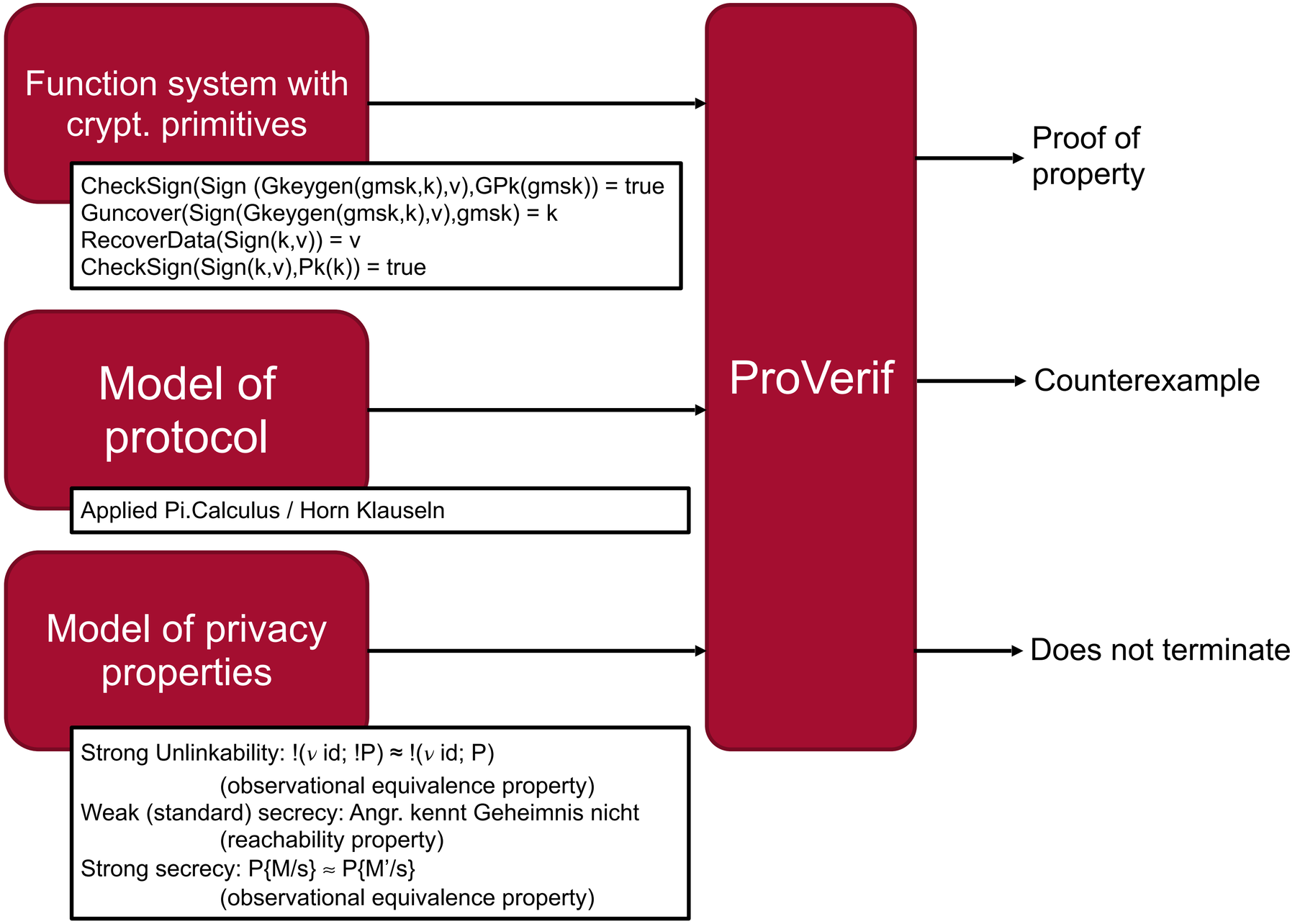


"POPCORN: Privacy-Preserving Charging for eMobility", ACM CCS CyCar 2013

Prototype


Charging station
Charge indicators
Electric vehicle
Modified Ethernet cable
POPCORN
Privacy-Preserving ChaRgiNg for e-mobility

Formal Proof with ProVerif



"Formal Verification of Privacy Properties in Electric Vehicle Charging", ESSOS 2015

Formal Proof with ProVerif

POPCORN
Privacy-Preserving ChaRgiNg for e-mobility 2.0

	Proven	Not proven
Weak secrecy (EV, MO)	✔	
Strong secrecy (EV, MO)	✔	
Resistance to offline guessing (EV, MO)	✔	
Anonymity (EV)	✔ ←	✘
Strong Unlinkability (EV)	✔ ←	✘
Weak Secrecy (EP)	✔ ←	✘

"Formal Verification of Privacy Properties in Electric Vehicle Charging", ESSOS 2015

How did Industry React?

Conclusions

Observation 1: Privacy Engineering Needs to Integrate into Overall Processes

– Think Privacy Engineering beyond only Privacy

Observation 2: Agile Development May Complicate Things Further

– Privacy engineering needs to become agile itself

Observation 3: Aligning Security and Privacy Helps Integration

– Reuse artifacts (like DFDs, Risk Analysis) where possible

– Think of joined teams

Observation 4: Limited Privacy Knowledge in Companies

– Motivation and training necessary

– Simplify good privacy practice

Institut für Verteilte Systeme
Institute of Distributed Systems

ulm university universität
uulm



Discussion

Frank Kargl | PEPR'19 | 2019-08-12