

Privacy and Security in Smart Energy Grids

Edited by

George Danezis¹, Stefan Katzenbeisser², Christiane Peters³, and
Bart Preneel⁴

1 University College London, GB, g.danezis@ucl.ac.uk

2 TU Darmstadt, DE, skatzenbeisser@acm.org

3 IBM Belgium, BE, christiane.pascale.peters@gmail.com

4 KU Leuven, BE, bart.preneel@esat.kuleuven.be

Abstract

This report documents the program and the outcomes of Dagstuhl Seminar 16032 “Privacy and Security in Smart Energy Grids”. Smart electricity grids augment the electricity distribution network with modern communications and computerized control to improve efficiency, reliability, and security of electricity distribution, and more flexible production. This initiative has been greeted by consumers and utilities not only with enthusiasm but also concern. Consumers worry about their privacy. Utilities worry about the security of their assets. These outcries and reactions have triggered academics and industry to look into designing privacy friendly architectures for smart metering. The Dagstuhl Seminar 16032 brought together academic researchers as well as utility experts in order to start an open dialogue on smart grid privacy and security problems and potential solutions to support customers and utilities. A particular focus of the seminar were problems related to two timely use-cases for the smart grid, namely smart charging of electric vehicles and distribution automation.

Seminar January 17–20, 2016 – <http://www.dagstuhl.de/16032>

1998 ACM Subject Classification K.6.5 Security and Protection

Keywords and phrases Critical infrastructure protection, smart energy grids

Digital Object Identifier 10.4230/DagRep.6.1.99


1 Executive Summary

George Danezis

Stefan Katzenbeisser

Christiane Peters

Bart Preneel

License  Creative Commons BY 3.0 Unported license
© George Danezis, Stefan Katzenbeisser, Christiane Peters, and Bart Preneel

Smart electricity grids augment the electricity distribution network with modern communications and computerized control to improve efficiency, reliability, and security of electricity distribution, and more flexible production. This initiative has been greeted by consumers and utilities not only with enthusiasm but also concern. Consumers worry about their privacy. Utilities worry about the security of their assets.

Consumer organizations across the globe protested against smart meters and smart homes collecting all their data, warning that security breaches in the databases of the utilities would expose privacy-critical data to attackers, or open to secondary uses leading to increased insurance premiums, behavioral advertising or privacy invasion. These outcries and reactions



Except where otherwise noted, content of this report is licensed under a Creative Commons BY 3.0 Unported license

Privacy and Security in Smart Energy Grids, *Dagstuhl Reports*, Vol. 6, Issue 1, pp. 99–107

Editors: George Danezis, Stefan Katzenbeisser, Christiane Peters, and Bart Preneel



Dagstuhl Reports

Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

have triggered academics and industry to look into designing privacy friendly architectures for smart metering.

The seminar 16032 in particular focused on the two use cases of smart charging of electric vehicles (EVs) and distribution automation. The seminar discussed these use cases with respect to the following challenges:

- security architectures,
- secure and privacy-friendly communication, and
- hardware and software security for constrained devices in the smart grid.

Smart Charging: Charging of electric vehicles is the next big challenge for privacy and security researchers: smart charging algorithms try to minimize loads on the grid by collecting various kinds of customer data, making it easy to reserve charging spots and book charge frequencies using smart-phone apps. The main motivation behind smart charging is to save copper for cables to match the load demands, given that an electric vehicle draws as much as a full household. Cables are designed to satisfy the demands at peak times. So profiling customers helps to foresee these demands and to calculate the cost of the needed grid infrastructure. Moreover, the cable designs use prediction algorithms to optimize loads, while assigning low priority to privacy issues, security architectures, and secure communication protocols.

Distribution Automation: Another problem lies in the task of automated electricity distribution. In a smart grid, safety critical events in transformer stations can be monitored and operated remotely. Adding communication also exposes assets to new vulnerabilities and attacks. Grid components are controlled by dedicated devices that pose a challenge in terms of their storage and computation capacities. Moreover, as with any critical infrastructure, security often conflicts with safety. As a consequence security often does not play any role in the design of communication protocols and devices, supported by the argument that most devices reside in physically protected substations. However, providing such physical security is expensive and hackers do not need physical access to the grid operator sites if they are connected to the utility's IT network.

The goal of this seminar was thus (i) to raise awareness of these critical problems affecting every European citizen now or at least in the foreseeable future, and (ii) to bring together academic researchers as well as utility experts in order to start an open dialogue on smart grid privacy and security problems and potential solutions to support customers and utilities.

2 Table of Contents

Executive Summary

George Danezis, Stefan Katzenbeisser, Christiane Peters, and Bart Preneel 99

Overview of Talks

In praise of distributed trusted computing bases

George Danezis 102

EV Smart Charging Security Architectures

Benessa Defend 102

Lessons Learned from Implementing Privacy-Preserving Protocols for Smart Meters

Benessa Defend 102

The Interplay of Data Resolution and Privacy in Smart Metering

Dominik Engel 103

α -Signatures: Some observations on the integrity of measurements in the privacy-preserving smart grid

Florian Kerschbaum 103

Field experiences with securing RTUs

Carlos Montes Portela 104

Smart Charging of EVs

Carlos Montes Portela 104

Charging my EV at my Friend's House

Mustafa Mustafa 105

Security of EV charging

Erik Poll 105

What about the software?

Erik Poll 106

Participants 107

3 Overview of Talks

3.1 In praise of distributed trusted computing bases

George Danezis (University College London, GB)

License  Creative Commons BY 3.0 Unported license
 © George Danezis

The Trusted Computing Base (TCB) is a foundational concept in computer security, defining the set of hardware, software and processes that need to be protected from the adversary to ensure the security properties of the system are not violated. However, the TCB as a monolithic entity is rather old fashioned. These days the integrity and confidentiality of the TCB is instead preserved through distributing the functionality across a number of components, each of which could fail. Such distributed TCBs have proved to be robust against extremely motivated and well-resourced adversaries, but engineering them remains a technical and cryptographic challenge.

3.2 EV Smart Charging Security Architectures

Benessa Defend (ENCS – The Hague, NL)

License  Creative Commons BY 3.0 Unported license
 © Benessa Defend

Joint work of Defend, Benessa; Montes Portela, Carlos; Kursawe, Klaus

We present an overview of the electric vehicle (EV) charging architecture from generation to consumption. The architectural overview includes various key stakeholders and shows the information flows between multiple parties for charging and billing purposes. We zoom in on the components inside EV charging stations and explore a number of threat scenarios from theft of charging cables to large-scale attacks on charging stations that could lead to a blackout. The talk closes with security considerations from the point of view of electricity grid operators whose objective is to maintain a balanced electricity grid with minimal outages.

3.3 Lessons Learned from Implementing Privacy-Preserving Protocols for Smart Meters

Benessa Defend (ENCS – The Hague, NL)

License  Creative Commons BY 3.0 Unported license
 © Benessa Defend

Main reference B. Defend, K. Kursawe, “Implementation of privacy-friendly aggregation for the smart grid”, in Proc. of the 1st ACM Workshop on Smart Energy Grid Security, pp. 65–74, ACM, 2013.

URL <http://dx.doi.org/10.1145/2516930.2516936>

This talk provides an update on the privacy-preserving smart meter aggregation activities that have continued since Dagstuhl Seminar 11511 that was held in December 2011. One of the privacy-preserving protocols developed by Kursawe et al. [1] was implemented on four real smart meters in collaboration with a smart meter manufacturer. Based on the success of this demonstration we teamed up with an electricity grid operator to conduct scalability and integration tests on 100 meters. We also cover several lessons-learned, including the importance of understanding use cases, framing privacy as a business enabler,

and the importance of good security metaphors. Currently the privacy-preserving aggregation protocol has been submitted to the DLMS/COSEM smart meter standard as an optional add-on; support from stakeholders is needed in order to finalize the adoption process.

References

- 1 Klaus Kursawe, George Danezis, Markulf Kohlweiss, “Privacy-Friendly Aggregation for the Smart-Grid,” in Privacy Enhancing Technologies Symposium’ (PETS), pp. 175–191, 2011.
- 2 Benessa Defend, Klaus Kursawe, “Implementation of privacy-friendly aggregation for the smart grid,” in SEGS@CCS 2013, pp. 65–74, 2013.

3.4 The Interplay of Data Resolution and Privacy in Smart Metering

Dominik Engel (FH Salzburg, AT)

License © Creative Commons BY 3.0 Unported license
© Dominik Engel

Joint work of Eibl, Günther; Engel, Dominik

Main reference D. Engel, G. Eibl, “Wavelet-Based Multiresolution Smart Meter Privacy”, IEEE Transactions on Smart Grid, 12 pages, 2015.

URL <http://dx.doi.org/10.1109/TSG.2015.2504395>

Through smart metering load profiles are measured per household. Personal data can be inferred from these load profiles, which has led to privacy concerns. Privacy is expected to increase with longer measurement intervals. In this talk, first the impact of data granularity on edge detection, a first step in appliance detection, is reviewed. Based on these insights, a method for generating multi-resolution representation of load profiles by using the wavelet transform is presented. By using a hierarchical keying scheme and different keys in the different keys on the various resolutions, users can decide which party can access their load profile at which resolution. Finally, open issues and further research directions are discussed.

3.5 α -Signatures: Some observations on the integrity of measurements in the privacy-preserving smart grid

Florian Kerschbaum (SAP SE – Karlsruhe, DE)

License © Creative Commons BY 3.0 Unported license
© Florian Kerschbaum

Main reference F. Kerschbaum, H. W. Lim, “Privacy-Preserving Observation in Public Spaces,” in Proc. of the 20th European Symp. on Research in Computer Security (ESORICS’15), LNCS, Vol. 9327, pp. 81–100, Springer, 2015.

URL http://dx.doi.org/10.1007/978-3-319-24177-7_5

The privacy architecture for the smart grid as put forward by Jawurek, Kerschbaum, Danezis and others hinges on some assumptions. Particularly integrity of measurements is ensured by secure hardware. In this talk I will investigate whether we can relax this assumption by using the concept of α -signatures – an extension of α -authentication introduced by Kerschbaum and Lim at ESORICS 2015.

3.6 Field experiences with securing RTUs

Carlos Montes Portela (Enexis B. V. – 's-Hertogenbosch, NL)

License © Creative Commons BY 3.0 Unported license
 © Carlos Montes Portela
URL <http://www.enecs.eu>

RTU stands for Remote Terminal Unit and is basically a PC for industrial purposes. Distribution System Operators (DSOs) use RTUs in their substations to monitor their electricity grids (eg. measurements of voltage and current levels) or to remotely switch parts of the grid off or on. Typically a master/slave architecture is used, where there is one master (control center of the DSO) and multiple slaves (the RTUs in the substations). The communication from and to the RTUs is done via a standardized protocol: IEC-60870-5-104 also known as the 104 protocol. Performance and reliability have had much more attention from the industry than security. As the number and magnitude of cyber-physical related attacks grows, it becomes more and more important for DSOs to have RTUs that are secure enough to cope with these risks appropriately.

DSO Enexis is rolling out station automation and wants to make sure that security is taken into account upfront. Therefore, ENCS (European Network for Cyber Security) was hired to setup security related requirements that can be used in European tenders. ENCS has delivered a good quality report that has already been used by Enexis during a tender. Other DSOs that are members of ENCS will do the same. As a result, RTU vendors will need to adhere to these requirements in order to win bids.

During this talk the RTU tendering process and the usage of the ENCS security requirements were discussed.

3.7 Smart Charging of EVs

Carlos Montes Portela (Enexis B. V. – 's-Hertogenbosch, NL)

License © Creative Commons BY 3.0 Unported license
 © Carlos Montes Portela
Joint work of Verheijen, Lennart; Klapwijk, Paul; Montes Portela, Carlos; Postma, André
Main reference C. Montes Portela, D. Geldtmeijer, M. van Eekelen, H. Slootweg, “A flexible and privacy friendly ICT architecture for Smart Charging of EV’s,” in Proc. of the 22nd Int’l Conf. on Electricity Distribution (CIRED’13), paper 0199, 2013.
URL http://www.cired.net/publications/cired2013/pdfs/CIRED2013_0199_final.pdf

Building infrastructures for charging electric vehicles (EVs) is a complex task, optimizing counteracting goals. The main aim is maximizing EV driver’s convenience, by using the available charging infrastructure and local grid capacity as efficiently as possible. By controlling the charging process, the DSO could optimize the grid usage and facilitate the integration of RES. Herewith additional investments necessary for (large scale) EV charging could be avoided or at least minimized. This is coined as ‘Smart Charging’ by Eurelectric [2]. During this talk the concept of smart charging has been explained.

Implementing Smart Charging in a liberalized context, calls for an interaction and corresponding information exchange between DSOs, Charge Spots, EVs, EV drivers, energy suppliers and possibly new market participants. Amongst the latter, one could count a Charge Service Provider (CSP) which deals with fulfilling the charge wish of the EV driver and a Charge Spot Operator (CSO), which deals with the operation of the Charge Spots. Without measures, one could derive the charge locations of EVs throughout time. If this

could be coupled to EV drivers, it would then become privacy sensitive data as it reveals the whereabouts of the latter. Based on the negative experiences with privacy during the roll-out of Smart Meters in the Netherlands, this could become a problem for the concept of Smart Charging. Furthermore, the interest of hackers and commercial parties for privacy sensitive data increases the likelihood of disclosure. Lastly, the fact that the proposed marked model for public EV charging is still evolving into its full maturity, calls for an ICT architecture that is flexible enough to deal with future changes. During this talk multiple variants of the evolving role model have been presented.

References

- 1 Montes Portela, Carlos, Geldtmeijer, Danny, van Eekelen, Marko & Slootweg, Han, “A flexible and privacy friendly ICT architecture for Smart Charging of EV’s,” in Proceedings Cired Conference 2013, paper 0199.
- 2 Geldtmeijer, Danny, Hommes, Klaas &, Postma, André, 2011, “Charging EVs in a liberalized electricity market,” in Proceedings Cired Conference 2011, paper 0889.

3.8 Charging my EV at my Friend’s House

Mustafa Mustafa (KU Leuven, BE)

License © Creative Commons BY 3.0 Unported license
© Mustafa Mustafa

Joint work of Mustafa Mustafa, Ning Zhang, Georgios Kalogridis, Zhong Fan

Main reference M. A. Mustafa, N. Zhang, G. Kalogridis, Z. Fan, “Roaming electric vehicle charging and billing: An anonymous multi-user protocol,” in Proc. of the 2014 IEEE Int’l Conf. on Smart Grid Communications (SmartGridComm’14), pp. 939–945, 2014.

URL <http://dx.doi.org/10.1109/SmartGridComm.2014.7007769>

In this talk, I will first briefly introduce the smart grid and how the current electricity markets work. Then, I will present on a high level a secure roaming electric vehicle (EV) charging protocol that helps preserve users’ privacy. This protocol protects the user’s identity privacy from other suppliers as well as the user’s privacy of location from its own supplier. Further, it allows the user’s contracted supplier to authenticate the EV and the user. Using two-factor authentication approach a multi-user EV charging is supported and different legitimate EV users (e.g. family members) can be held accountable for their charging sessions. Finally, I will give some high level ideas on how this protocol can be extended to integrate EV aggregators which could help EV users to participate in the balancing electricity market.

3.9 Security of EV charging

Erik Poll (Radboud University Nijmegen, NL)

License © Creative Commons BY 3.0 Unported license
© Erik Poll

Charging Electric Vehicles (EVs) involves many parties and many information flows between them. Besides privacy concerns, the big impact of EV charging on the grid raises important security concerns w.r.t. grid stability. However, currently little attention is paid to security (more specifically, to authentication and integrity) in protocols for information exchanges to support EV charging.

References

- 1 Fabian van den Broek, Erik Poll, and Bárbara Vieira, “Securing the information infrastructure for EV charging”, International Workshop on Communication Applications in Smart Grid (CASG 2015), LNICST Vol. 154, pp. 61–74, Springer, 2015.

3.10 What about the software?

Erik Poll (Radboud University Nijmegen, NL)

License © Creative Commons BY 3.0 Unported license
© Erik Poll

Joint work of Erik Poll, Joeri de Ruiter, Aleksy Schubert

Main reference E. Poll, J. de Ruiter, A. Schubert, “Protocol state machines and session languages: specification, implementation, and security flaws”, in Proc. of the 2015 IEEE Security and Privacy Workshops (SPW’15), pp. 125–133, IEEE, 2015.

URL <http://dx.doi.org/10.1109/SPW.2015.32>

Software – or rather, the presence of flaws in software – is a major root cause of security problems. Language-theoretic security is a collection of ideas to tackle an important class of security flaws in software, namely flaws in handling (possibly malicious) input. These ideas also seem highly relevant for the protocols using in the smart grids. We used these ideas in fuzzing GSM and in analysing the protocol state machines of TLS.

Participants

- Nikita Borisov
University of Illinois – Urbana
Champaign, US
- George Danezis
University College London, GB
- Benessa Defend
ENCS – The Hague, NL
- Dominik Engel
FH Salzburg, AT
- Zekeriya Erkin
TU Delft, NL
- Benedikt Gierlichs
KU Leuven, BE
- Stefan Katzenbeisser
TU Darmstadt, DE
- Florian Kerschbaum
SAP SE – Karlsruhe, DE
- Erwin Kooi
Alliander – Duiven, NL
- Klaus Kursawe
ENCS – The Hague, NL
- Éireann Leverett
University of Cambridge, GB
- Carlos Montes Portela
Enexis B.V. –
's-Hertogenbosch, NL
- Mustafa Mustafa
KU Leuven, BE
- Christiane Peters
IBM Belgium, BE
- Erik Poll
Radboud University Nijmegen,
NL
- Bart Preneel
KU Leuven, BE
- Ahmad-Reza Sadeghi
TU Darmstadt, DE
- Kazuo Sako
NEC – Kawasaki, JP
- Matthias Schunter
INTEL ICRI – Darmstadt, DE
- Neeraj Suri
TU Darmstadt, DE
- Makoto Takahashi
Tohoku University – Sendai, JP
- Pol Van Aubel
Radboud University
Nijmegen, NL
- Ingrid Verbauwhede
KU Leuven, BE
- Jos Weyers
TenneT – Arnhem, NL

