

Privacy and Security in Smart Energy Grids

Edited by

Stefan Katzenbeisser¹, Klaus Kursawe², Bart Preneel³, and
Ahmad-Reza Sadeghi⁴

1 TU Darmstadt, DE, katzenbeisser@seceng.informatik.tu-darmstadt.de

2 University of Nijmegen, NL, klaus.kursawe@gmail.com

3 K.U. Leuven, BE, Bart.Preneel@esat.kuleuven.be

4 TU Darmstadt, DE, ahmad.sadeghi@trust.cased.de

Abstract

The “smart energy grid” promises to improve the reliability and efficiency of the future energy grid by exchanging detailed usage information between the end consumers and the utilities. This application raises different questions with regard to privacy and security. For instance, detailed meter readings enable to infer detailed information on the private life of the consumers; furthermore, manipulations of meter readings open the possibility of fraud. The goal of the seminar was thus to raise awareness of the privacy and security problems associated with smart meters and 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.

Seminar 18.–21. December, 2011 – www.dagstuhl.de/11511

1998 ACM Subject Classification K.4.1 Computers and Society, Public Policy Issues, Privacy

Keywords and phrases privacy, security, smart grid, digital metrology

Digital Object Identifier 10.4230/DagRep.1.12.62


1 Executive Summary

Klaus Kursawe

Stefan Katzenbeisser

Bart Preneel

Ahmad-Reza Sadeghi

License  Creative Commons BY-NC-ND 3.0 Unported license

© Klaus Kursawe, Stefan Katzenbeisser, Bart Preneel, Ahmad-Reza Sadeghi

The smart grid initiative is an attempt to improve reliability and efficiency of the electricity grid by adding communication and intelligence to its components all the way from end-user devices to the utilities. On the end user side, detailed usage information will be transferred to both home systems and the utilities; the utility can provide load- and pricing information to the meters and end-devices in real time. On the grid side, intelligent systems will allow for a more flexible energy distribution. Naturally, adding smartness to a critical and sizeable infrastructure system such as the electricity grid imposes extreme requirements on security and privacy, while facing numerous conflicting requirements from the different players. In addition, legislation is pushing hard to implement a large scale smart grid in a very short time: In Europe, the commission plans to achieve 80% smart grid coverage by 2020, with some countries starting to roll out meters at a large scale in 2012; in the US, the rollout has already started.



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

Privacy and Security in Smart Energy Grids, *Dagstuhl Reports*, Vol. 1, Issue 12, pp. 62–68

Editors: Stefan Katzenbeisser, Klaus Kursawe, Bart Preneel, and Ahmad-Reza Sadeghi



DAGSTUHL
REPORTS

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

In such a setting, security and privacy are vital. A security breach of a smart energy grid can have severe consequences for power availability. With respect to privacy, the information gathered by the utility reveals a wealth of information about individual customers: examples are the day rhythm (power consumption data may reveal that a customer always comes home after the bars close, and has too little time between getting up and leaving the house to have breakfast), religious patterns (a devout Muslim may turn on the light for a morning prayer, or a catholic family may always leave home during the Sunday sermon), relationship patterns (energy usage may identify the days on which a group of people stayed in a house and the time when they went to bed), and even TV schedules (by combining electricity and water consumption measurements).

While it is not clear yet to which extent this data is going to be exploited, the potential privacy implications are substantial and have already been identified (after interoperability) as the second most important issue with the smart grid by NIST.

It is thus essential to build security and privacy protection into smart energy grids right from the start. The goal of this seminar was thus to raise awareness of this critical problem that may affect every European citizen within a couple of years and 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.

Topics covered during the seminar were:

- **Communication Security.** For the smart grid to work efficiently, end-user devices will need to communicate with the utility. The main challenge is that the end devices may be extremely limited in their capacity, and that commissioning—i.e., integration of a new device into a home- or office network—has to be simple and efficient. This will require new ways of secure communication between power consuming devices and smart meters as well as new ways to set up communication networks covering extremely small devices (such as light bulbs).
- **Privacy.** The amount of data collected about individual users in a smart grid setting is unprecedented, and leads to massive concerns about user's privacy. The setting is rather unique for privacy research: the data is not gathered for the profit of some company, but for the more noble cause of global energy savings, and the nature of the system makes it hard to temporarily opt out. Flexible Privacy-Enhancing Technologies are required to balance the conflicting requirements of privacy and data usage.
- **Implementation Security.** Already now, the first attacks on implementations of smart meters have been published. With a huge number of small embedded devices suddenly getting connected, implementation security becomes critical. Unfortunately, vendors of those devices are usually not experienced in protecting against network-based attacks, and resource constraints on such devices do not allow implementation of many standard security solutions designed to protect larger computer systems. Thus, new hardware security mechanisms are required.
- **Grid Architectures.** The smart grid combines architectural requirements that are inherently contradictory. On one side, control networks for critical systems should always put safety first, i.e., rather risk a data loss than a disruption in functionality. On the other side, this particular network deals with a huge amount of privacy related and security critical data, requiring adequate protection from data theft. New architectures need to be designed to accommodate both privacy and dependability at the same time.

2 Table of Contents

Executive Summary

Klaus Kursawe, Stefan Katzenbeisser, Bart Preneel, Ahmad-Reza Sadeghi 62

Overview of Talks

Metrology for the 21st Century: Security and Privacy
George Danezis 65

Smart Meter Security: Overview of European Initiatives and Member State Activities
Michael John 65

Some protective measures for privacy in Smart Grids
Florian Kerschbaum 65

Security in a changing DSO infrastructure
Erwin Kooi 66

Overview on Smart Grid Security and Privacy
Klaus Kursawe 66

Demand response of Smart Metering
Günter Müller 66

Can Security- and Privacy-Critical Applications be Cloudified? TLOUDS says YES!
Paulo Verissimo 67


What's going on in your neighborhood: Security and privacy analysis of utility meters
Wenyuan Xu 67

Participants 68

3 Overview of Talks

3.1 Metrology for the 21st Century: Security and Privacy


George Danezis (Microsoft Research UK – Cambridge, GB)

License  Creative Commons BY-NC-ND 3.0 Unported license
© George Danezis

Metrology as a field deals with measuring quantities, and legal metrology with devices that measure quantities relating to legal contracts. Modern meters are networked digital devices that are relied upon by multiple parties for their business, as in modern smart grid proposals. We argue that such meters should provide high integrity for their readings. Furthermore, through the use of modern signature and aggregation protocols we can require meters to support privacy: any computation can be performed on the readings privately by the data subject, without revealing those readings. These meters can be deployed in a variety of ways that are in line with current practices.

3.2 Smart Meter Security: Overview of European Initiatives and Member State Activities


Michael John (Elster GmbH – Mainz, DE)

License  Creative Commons BY-NC-ND 3.0 Unported license
© Michael John

The European Commission initiated in 2009 the Task Force Smart Grids in order to facilitate the goals of the Third Energy Package. The mission of the Task Force was to advise the Commission's policy and regulation directions at EU level. This talk provided a summary of the activities of the Task Force's Expert Group on Smart Grid Security and Privacy as well as corresponding EU activities on standardization. Furthermore, an overview of the smart meter roll-outs in the different member states was given, outlining the diversity of the deployed solutions and their security levels, arguing for the need of EU-wide standards.

3.3 Some protective measures for privacy in Smart Grids


Florian Kerschbaum (TU Dresden, DE)

License  Creative Commons BY-NC-ND 3.0 Unported license
© Florian Kerschbaum

Smart Metering collects time-granular consumption profiles. These profiles can be pseudonymized and then shared. We attempt a re-identification attack. First, we detect anomalies in the data, e.g. days of low or high consumption. Then we link all profiles based on similarity. We achieve 80%-90% accuracy in linking pseudonyms on our test data. The anomaly detection proves resistant against lower granularity of the collected data.

3.4 Security in a changing DSO infrastructure


Erwin Kooi (Alliander – Duiven, NL)

License  Creative Commons BY-NC-ND 3.0 Unported license
© Erwin Kooi

The main drivers for smart grids from a DSO perspective are facilitating the energy transition and reducing time to repair of faults. The paradigm “supply follows demand” will change to “demand follows supply”, as supply of e.g. solar panels cannot be controlled. The grid will have to be able of transporting or managing the excess load or excess supply at lower levels in the grid. Having more insight in lower parts of the grid will help engineers troubleshoot faults and fault place locations. This insight will have to be done with respect for the privacy of our customers and should be done across all DSO’s.

3.5 Overview on Smart Grid Security and Privacy


Klaus Kursawe (Radboud University Nijmegen, NL)

License  Creative Commons BY-NC-ND 3.0 Unported license
© Klaus Kursawe

Due to the perceived benefits and political pressure (e.g., the 20-20-20 rules in the 3rd energy package of the European Commission), the introduction of IT into the management of the electricity grid is rapidly progressing. This overview covers the motivation for this trend, the corresponding security and privacy issues, and the activities of the major regulatory bodies. On the privacy side, a protocol is described that allows the industry to operate the grid on aggregated data only, in a way that no personal data ever needs to exist outside the smart meter in unencrypted form.

3.6 Demand response of Smart Metering


Günter Müller (Universität Freiburg, DE)

License  Creative Commons BY-NC-ND 3.0 Unported license
© Günter Müller

Smart Metering is still a technical challenge. The objective is to collect enough information to manage the supply of energy. This generates a privacy issue, since the communication from smart meter to supplier is two ways. The smart meter reports not just the demand of energy but from the pattern of energy usage behavioral patterns can be deduced. To consider the privacy question as a technical question alone is not sufficient. The main questions are: Is energy in short supply? If yes, smart metering has a key role and privacy may be of secondary nature. If there is enough energy, just the supplier has an interest to know about behavioral patterns. Like in gas stations increase gasoline cost just short of vacation periods or for the weekend, power suppliers can adjust privacy according to demand. Privacy is to be designed to keep a balance of power between supplier and customer. This is beyond access control techniques as suggested today.

3.7 Can Security- and Privacy-Critical Applications be Cloudified? T-CLOUDS says YES!

Paulo Verissimo (University of Lisboa, PT)


License  Creative Commons BY-NC-ND 3.0 Unported license
© Paulo Verissimo

Joint work of Fernando André, Alysson Bessani, Miguel Correia, Pedro Costa, Marcelo Pasin, Bruno Quaresma, Paulo Sousa, Paulo Verissimo

As data and computation are moving to the cloud, worries about failures and disclosures increase. Whilst there is still some hesitation about moving critical applications onto the cloud, like e.g., medical records, financial data or smart energy grid control, time will come. This presentation discusses an approach towards a resilient cloud-of-clouds infrastructure, T-CLOUDS. A versatile architecture is introduced as well as some related algorithms and use cases, like dependable storage preserving integrity and confidentiality, or Byzantine fault-tolerant MapReduce.

3.8 What's going on in your neighborhood: Security and privacy analysis of utility meters

Wenyuan Xu (University of South Carolina, US)

License  Creative Commons BY-NC-ND 3.0 Unported license
© Wenyuan Xu

Automatic meter reading (AMR) meters have been widely deployed in US and will be integrated into automatic meter infrastructure (AMI) in the near future. Thus, it is important to understand the security and privacy implication of the existing AMR meters. We have reverse-engineered a popular brand of AMR meters and shown that we are able to eavesdrop nearby AMR meters within 300 meters using a low noise amplifier and a 5 bBi antenna. Additionally, we can spoof AMR meters with arbitrary meter readings.

Participants

- Nikita Borisov
Univ. of Illinois – Urbana, US
- Binbin Chen
ADSC – Singapore, SG
- George Danezis
Microsoft Research UK –
Cambridge, GB
- Peter Ebinger
AGT Group (R&D) GmbH –
Darmstadt, DE
- Flavio D. Garcia
Radboud Univ. Nijmegen, NL
- Jorge Guajardo Merchan
Robert Bosch LLC –
Pittsburgh, US
- Matthias Hollick
TU Darmstadt, DE
- Bart Jacobs
Radboud Univ. Nijmegen, NL
- Michael John
Elster GmbH – Mainz, DE
- Stefan Katzenbeisser
TU Darmstadt, DE
- Florian Kerschbaum
TU Dresden, DE
- Erwin Kooi
Alliander – Duiven, NL
- Klaus Kursawe
Radboud Univ. Nijmegen, NL
- Leonardo Martucci
TU Darmstadt, DE
- Günter Müller
Universität Freiburg, DE
- Bart Preneel
K.U. Leuven, BE
- Carsten Rudolph
Fraunhofer SIT – Darmstadt, DE
- Ahmad-Reza Sadeghi
TU Darmstadt, DE
- Kazue Sako
NEC – Kawasaki, JP
- Radu Sion
Stony Brook University, US
- Christian Stübke
Sirrix AG Bochum, DE
- Gene Tsudik
Univ. of California – Irvine, US
- Ingrid Verbauwhede
K.U. Leuven, BE
- Paulo Verissimo
University of Lisboa, PT
- Khan Ferdous Wahid
Fraunhofer SIT – Darmstadt, DE
- Jos Weyers
TenneT – Arnhem, NL
- Wenyan Xu
University of South Carolina, US

