Second Smart Energy Grid Security Workshop (SEGS 2014)

Klaus Kursawe
ENCS

Klaus.Kursawe@ENCS.EU

Benessa Defend
ENCS

Benssa.Defend@ENCS.EU

ABSTRACT

In the last year, the digitalization of the power grids has been pushed further, creating an ever increasing need for security approaches in this domain. One of the most prominent and visible aspects are smart meters, which are being deployed in millions of homes with the intend to optimize billing, but also to generate data for energy saving, load balancing, and other use cases. The first session of the workshop focuses on the privacy of smart meter data, which is an important precondition for a successful and widely accepted rollout, and to make efficient use of the smart metering data. For the overall smartgrid, the workshop takes a higher level view, discussing risk analysis and overall security strategy approaches towards a secure grid. Finally, the topic addresses issues of implementations, discussing new findings on weaknesses in smart grid deployments as well as testing tools.

Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General-Security and protection (e.g., firewalls); C.3 [**Special-Purpose and Application-Based Systems**]: Real-time and embedded systems; D.4.6 [**Operating Systems**]: Security and Protection; J.7 [**Computers in Other Systems**]: Industrial Control; K.4.1 [**Computers and Society**]: Public Policy Issues; K.6.5 [**Management of Computing and Information Systems**]: Security and Protection

Keywords

Smart grid; critical infrastructure; security; data protection; privacy

1. INTRODUCTION

In the last year, the digitalization of the power grids has been pushed further, with an increasing number of countries engaging in large scale rollouts of smart grid components. While the topic of security is getting more attention, we still face insufficient understanding and communication between the electricity sector and the security community. Given the expected lifetime of the systems deployed now, and the fact that the first large scale attacks have already been seen, fostering this communication and working towards applicable solutions is more important than ever.

In spite of the growing number of events and conferences focusing on the digital grid, the gap in the security research community specially addressing smart grids is still wide, and many of the systems rolled out now have a wealth of unaddressed security issues. This workshop aims to fill that void and encourage more research into the area of smart grid security by providing a forum for security researchers to present their work. This workshop serves as an opportunity to foster collaboration between the power industry and the ACM CCS research community.

The scope of the workshop encompasses all aspects of the smart grid, including distribution, transmission, generation, metering, e-mobility, and integration of distributed energy resources. SEGS publications offer perspectives from both academia and industry, and present novel research on theoretical and practical aspects of smart grid security and privacy, including design, analysis, experimentation, and fielded systems. SEGS also aims for the integration of other communities, such as law, economics, and HCI, which present these communities' perspectives on technological issues. We hope that the workshop will provide the participants with the opportunity to share ideas and practical experience, and will result in progress towards more resilient power systems.

2. SCOPE

The SEGS Workshop covers all aspects of Smart Grid security, including but not limited to the following topics:

- Smart grid architectures and models
- Smart grid networks and communication
- Security and dependability in safety-critical, real-time systems
- Data protection and privacy
- Grid management
- Trust and assurance
- Intrusion detection and monitoring on smart grids
- Algorithms and protocols for critical infrastructures
- Risk and threat analysis
- Smartgrid standards, testing, and certification
- Testbeds and field trials
- Usability and legal issues on grid security
- Cloud computing and smart grids

CCS´14, November 3-7, 2014, Scottsdale, Arizona, USA.
Copyright 2014 ACM 987-1-4503-2957-6/14/11 $15.00.
http://dx.doi.org/10.1145/2660267.2660389

PROGRAM COMMITTEE

- Kevin Butler, University of Oregon, US
- George Danezis, University College London, UK
- Benessa Defend, ENCS, Netherlands
- Dominik Engel, Salzburg University of Applied Sciences, Austria
- Zekeriya Erkin, Delft University of Technology, Netherlands
- José M. Fernandez, Polytechnique Montréal, Canada
- Robert Griffin, RSA, Switzerland
- Maarten Hoeve, ENCS, Netherlands
- Davide Iacono, ResilTech, Italy
- David Irwin, University of Massachusetts Amherst, US
- Stefan Katzenbeisser, TU Darmstadt, Germany
- Erwin Kooi, Alliander, Netherlands
- Marina Krotofil, Hamburg University of Technology, Germany
- Jason Larsen, IOActive, US
- Eireann Leverett, IOActive, UK
- Andrés Molina-Markham, Dartmouth College, US
- Henrich Pöhls, University of Passau, Germany
- Bart Preneel, KU Leuven, Belgium
- Matthias Schunter, ICRI-SC, Germany
- Paul Smith, Austrian Institute of Technology, Austria
- Eyal Udassin, C4 Security, Israel
- Alfonso Valdes, University of Illinois Urbana-Champaign, US
- Barbara Vieira, Radboud University, Netherlands
- Rani Yesudas, Australian National University, Australia
- Kenzo Yoshimatsu, Control System Security Center, Japan