Lecture Notes in Computer Science 8448

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

More information about this series at http://www.springer.com/series/7410

Jorge Cuellar (Ed.)

Smart Grid Security

Second International Workshop,
SmartGridSec 2014
Munich, Germany, February 26, 2014
Revised Selected Papers

Springer

Editor
Jorge Cuellar
Siemens AG
Munich
Germany

ISSN 0302-9743 ISSN 1611-3349 (electronic)
ISBN 978-3-319-10328-0 ISBN 978-3-319-10329-7 (eBook)
DOI 10.1007/978-3-319-10329-7

Library of Congress Control Number: 2014946607

Springer Cham Heidelberg New York Dordrecht London

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

This volume brings together a selection of papers presented at SmartGridSec 2014 the Second Open NESSoS - EIT ICT Labs Workshop on Smart Grid Security, held at the Technical University of Munich, on February 26th, 2014. The papers were carefully peer-reviewed and the versions published here are corrected and extended for the purposes of these post-proceedings.

NESSoS – the Network of Excellence on Engineering Secure Future Internet Software Services and Systems – organized the workshop in collaboration with the action line smart energy systems of the EIT ICT Labs. NESSoS aims to establish Europe as the scientific leader in engineering secure software by addressing the current fragmentation of activities across Europe through the establishment of a joint virtual research lab on Engineering Secure Software Services, integrating the research, dissemination, and technology transfer activities of the researchers and practitioners in the area. NESSoS believes that in order to build secure systems, it is necessary to use, from the beginning, sound security engineering processes. Although the project already finished at the end of March, 2014, the community will be creating the IFIP Working Group 11.14 on Secure Engineering, where the activities will continue. The EIT ICT Labs is one of the Knowledge and Innovation Communities (KICs) set up by the European Institute of Innovation and Technology (EIT), as an initiative of the European Union. EIT ICT Labs brings together researchers and practitioners to work across the 'Knowledge Triangle' of education-research-innovation. EIT ICT Labs' partners are top ranked universities, leading research centres, and global companies in the field of ICT.

The engineering, deployment, and operation of the future Smart Grid will be an enormous project that will require the active participation of many stakeholders with different interests and views regarding the security and privacy goals, technologies, and solutions. There is an increasing need for workshops that bring together researchers from different communities, from academia and industry, to discuss open research topics in the area of future Smart Grid security.

The following set of papers illustrate the wide topic range related to the future Smart Grid:

A. Paverd, A. Martin, and I. Brown take a closer look at a particular strategy for demand response: demand bidding. Analyzing the realistic adversary models, they conclude that the current proposals cannot achieve the privacy goals that should be expected. They propose a new solution for this problem based on a trusted remote entity based on TPM technology.

D. Bytschkow, J. Quilbeuf, G. Igna, and H. Ruess propose a model-based design methodology for embedded systems, relying in particular on a separation kernel, as the one developed by MILS.

K. Beckers, M. Heisel, L. Krautsevich, F. Martinelli, and A. Yautsiukhin provide a structured method to analyze, in the context of Smart Grid, the attacker motivation as a

hierarchy of goals, and relate to specific vulnerability attack graphs. A. Armando, R. Carbone, E.G. Chekole, C. Petrazzuolo, A. Ranalli, and S. Ranise propose a framework to harmonize and enforce the requirements of different stakeholders in different domains, as they often appear in Smart Grid, based on the attribute based access control for a selective release of smart metering data in multi-domain smart grids.

J. King-Lacroix and A. Martin propose a multi-stakeholder network architecture for the smart home and, correspondingly, a set of modifications to ZigBee. The goal is to solve the trust issues between end-users and providers or operators.

Pöhls and Karwe tackle a question of resolving a conflict between privacy and integrity: Privacy can often be protected by passing data in a lower resolution, but in that case, how can end-to-end integrity be guaranteed?

K. Beckers, S. Faßbender, M. Heisel, and S. Suppan present a structured method for identifying possible security threats in the smart home scenario and analyzing their severity and relevance.

C. Rottondi, S. Fontana, and G. Verticale the interaction between Electric Vehicles (EVs) and the Smart Grid and their privacy-preserving interaction.

T. Hartmann, F. Fouquet, J. Klein, G. Nain, and Y. Le Traon suggest that unforeseen attacks and failures cannot be effectively countered proactively, but that a reactive and corrective approach based on simulation and reasoning techniques will be necessary to intelligently monitor and continuously adapt the smart grid to new conditions.

M. Karwe and J. Strüker discuss privacy energy issues and potential solutions in Demand Response systems, which are the cornerstone of the first step in a future smart grid, and how the Smart Metering Gateway concept of the German BSI can accommodate the different types of Demand Response.

F. Moyano, C. Fernández-Gago, K. Beckers, and M. Heisel claim that, complimentary to classical authentication and authorization mechanisms, the concepts of trust and reputation should play an explicit role when deciding how to interact with external agents in an open system like the Smart Grid. They propose a general framework to integrate such concepts in a Smart Grid environment.

T. Holczer, M. Félegyházi, Dl Buza, F. Juhász, and G. Miru present a proposal for honeypot systems to detect targeted attacks against industrial control systems and in particular smart energy systems.

This workshop has been partially funded by the European Commission through the FP7 project NESSoS (FP7 256890). We are also glad to acknowledge the excellent support from EasyChair both during the review process as well as for preparing the post-proceedings.

May 2014

Jorge Cuellar
Santiago Suppan

Organization

Program Committee

Alessandro Armando	Fondazione Bruno Kessler, Italy
Gabriele Costa	University of Genoa, Italy
Alberto Crespo-Garcia	Atos, France
Jorge Cuellar	Siemens AG, CT RTC ITS, Germany
Lieven Desmet	Katholieke Universiteit Leuven, Belgium
Keqin Li	SAP, France
Javier Lopez	University of Malaga, Spain
Fabio Massacci	University of Trento, Italy
Marius Minea	Universitatea Politehnica Timişoara, Romania
Martin Ochoa	Technical University of Munich, Germany
George Oikonomou	University of Bristol, UK
Santiago Suppan	University of Regensburg, Germany
Elias Tragos	Foundation for Research and Technology (FORTH), Greece
Luca Viganò	Kings College, UK

Contents