Advances in Information Security

Volume 71

Series editor
Sushil Jajodia, George Mason University, Fairfax, VA, USA

More information about this series at http://www.springer.com/series/5576

Anne V. D. M. Kayem • Stephen D. Wolthusen
Christoph Meinel
Editors

Smart Micro-Grid Systems Security and Privacy

Springer

Editors
Anne V. D. M. Kayem
Hasso-Plattner-Institute, Faculty of Digital Engineering
University of Potsdam
Potsdam, Germany

Christoph Meinel
Hasso-Plattner-Institute, Faculty of Digital Engineering
University of Potsdam
Potsdam, Germany

Stephen D. Wolthusen
Department of Mathematics and Information Security
Royal Holloway, University of London
Egham, Surrey, UK

Norwegian Information Security Laboratory
Gjovik University College,
Norwegian University of Science and Technology
Trondheim, Norway

ISSN 1568-2633
Advances in Information Security
ISBN 978-3-319-91426-8 ISBN 978-3-319-91427-5 (eBook)
https://doi.org/10.1007/978-3-319-91427-5

Library of Congress Control Number: 2018950667

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

. . . To Scientists in the field of Cyber-Physical Systems. . .

Preface

People who work in the field of energy management have the pleasure of working on a topic whose results are visualisable and beneficial to society. There is also the payoff of knowing that economic growth, and perhaps even life as we know it, would be impossible without power or energy. Energy grid models play a crucial role in idealisations of real-world economies.

Until recently, however, energy grid management systems have largely remained the preserve of electrical engineers and researchers. Its concepts are not really esoteric or difficult, but they are relatively new to the computer science community, so it has taken a while to sort out the best ways of designing energy grids that can be controlled using a cyber system.

Now after more than 30 years of development, smart grids and micro-grid technologies have matured to the point where they are ready to take their place in discussions on computing that are centred on matters of security and privacy. This book is intended to provide an overview of some of the primary techniques that can be used to model adversarial scenarios in both smart grids and micro-grids. In designing energy systems to operate as a combination of a cyber (algorithms and software systems to control energy generation hardware) and physical system (energy generation components and grid), we now find ourselves having to handle aspects such as data manipulations to enable energy theft, masking adversarial behaviours as faulty behaviour, price signal manipulation, and inference of private user behaviours, to name but a few potential security and privacy vulnerabilities. The material covered, in terms of adversarial scenarios, draws from classical attacks centred on energy theft, misattribution, and grid destabilisation. The focus is on how these attacks, masked as system failures or component malfunctions, can be used to cause the breakdown of energy grids without drawing attention to the adversary.

We assume that the reader has some familiarity with basic concepts in computer science, security and privacy, and smart grid technologies. In a nutshell, the reader should be able to write programs and have some understanding of energy flow control manipulation. Otherwise, the book is intended to be self-contained.

This book is meant to be used as a reference manual for researchers and students, in need of concrete examples on how to model malicious scenarios in smart girds and micro-grids. The book can also be used to introduce graduate students to the field of security and privacy in smart grids and micro-grids. Supplemented by papers from the literature, the book can also serve as the basis for an introductory graduate course on cyber-physical systems, or as the basis for self-study by researchers in the fields of cyber-physical systems, resource constrained computing, and smart grids/micro-grids, who want access to the literature in this field.

Related Books Related texts include *Smart Grid Infrastructure and Networking by Iniewski; Distributed Algorithms by Lynch; Introduction to Algorithms by Cormen, Leiserson, Rivest, and Stein; and Fault Tolerance in Distributed Systems by Jalote.* This book could be considered as supplementary to each of these in studying smart grids/micro-grids particularly ones in which management is distributed.

How to Use This Book Since readers of this book are likely to come from different backgrounds, being aware of the implicit structure of this book might be helpful. With this in mind, Chap. 1 puts the material of the book into perspective and will help readers understand the basic objectives of the book as well as the role of the remaining chapters in meeting those objectives. Chapters 2 and 3 are focused on presenting attacks and countermeasures on state estimation, as well as an example of an authentication protocol in smart grids. Chapter 4 presents a survey of potential vulnerabilities in authentication protocols for smart grids highlighting the similarities with standard authentication systems. Chapters 5–7 discuss micro-grid architectures, focusing on the special case of resource constrained smart micro-grids. Resource constrained smart micro-grids are a special case of micro-grids designed to operate autonomously in rural/remote environments where connectivity to standard smart micro-grids is logistically or economically infeasible. Since such micro-grids are typically supported by a lossy communications network, adversarial scenarios must be modelled to account for unreliability, and special properties of flow control identified in order to differentiate benign faulty behaviours from malicious attempts at subversion.

We hope that you will find this book rewarding in many ways, and that it will serve as a basis for even more exciting discoveries on this topic.

Potsdam, Germany — Anne V. D. M. Kayem
Potsdam, Germany — Christoph Meinel
London, UK — Stephen D. Wolthusen
March 2018

Acknowledgements

We begin by expressing our heartfelt gratitude to the Norwegian Research Council, South African National Research Foundation, and the Hasso-Plattner-Institute for the funding and infrastructural support provided to facilitate this work. This book would not have been possible without your support!

In addition, we would like to thank all the reviewers, for taking the trouble to painstakingly provide feedback to the authors both on the chapter proposals and the full chapter submissions. In particular, special thanks to Andrew Adamatzky (University of West England, UK), Chris Mitchell (Royal Holloway, University of London, UK), Cristina Alcaraz (University of Malaga, Spain), Dieter Hutter (University of Bremen, and DFKI, Germany), Ingo Stengel (University of Applied Sciences, Karlsruhe, Germany), Martin Strohmeier (University of Oxford, UK), Stephen Marsh (University of Ontario Institute of Technology, Canada), Sule Yildirim-Yayilgan (Norwegian University of Science and Technology, Norway), Sylvia Osborn (University of Western Ontario, Canada), Trupil Limbasiya (Birla Institute of Technology & Science (BITS), India), and Zeyar Aung (Masdar Institute, Khalifa University of Science and Technology, UAE).

Compiling a contributed volume requires not only content from the authors but also a commitment to deliver high-quality material in a timely manner. We would like to take this opportunity to express our heartfelt gratitude to all the authors for making this a pain-free process. Special thanks to Ammara Gul (Royal Holloway, University of London, UK); Anesu Marufu and Pacome Ambassa (University of Cape Town, South Africa); Stephen Wolthusen (Royal Holloway, University of London, UK, & Norwegian University of Science and Technology, Norway); Trupil Limbasiya, Aakriti Arya, and Pragya Verma (NIIT University, India); and Hikaru Kishimoto (Osaka University, Japan), Naoto Yanai (Osaka University, Japan), and Shingo Okamura (National Institute of Technology, Nara College, Japan). Thank you for your patience and contributions.

While we were compiling this book, we received informal feedback from several colleagues. In particular, we would like to thank Leonard Barolli, Sylvia Osborn, Dieter Hutter, and Tei-Wei Kuo for their constructive feedback and suggestions.

Finally, we would also like to thank our editorial managers Susan Lagerstrom-Fife, Jennifer Malat, and Caroline Flanagan for providing the editorial support needed to compile this book. You seemed to know exactly when to keep quiet to let us get on with our work, and when to push for deliverables!

Contents

Contributors

Pacome L. Ambassa Department of Computer Science, University of Cape Town, Rondebosch, Cape Town, South Africa

Aakriti Arya NIIT University, Neemrana, Rajasthan, India

Ammara Gul Department of Mathematics and Information Security, Royal Holloway University of London, Egham, Surrey, UK

Anne V. D. M. Kayem Hasso-Plattner-Institute, Faculty of Digital Engineering, University of Potsdam, Potsdam, Germany

Hikaru Kishimoto Osaka University, Suita, Osaka, Japan

Trupil Limbasiya Birla Institute of Technology & Science (BITS), Pilani, Goa, India

Anesu M. C. Marufu Department of Computer Science, University of Cape Town, Cape Town, South Africa

Christoph Meinel Hasso-Plattner-Institute, Faculty of Digital Engineering, University of Potsdam, Potsdam, Germany

Shingo Okamura National Institute of Technology, Nara College, Yamatokoriyama, Nara, Japan

Stephen D. Wolthusen Department of Mathematics and Information Security, Royal Holloway, University of London, Egham, Surrey, UK

Norwegian Information Security Laboratory, Gjovik University College, Norwegian University of Science and Technology, Trondheim, Norway

Naoto Yanai Osaka University, Suita, Osaka, Japan

List of Reviewers

Andrew Adamatzky University of West England, UK

Anne V. D. M. Kayem Hasso-Plattner-Institute, Germany

Chris Mitchell Royal Holloway, University of London, UK

Cristina Alcaraz University of Malaga, Spain

Dieter Hutter University of Bremen, and DFKI, Germany

Ingo Stengel University of Applied Sciences, Karlsruhe, Germany

Martin Strohmeier University of Oxford, UK

Stephen Marsh University of Ontario Institute of Technology, Canada

Sule Yildirim-Yayilgan Norwegian University of Science and Technology, Norway

Sylvia Osborn University of Western Ontario, Canada

Trupil Limbasiya Birla Institute of Technology & Science (BITS), India

Zeyar Aung Masdar Institute, Khalifa University of Science and Technology, UAE