

Bruce McMillin · Thomas Roth
Elisa Bertino · Ravi Sandhu *Editors*

Cyber-Physical Security and Privacy in the Electric Smart Grid

Cyber-Physical Security and Privacy in the Electric Smart Grid

Synthesis Lectures on Information Security, Privacy & Trust

Editors

Elisa Bertino, *Purdue University*

Ravi Sandhu, *University of Texas, San Antonio*

The Synthesis Lectures Series on Information Security, Privacy, and Trust publishes 50- to 100-page publications on topics pertaining to all aspects of the theory and practice of Information Security, Privacy, and Trust. The scope largely follows the purview of premier computer security research journals such as ACM Transactions on Information and System Security, IEEE Transactions on Dependable and Secure Computing and Journal of Cryptology, and premier research conferences, such as ACM CCS, ACM SACMAT, ACM AsiaCCS, ACM CODASPY, IEEE Security and Privacy, IEEE Computer Security Foundations, ACSAC, ESORICS, Crypto, EuroCrypt and AsiaCrypt. In addition to the research topics typically covered in such journals and conferences, the series also solicits lectures on legal, policy, social, business, and economic issues addressed to a technical audience of scientists and engineers. Lectures on significant industry developments by leading practitioners are also solicited.

Cyber-Physical Security and Privacy in the Electric Smart Grid

Bruce McMillin and Thomas Roth

2017

Blocks and Chains: Introduction to Bitcoin, Cryptocurrencies, and Their Consensus Mechanisms

Aljosha Judmayer, Nicholas Stifter, Katharina Krombholz, and Edgar Weippl

2017

Digital Forensic Science: Issues, Methods, and Challenges

Vassil Roussev

2016

Differential Privacy: From Theory to Practice

Ninghui Li, Min Lyu, Dong Su, and Weining Yang

2016

Privacy Risk Analysis

Sourya Joyee De and Daniel Le Métayer
2016

Introduction to Secure Outsourcing Computation

Xiaofeng Chen
2016

Database Anonymization: Privacy Models, Data Utility, and Microaggregation-based Inter-model Connections

Josep Domingo-Ferrer, David Sánchez, and Jordi Soria-Comas
2016

Automated Software Diversity

Per Larsen, Stefan Brunthaler, Lucas Davi, Ahmad-Reza Sadeghi, and Michael Franz
2015

Trust in Social Media

Jiliang Tang and Huan Liu
2015

Physically Unclonable Functions (PUFs): Applications, Models, and Future Directions

Christian Wachsmann and Ahmad-Reza Sadeghi
2014

Usable Security: History, Themes, and Challenges

Simson Garfinkel and Heather Richter Lipford
2014

Reversible Digital Watermarking: Theory and Practices

Ruchira Naskar and Rajat Subhra Chakraborty
2014

Mobile Platform Security

N. Asokan, Lucas Davi, Alexandra Dmitrienko, Stephan Heuser, Kari Kostiaainen, Elena Reshetova, and Ahmad-Reza Sadeghi
2013

Security and Trust in Online Social Networks

Barbara Carminati, Elena Ferrari, and Marco Viviani
2013

RFID Security and Privacy

Yingjiu Li, Robert H. Deng, and Elisa Bertino
2013

Hardware Malware

Christian Krieg, Adrian Dabrowski, Heidelinde Hobel, Katharina Krombholz, and Edgar Weippl
2013

Private Information Retrieval

Xun Yi, Russell Paulet, and Elisa Bertino
2013

Privacy for Location-based Services

Gabriel Ghinita
2013

Enhancing Information Security and Privacy by Combining Biometrics with Cryptography

Sanjay G. Kanade, Dijana Petrovska-Delacrétaz, and Bernadette Dorizzi
2012

Analysis Techniques for Information Security

Anupam Datta, Somesh Jha, Ninghui Li, David Melski, and Thomas Reps
2010

Operating System Security

Trent Jaeger
2008

© Springer Nature Switzerland AG 2022
Reprint of original edition © Morgan & Claypool 2017

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means—electronic, mechanical, photocopy, recording, or any other except for brief quotations in printed reviews, without the prior permission of the publisher.

Cyber-Physical Security and Privacy in the Electric Smart Grid

Bruce McMillin and Thomas Roth

ISBN: 978-3-031-01225-9 paperback

ISBN: 978-3-031-02353-8 ebook

DOI 10.1007/978-3-031-02353-8

A Publication in the Morgan & Claypool Publishers series

SYNTHESIS LECTURES ON INFORMATION SECURITY, PRIVACY & TRUST

Lecture #21

Series Editors: Elisa Bertino, *Purdue University*

Ravi Sandhu, *University of Texas, San Antonio*

Series ISSN

Print 1945-9742 Electronic 1945-9750

Cyber-Physical Security and Privacy in the Electric Smart Grid

Bruce McMillin

Missouri University of Science and Technology

Thomas Roth

National Institute of Standards and Technology

*SYNTHESIS LECTURES ON INFORMATION SECURITY,
PRIVACY & TRUST #21*

ABSTRACT

This book focuses on the combined cyber and physical security issues in advanced electric smart grids. Existing standards are compared with classical results and the security and privacy principles of current practice are illustrated. The book paints a way for future development of advanced smart grids that operated in a peer-to-peer fashion, thus requiring a different security model. Future defenses are proposed that include information flow analysis and attestation systems that rely on fundamental physical properties of the smart grid system.

KEYWORDS

smart grid, security, privacy, cyber-physical, standards

Contents

	Preface	xi
1	The Smart Grid as a Cyber-Physical System	1
1.1	Smart Grid Architectures	1
1.1.1	Advanced Metering Infrastructure	1
1.1.2	Microgrid Architecture	2
1.1.3	Fully Distributed Smart Grid	3
1.1.4	Transmission Grid	4
2	The Basics of Cyber-Physical Security	7
2.1	A Look at the History of SCADA Systems and Security	8
2.1.1	Classic Models of Security: BLP and Biba	10
2.2	Security Partitions in the Smart Grid	12
2.3	Vulnerability Assessments of Power Systems	18
2.3.1	Information Flow Disruption	20
3	Defenses	21
3.1	Attestation through Physical Properties	21
3.2	Attestation through Reputation	23
3.3	Statistical Control Approaches	23
4	Attack Motivation	25
5	Privacy	27
5.1	NILM	27
5.2	Quantifying the Human Element	29
6	Standards	31
6.1	NERC	31
6.1.1	NERC CIP	31

6.2	SGIP and NIST	32
6.2.1	NISTiR 7628	32
6.2.2	NIST 800-030	35
6.2.3	openFMB	37
6.2.4	Mandate M/441, CG-SM, and SGAM	37
7	Summary	39
	References	41
	Authors' Biographies	51

Preface

A few years ago, the first author was in a research meeting with power engineers looking at building a complex power system testbed for studying dynamics. What about “security?” and the knowing response around the room was “of course it’s secure, at long it’s not overstressed.” Funny response. After some more discussion, it became apparent power system security is a different concept than cyber security, the former being a measure of the system’s operation [20]¹ (what a computer scientist might refer to as safe and live). “No, what if somebody reads the voltage and power settings?” “Who cares,” was the response. And so, with this thought in mind, we begin this book.

The work described herein represents a view developed over the last 17 years of working in what is now known as the “smart grid,” both for transmission (high voltage over long distances between electric substations) and distribution (lesser voltage with delivery to customers from a substation). The national laboratories that work in the Department of Energy’s mission, national and international standards bodies, experimentation in the research lab for both transmission and distribution have all helped to begin to frame the cyber aspects of electric power security. The cyber aspects become more intertwined with the electric power system, so much so that cyber-physical security seems an appropriate moniker. As this book will uncover, cyber processing and communications system can both help and hinder the resiliency of a power system. The power system still retains some inherent resiliency and its state of operation can provide assistance in its protection from attack.

Bruce McMillin and Thomas Roth
July 2017

¹“Power system security is the ability to maintain the flow of electricity from the generators to the customers, especially under disturbed conditions.”