Synthesis Lectures on
Information Security, Privacy, and Trust

SYNTHESIS
COLLECTION OF TECHNOLOGY

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

Cyber-Physical Security and Privacy in the Electric Smart Grid

Springer

Cyber-Physical Security and Privacy in the Electric Smart Grid

Synthesis Lectures on Information Security, Privacy & Trust

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.

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 Kostiainen, 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

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

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."