Advances in Information Security

Volume 67

Series editor

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

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

Ehab Al-Shaer • Mohammad Ashiqur Rahman

Security and Resiliency Analytics for Smart Grids

Static and Dynamic Approaches

Springer

Ehab Al-Shaer
Department of Software and Information Systems
University of North Carolina, Charlotte
Charlotte, NC, USA

Mohammad Ashiqur Rahman
Department of Computer Science
Tennessee Tech University
Cookeville, TN, USA

ISSN 1568-2633
Advances in Information Security
ISBN 978-3-319-32870-6 ISBN 978-3-319-32871-3 (eBook)
DOI 10.1007/978-3-319-32871-3

Library of Congress Control Number: 2016938524

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG Switzerland

The whole of science is nothing more than a refinement of everyday thinking.

— Albert Einstein

Preface

Driven by the rapid advancement of technology and the growing need of business requirements, cyber communications are embedded in many physical systems. The integration of cyber and physical capabilities leads to the creation of many applications with enormous societal impact and economic benefit. The emerging systems that connect the cyber-world of computing and communications with the physical world are cyber-physical systems (CPS). Operations are monitored, analyzed, and controlled in CPS using cyber systems that interconnect physical components. Many CPS are defined as critical infrastructures due to their national importance. According to the U.S. Department of Homeland Security, "Critical infrastructures are the assets, systems, or networks, whose incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety". Any damage or unavailability of such a critical infrastructure often has a massive and broader impact.

This book targets a state-of-the-art important concern of protecting critical infrastructures like smart grids. The work presents various static and dynamic security analysis techniques that can automatically verify smart grid security and resiliency and provably identify potential attacks in a proactive manner. These techniques serve three major security and resiliency analysis objectives. The first objective is to formally verify the compliance of smart grid configurations with the security and resiliency guidelines. More specifically, a formal framework is presented that verifies the compliance of the advanced metering infrastructure and supervisory control and data acquisition system with the security and resiliency requirements, and generates remediation plans for potential security violations. The second objective is the formal verification of the security and resiliency of smart grid control systems. In this respect, a formal model is presented that analyzes attack evasions on state estimation, a core control module of the supervisory control system in smart grids. The model identifies attack vectors that can compromise state estimation. This part also includes risk mitigation techniques that formally synthesize proactive security plans that make such attacks infeasible. The last effort discusses the dynamic security analysis for smart grid. It is shown that AMI behavior can be modeled using event logs collected at smart collectors, which in turn can be

verified using the specification invariants generated from the configurations of the AMI devices.

Although the focus of this book is the smart grid security and resiliency, the presented formal analytics are generic enough to be extended for other cyber-physical systems, especially which are involved with industrial control systems (ICS). Therefore, industry professionals and academic researchers will find this book as an exceptional resource to learn theoretical and practical aspects of applying formal methods for the protection of critical infrastructures.

Unlike the existing books on the smart grid security that mostly discuss various security issues and corresponding challenges, this book offers unique solutions addressing these challenges. The book covers novel techniques which can automatically, provably, and efficiently analyze the security and resiliency of the smart grids. The distinct features included in this book are formal modeling of smart grid configurations, proactive and noninvasive verification of smart grid security and resiliency properties, identification of potential threats, and corresponding mitigations. This book includes various illustrative case studies and extensive evaluation results demonstrating the efficacy of the formal techniques. We expect this book will maximize reader insights into theoretical and practical aspects of applying formal methods for the protection of critical infrastructures.

Charlotte, NC, USA — Ehab Al-Shaer
Cookeville, TN, USA — Mohammad Ashiqur Rahman
February 2016

Acknowledgements

Special thanks to Dr. Rajesh Kavasseri (North Dakota State University, USA), Dr. Rakesh Bobba (Oregon State University, USA), Dr. Padmalochan Bera (IIT Bhubaneswar, India), and Muhammad Qasim Ali (Goldman Sachs, USA) for their precious inputs to this text.

We also want to thank Susan Lagerstrom-Fife, Editor, Computer Science, Springer, USA for her support and advice on this book. We would also like to thank Jennifer Malat, Assistant Editor, Computer science, Springer, USA for her efforts.

Contents

Acronyms

A list of selected acronyms that are often used in this book:

AGC	Automatic Generation Control
AMI	Advanced Metering Infrastructure
AMR	Automatic Meter Reading
CPS	Cyber-Physical System
CTL	Computation Tree Logic
DC	Direct Current
DDoS	Distributed Denial of Service
D-FACTS	Distributed Flexible AC Transmission System
DTMC	Discrete-Time Markov Chain
EMS	Energy Management System
FERC	Federal Energy Regulatory Commission
GPS	Global Positioning System
HAN	Home Area Network
HMI	Human Machine Interface
ICS	Industrial Control System
IDS	Intrusion Detection System
IED	Intelligent Electronic Device
IPSec	Internet Protocol Security
LMC	Labeled Markov Chain
LTL	Linear Temporal Logic
MDP	Markov Decision Process
MTD	Moving Target Defense
MTU	Master Terminal Unit
NAN	Neighborhood Area Network
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NMS	Network Management System
OPF	Optimal Power Flow
PDC	Phasor Data Concentrator

PLC	Programmable Logic Controller
PMU	Phasor Measurement Unit
ROC	Receiver Operating Characteristics
RTU	Remote Terminal Unit
SAT	Boolean Satisfiability Problem
SCADA	Supervisory Control and Data Acquisition
SMT	Satisfiability Modulo Theories
TPM	Trusted Platform Module
UFDI	Undetected False Data Injection
WAN	Wide Area Network