Contents

Contributing Authors ix

Preface xix

PART I THEMES AND ISSUES

1
On the Security Implications of Disruptive Technologies 3
Neil Robinson and Lorenzo Valeri

2
Cyber Security: Are Economic Incentives Adequate? 15
Scott Dynes, Eric Goetz and Michael Freeman

3
Government Intervention in Information Infrastructure Protection 29
Dan Assaf

PART II INFRASTRUCTURE SECURITY

4
Security of Information Flow in the Electric Power Grid 43
Han Tang and Bruce McMillin

5
Securing Positive Train Control Systems 57
Mark Hartong, Rajni Goel and Duminda Wijesekera

6
Lessons Learned from the Maroochy Water Breach 73
Jill Slay and Michael Miller

7
Reducing Risk in Oil and Gas Production Operations 83
Stig Johnsen, Rune Ask and Randi Roisli

PART III CONTROL SYSTEMS SECURITY

8
Securing Current and Future Process Control Systems 99
Robert Cunningham, Steven Cheung, Martin Fong, Ulf Lindqvist, David Nicol, Ronald Pawlowski, Eric Robinson, William Sanders, Sankalp Singh, Alfonso Valdes, Bradley Woodworth and Michael Zhivich

9
Security Strategies for SCADA Networks 117
Rodrigo Chandia, Jesus Gonzalez, Tim Kilpatrick, Mauricio Papa and Sujeet Shenoi

10
Security Enhancements for Distributed Control Systems 133
Jeffrey Hieb, James Graham and Sandip Patel

11
Security Challenges of Reconfigurable Devices in the Power Grid 147
Suvda Myagmar, Roy Campbell and Marianne Winslett

12
Intrusion Detection and Event Monitoring in SCADA Networks 161
Paul Oman and Matthew Phillips

13
Passive Scanning in Modbus Networks 175
Jesus Gonzalez and Mauricio Papa

14
Formal Modeling and Analysis of the Modbus Protocol 189
Bruno Dutertre

15
Security Analysis of Multilayer SCADA Protocols 205
Janica Edmonds, Mauricio Papa and Sujeet Shenoi

16
Remote Forensic Analysis of Process Control Systems 223
Regis Friend Cassidy, Adrian Chavez, Jason Trent and Jorge Urrea

17
Creating a European SCADA Security Testbed 237
Henrik Christiansson and Eric Luiijf

PART IV NETWORK INFRASTRUCTURE SECURITY

18
Protecting Internet Services from Low-Rate DoS Attacks 251
Yajuan Tang, Xiapu Luo and Rocky Chang

19
Detecting Wormhole Attacks in Wireless Sensor Networks 267
Yurong Xu, Guanling Chen, James Ford and Fillia Makedon

20
Detecting Non-Discoverable Bluetooth Devices 281
Daniel Cross, Justin Hoeckle, Michael Lavine, Jason Rubin and Kevin Snow

PART V INFRASTRUCTURE INTERDEPENDENCIES

21
Risk Analysis in Interdependent Infrastructures 297
Yacov Haimes, Joost Santos, Kenneth Crowther, Matthew Henry, Chenyang Lian and Zhenyu Yan

22
Analysis of Interdependencies Between Italy's Economic Sectors 311
Roberto Setola

23
The ISE Metamodel for Critical Infrastructures 323
Felix Flentge and Uwe Beyer

24
Multigraph Dependency Models for Heterogeneous Infrastructures 337
Nils Svendsen and Stephen Wolthusen

25
Visualizing Cascading Failures in Critical Cyber Infrastructures 351
Jason Kopylec, Anita D'Amico and John Goodall

PART VI RISK ASSESSMENT

26
A Service-Oriented Approach for Assessing Infrastructure Security 367
Marcelo Masera and Igor Nai Fovino

27
Analysis of Electrical Power and Oil and Gas Pipeline Failures 381
Jeffrey Simonoff, Carlos Restrepo, Rae Zimmerman and Zvia Naphtali