SYNGRESS

Industrial Network Security

Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems

Second Edition

Eric D. Knapp
Joel Thomas Langill

Industrial Network Security

Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems

Second Edition

Industrial Network Security

Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems

Second Edition

Eric D. Knapp
Joel Thomas Langill

Technical Editor
Raj Samani

ELSEVIER

AMSTERDAM • BOSTON • HEIDELBERG • LONDON
NEW YORK • OXFORD • PARIS • SAN DIEGO
SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO

Syngress is an Imprint of Elsevier

SYNGRESS.

Acquiring Editor: Chris Katsaropoulos
Editorial Project Manager: Benjamin Rearick
Project Manager: Surya Narayanan Jayachandran
Cover Designer: Maria Ines Cruz

Syngress is an imprint of Elsevier
225 Wyman Street, Waltham, MA 02451, USA

Notices
Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods, professional practices, or medical treatment may become necessary. Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information, methods, compounds, or experiments described herein. In using such information or methods they should be mindful of their own safety and the safety of others, including parties for whom they have a professional responsibility. To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions, or ideas contained in the material herein.

Library of Congress Cataloging-in-Publication Data
Application Submitted

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

ISBN: 978-0-12-420114-9

For information on all Syngress publications visit our website at www.syngress.com.

Contents

About the Authors xv
Preface xvii
Acknowledgments xix

CHAPTER 1 Introduction 1
Book Overview and Key Learning Points 1
Book Audience 2
Diagrams and Figures 2
The Smart Grid 3
How This Book is Organized 3
Chapter 2: About Industrial Networks 3
Chapter 3: Industrial Cyber Security, History, and Trends 4
Chapter 4: Introduction to ICS and Operations 4
Chapter 5: ICS Network Design and Architecture 4
Chapter 6: Industrial Network Protocols 4
Chapter 7: Hacking Industrial Systems 5
Chapter 8: Risk and Vulnerability Assessments 5
Chapter 9: Establishing Zones and Conduits 5
Chapter 10: Implementing Security and Access Controls 5
Chapter 11: Exception, Anomaly, and Threat Detection 5
Chapter 12: Security Monitoring of Industrial Control Systems 6
Chapter 13: Standards and Regulations 6
Changes Made to the Second Edition 6
Conclusion 7

CHAPTER 2 About Industrial Networks 9
The Use of Terminology Within This Book 9
Attacks, Breaches, and Incidents: Malware, Exploits, and APTs 11
Assets, Critical Assets, Cyber Assets, and Critical Cyber Assets 11
Security Controls and Security Countermeasures 12
Firewalls and Intrusion Prevention Systems 12
Industrial Control System 13
DCS or SCADA? 15
Industrial Networks 15

Industrial Protocols 15
Networks, Routable Networks, and Nonroutable Networks 18
Enterprise or Business Networks 20
Zones and Enclaves 22
Network Perimeters or "Electronic Security Perimeters" 24
Critical Infrastructure 26
Common Industrial Security Recommendations 29
Identification of Critical Systems 29
Network Segmentation/Isolation of Systems 31
Defense in Depth 33
Access Control 34
Advanced Industrial Security Recommendations 35
Security Monitoring 36
Policy Whitelisting 36
Application Whitelisting 36
Common Misperceptions About Industrial Network Security 37
Assumptions Made in This Book 38
Summary 39
Endnotes 39

CHAPTER 3 Industrial Cyber Security History and Trends 41
Importance of Securing Industrial Networks 41
The Evolution of the Cyber Threat 44
APTs and Weaponized Malware 47
Still to Come 50
Defending Against Modern Cyber Threats 51
Insider Threats 52
Hacktivism, Cyber Crime, Cyber Terrorism, and Cyber War 53
Summary 55
Endnotes 55

CHAPTER 4 Introduction to Industrial Control Systems and Operations 59
System Assets 59
Programmable Logic Controller 59
Remote Terminal Unit 63
Intelligent Electronic Device 64
Human–Machine Interface 64

Supervisory Workstations 67
Data Historian 67
Business Information Consoles and Dashboards 68
Other Assets 69
System Operations 70
Control Loops 70
Control Processes 72
Feedback Loops 73
Production Information Management 73
Business Information Management 74
Process Management 76
Safety Instrumented Systems 78
The Smart Grid 80
Network Architectures 82
Summary 82
Endnotes 83

CHAPTER 5 Industrial Network Design and Architecture 85
Introduction to Industrial Networking 87
Common Topologies 92
Network Segmentation 96
Higher Layer Segmentation 99
Physical vs. Logical Segmentation 104
Network Services 106
Wireless Networks 107
Remote Access 108
Performance Considerations 111
Latency and Jitter 111
Bandwidth and Throughput 112
Type of Service, Class of Service, and Quality of Service 112
Network Hops 113
Network Security Controls 113
Safety Instrumented Systems 114
Special Considerations 115
Wide Area Connectivity 115
Smart Grid Network Considerations 116
Advanced Metering Infrastructure 118
Summary 119
Endnotes 119

CHAPTER 6 Industrial Network Protocols 121
Overview of Industrial Network Protocols 121
Fieldbus Protocols 123
Modicon Communication Bus 123
Distributed Network Protocol 130
Process Fieldbus 139
Industrial Ethernet Protocols 141
Ethernet Industrial Protocol 142
PROFINET 146
EtherCAT 147
Ethernet POWERLINK 148
SERCOS III 149
Backend Protocols 150
Open Process Communications 150
Inter-Control Center Communications Protocol 157
Advanced Metering Infrastructure and the Smart Grid 162
Security Concerns 164
Security Recommendations 164
Industrial Protocol Simulators 164
Modbus 165
DNP3 / IEC 60870-5 165
OPC 165
ICCP / IEC 60870-6 (TASE.2) 165
Physical Hardware 166
Summary 166
Endnotes 166

CHAPTER 7 Hacking Industrial Control Systems 171
Motives and Consequences 171
Consequences of a Successful Cyber Incident 171
Cyber Security and Safety 172
Common Industrial Targets 174
Common Attack Methods 186
Man-in-the-Middle Attacks 186
Denial-of-Service Attacks 187
Replay Attacks 188
Compromising the Human–Machine Interface 189
Compromising the Engineering Workstation 189
Blended Attacks 190

Examples of Weaponized Industrial Cyber Threats 190
Stuxnet 191
Shamoon/DistTrack 195
Flame/Flamer/Skywiper 195
Attack Trends 196
Evolving Vulnerabilities: The Adobe Exploits 197
Industrial Application Layer Attacks 198
Antisocial Networks: A New Playground for Malware 200
Dealing with an Infection 203
Summary 205
Endnotes 206

CHAPTER 8 Risk and Vulnerability Assessments 209
Cyber Security and Risk Management 210
Why Risk Management is the Foundation of Cyber Security 210
What is Risk? 211
Standards and Best Practices for Risk Management 213
Methodologies for Assessing Risk Within Industrial Control Systems 216
Security Tests 216
Establishing a Testing and Assessment Methodology 219
System Characterization 223
Data Collection 227
Scanning of Industrial Networks 228
Threat Identification 241
Threat Actors/Sources 241
Threat Vectors 243
Threat Events 243
Identification of Threats During Security Assessments 244
Vulnerability Identification 246
Vulnerability Scanning 248
Configuration Auditing 250
Vulnerability Prioritization 251
Risk Classification and Ranking 253
Consequences and Impact 253
How to Estimate Consequences and Likelihood 254
Risk Ranking 256
Risk Reduction and Mitigation 257
Summary 258
Endnotes 259

CHAPTER 9 Establishing Zones and Conduits 261
Security Zones and Conduits Explained 263
Identifying and Classifying Security Zones and Conduits 264
Recommended Security Zone Separation 265
Network Connectivity 266
Control Loops 267
Supervisory Controls 268
Plant Level Control Processes 268
Control Data Storage 270
Trading Communications 271
Remote Access 272
Users and Roles 272
Protocols 274
Criticality 275
Establishing Security Zones and Conduits 277
Summary 279
Endnotes 280

CHAPTER 10 Implementing Security and Access Controls 283
Network Segmentation 287
Zones and Security Policy Development 288
Using Zones within Security Device Configurations 288
Implementing Network Security Controls 290
Selecting Network Security Devices 290
Implementing Network Security Devices 293
Implementing Host Security and Access Controls 309
Selecting Host Cyber Security Systems 311
External Controls 316
Patch Management 316
How Much Security is Enough? 320
Summary 321
Endnotes 321

CHAPTER 11 Exception, Anomaly, and Threat Detection 323
Exception Reporting 324
Behavioral Anomaly Detection 326
Measuring Baselines 327
Anomaly Detection 330
Behavioral Whitelisting 333
User Whitelists 334

Asset Whitelists 335
Application Behavior Whitelists 337
Threat Detection 340
Event Correlation 341
Correlating Between IT and OT Systems 347
Summary 349
Endnotes 349

CHAPTER 12 Security Monitoring of Industrial Control Systems 351
Determining what to Monitor 352
Security Events 353
Assets 356
Configurations 358
Applications 360
Networks 361
User Identities and Authentication 362
Additional Context 365
Behavior 365
Successfully Monitoring Security Zones 367
Log Collection 368
Direct Monitoring 368
Inferred Monitoring 369
Information Collection and Management Tools 372
Monitoring Across Secure Boundaries 376
Information Management 376
Queries 377
Reports 379
Alerts 381
Incident Investigation and Response 381
Log Storage and Retention 382
Nonrepudiation 382
Data Retention/Storage 382
Data Availability 384
Summary 385
Endnotes 385

CHAPTER 13 Standards and Regulations 387
Common Standards and Regulations 388
NERC CIP 389
CFATS 389

ISO/IEC 27002 390
NRC Regulation 5.71 390
NIST SP 800-82 392
ISA/IEC-62443 392
ISA 62443 Group 1: "General" 392
ISA 62443 Group 2: "Policies and Procedures" 393
ISA 62443 Group 3: "System" 393
ISA 62443 Group 4: "Component" 394
Mapping Industrial Network Security to Compliance 395
Industry Best Practices for Conducting ICS Assessments 395
Department of Homeland Security (USA) / Centre for Protection of National Infrastructure (UK) 396
National Security Agency (USA) 397
American Petroleum Institute (USA) / National Petrochemical and Refiners Association (USA) 397
Institute for Security and Open Methodologies (Spain) 398
Common Criteria and FIPS Standards 398
Common Criteria 398
FIPS 140-2 400
Summary 400
Endnotes 406

Appendix A Protocol Resources 409
Modbus Organization 409
DNP3 Users Group 409
OPC Foundation 410
Common Industrial Protocol (CIP) / Open Device Vendor Association (ODVA) 410
PROFIBUS & PROFINET International (PI) 410

Appendix B Standards Organizations 411
North American Reliability Corporation (NERC) 411
The United States Nuclear Regulatory Commission (NRC) 411
NRC Title 10 CFR 73.54 412
NRC RG 5.71 412
United States Department of Homeland Security 412
Chemical Facilities Anti-Terrorism Standard (CFATS) 412
CFATS Risk-Based Performance Standards (RBPS) 412
International Society of Automation (ISA) 413
International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) 413

Appendix C NIST Security Guidelines **415**
National Institute of Standards and Technology,
Special Publications 800 Series 415

Glossary **417**
Endnotes 424

Index **425**

INDUSTRIAL N

Securing Critical Infrastructur and Other Industrial Control S

SYNGRESS

How to understand and address the unique security concerns that face the world's most important networks

As the sophistication of cyber-attacks increases, understanding how to defend critical infrastructure systems—electric utilities, water, oil, natural gas, transportation, and other vital systems—becomes more important, and increasingly mandated. ***Industrial Network Security, Second Edition*** arms you with the knowledge you need to understand the vulnerabilities of these supervisory and distributed control systems, and to learn how to protect them.

The book examines the unique protocols and applications that are the foundation of industrial control systems, and provides clear guidelines for their protection. This how-to guide gives you thorough understanding of the unique challenges facing critical infrastructures, new guidelines and security measures for critical infrastructure protection, knowledge of new and evolving security tools, and pointers on industrial protocols and security implementation.

- Expanded coverage of industrial networks and protocols
- Industrial cyber security history and trends, with real-world examples of threats and countermeasures
- Updated network diagrams and expanded network architecture guidelines
- Comprehensive coverage of risk management tools and methodologies for industrial control system assessments
- Updated coverage on understanding, designing and deploying industrial security zones and conduits
- Insight into strategies for improving situational awareness within industrial networks

Eric D. Knapp is a recognized expert in industrial control systems cyber security, and the co-author of *Applied Cyber Security and the Smart Grid.*

Joel Langill founded the popular ICS security website SCADAhacker.com and serves on the Board of Advisors for Scada Fence Ltd. and the ISA99 committee.

Eric D. Knapp
Joel Langill

Raj Samani, Technical Editor

ISBN 978-0-12-420114-9
9 780124 201149

store.elsevier.com/Syngress