SYNGRESS

Foreword by Dr. Anton A. Chuvakin

Industrial Network Security

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

Eric D. Knapp

Industrial Network Security

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

Eric Knapp

Technical Editor
James Broad

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: Angelina Ward
Development Editor: Matt Cater
Project Manager: Jessica Vaughan
Designer: Joanne Blank

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 or professional practices may become necessary. Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information or methods 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
Knapp, Eric.
Industrial network security : securing critical infrastructure networks for Smart Grid, SCADA, and other industrial control systems / Eric Knapp.
p. cm.
Summary: "This book attempts to define an approach to industrial network security that considers the unique network, protocol and application characteristics of an industrial control system, while also taking into consideration a variety of common compliance controls"–Provided by publisher.
Includes bibliographical references.
ISBN 978-1-59749-645-2 (pbk.)
1. Process control–Security measures. 2. Computer security. I. Title.
TS156.8.K58 2011
670.42'7–dc23
2011018442

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

ISBN: 978-1-59749-645-2

Printed in the United States of America

11 12 13 14 15 10 9 8 7 6 5 4 3 2 1

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

Industrial Network Security

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

About the Author

Eric D. Knapp is the Director of Critical Infrastructure Markets for NitroSecurity, where he leads the identification, evaluation, and implementation of new security technologies specific to the protection of critical infrastructure, Supervisory Control And Data Acquisition (SCADA), and industrial control networks.

Eric has 20 years of experience in Information Technology, specializing in industrial automation technologies, infrastructure security, and applied Ethernet protocols as well as the design and implementation of Intrusion Prevention Systems and Security Information and Event Management systems in both enterprise and industrial networks. In addition to his work in information security, Eric is an award-winning author. He studied English and Writing at the University of New Hampshire and the University of London and holds a degree in communications.

About the Technical Editor

James Broad (CISSP, C|EH, C)PTS, Security+, MBA) is the President and owner of Cyber-Recon, LLC, where he and his team of consultants specialize in Information Security, Information Assurance, and Certification and Accreditation and offer other security consultancy services to corporate and government clients.

As a security professional with over 20 years of real-world IT experience, James is an expert in many areas of IT security, specializing in security engineering, penetration testing, and vulnerability analysis and research. He has provided security services in the Nation's most critical sectors including defense, law enforcement, intelligence, finance, and healthcare.

James has a Master's of Business Administration degree with specialization in Information Technology (MBA/IT) from the Ken Blanchard College of Business, Bachelor's degrees in Computer Programming and Security Management from Southwestern University and is currently a Doctoral Learner pursuing a PhD in Information Security from Capella University. He is a member of ISSA and (ISC)$^{2®}$. James currently resides in Stafford, Virginia with his family: Deanne, Micheal, and Temara.

Foreword

One of the most mysterious areas of information security is industrial system security. No other area of information security contains that many myths, mistakes, misconceptions and outright lies. Information available online, while voluminous, will only lead information security professionals and industrial systems professionals to more confusion and more misconceptions—which may result in not only costly, but also life-threatening, mistakes.

What raises the mystery even higher is that the stakes in the area of industrial security are extremely high. While the loss of trade secret information may kill a business, the loss of electricity generating capability may kill not just one person, but potentially thousands.

And finally the mystery is solved—with this well-researched book on industrial system network security.

The book had a few parts of particular interest to me. I liked that the book covers the "myth of an air gap"—now in the age of wireless, the air gap is not what it used to be and should not be assumed to be "the absolute security." I also liked that safety versus security is covered: industrial engineers might know more about the former while my InfoSec colleagues know more about the latter. Today's interconnected industrial systems absolutely need both! Finally, I also liked the book's focus on risk and impact, and not simply on following the regulatory minimum.

Both information security and industrial engineers, which are currently two distinctly different tribes, would benefit from this book. And, hopefully *Industrial Network Security* will bring the much needed union of both tribes, thus helping us build a more secure business and industrial system.

—Dr. Anton A. Chuvakin
Security Warrior Consulting

Contents

CHAPTER

Introduction

1

INFORMATION IN THIS CHAPTER:

- Book Overview and Key Learning Points
- Book Audience
- Diagrams and Figures
- The Smart Grid
- How This Book Is Organized

BOOK OVERVIEW AND KEY LEARNING POINTS

This book attempts to define an approach to industrial network security that considers the unique network, protocol, and application characteristics of an **industrial control system**, while also taking into consideration a variety of common compliance controls.

Although many of the techniques described herein—and much of the general guidance provided by regulatory standards organizations—are built upon common enterprise security methods and reference readily available information security tools, there is little information available about how to implement these methods. This book attempts to rectify this by providing deployment and configuration guidance where possible, and by identifying why security controls should be implemented, where they should implemented, how they should be implemented, and how they should be used.

BOOK AUDIENCE

To adequately discuss industrial network security, the basics of two very different systems need to be understood: the Ethernet and Transmission Control Protocol/Internet Protocol (TCP/IP) networking communications used ubiquitously in the enterprise, and the **SCADA** and field bus protocols used to manage and/or operate industrial automated systems.

As a result, this book possesses a bifurcated audience. For the plant operator with an advanced electrical engineering degree and a decade of logic programming for Modbus controllers, the basics of industrial network protocols in Chapter 4 have been presented within the context of security in an attempt to not only provide value to such a reader, but also to get that reader thinking about the subtle implications of cyber security. For the information security analyst with a Certified Information Systems Security Professional (CISSP) certification, basic information security practices have been provided within the new context of an industrial control system.

There is an interesting dichotomy between the two that provides a further challenge. Enterprise security typically strives to secure the users and **hosts** on a network while at the same time enables the broad range of open communication services required within modern business. Industrial control systems, on the other hand, strive for the efficiency and reliability of a single, often fine-tuned system. Only by giving the necessary consideration to both sides can the true objective be achieved: a secure industrial network that supports reliable operation while also providing business value to the larger enterprise.

To further complicate matters, there is a third audience: the compliance officer who is mandated with meeting certain regulatory standards in order to survive an audit with minimal penalties and/or fines. Compliance continues to drive information security budgets, and therefore the broader scope of industrial networks must also be narrowed on occasion to the energy industries, where (at least in the United States) electrical energy, nuclear energy, oil, and gas are tightly regulated. Compliance controls are discussed in this book solely within the context of implementing cyber security controls. The recommendations given are intended to improve security and should not be interpreted as advice concerning successful compliance management.

DIAGRAMS AND FIGURES

The network diagrams used throughout this book have been intentionally simplified and have been designed to be as generic as possible while adequately representing industrial networks across a very wide range of industrial systems. As a result, the diagrams will undoubtedly differ from real industrial network designs and may exclude details specific to one particular industry while including details that are specific to another. However, they will provide a high-level understanding of the specific industrial network security controls being discussed.

THE SMART GRID

Although the smart grid is of major concern and interest, for the most part it is treated as any other industrial network within this book, with specific considerations being made only when necessary (such as when considering available **attack vectors**). As a result, there are many security considerations specific to the smart grid that are unfortunately not included. This is partly to maintain focus on the more ubiquitous

ICS and SCADA security requirement, partly due to the relative immaturity of smart grid security and partly due to the specialized and complex nature of these systems. Although this means that specific measures for securing synchrophasers, meters, etc. are not provided, the guidance and overall approach to security that is provided herein is certainly applicable to smart grid networks. For more in-depth reading on smart grid network security, consider *Securing the Smart Grid: Next Generation Power Grid Security* by Tony Flick and Justin Morehouse (ISBN: 978-1-59749-570-7, Syngress).

HOW THIS BOOK IS ORGANIZED

This book is divided into a total of eleven chapters, followed by three appendices guiding the reader where to find additional information and resources about industrial protocols, standards and regulations, and relevant **NIST** security guidelines. An extensive glossary is also provided to accommodate the wealth of both information security and industrial networking terms and acronyms used throughout the book.

The chapters begin with an introduction to industrial networking, and what a cyber attack against an industrial control systems might represent in terms of potential risks and consequences, followed by details of how industrial networks can be assessed, secured, and monitored in order to obtain the strongest possible security, and conclude with a detailed discussion of various compliance controls, and how those specific controls map back to network security practices.

It is not necessary to read this book cover to cover, in order. The book is intended to offer insight and recommendations that relate to both specific security goals as well as the cyclical nature of the security process. That is, if faced with performing a **vulnerability assessment** on an industrial control network, begin with Chapter 6; every effort has been made to refer the reader to other relevant chapters where additional knowledge may be necessary.

Chapter 2: About Industrial Networks

In this chapter, there is a brief introduction to industrial networks as they relate to "**critical infrastructure**," those infrastructures upon which our society, industry, and way of life depend. The dependencies of critical infrastructures upon industrial control systems lead naturally to a discussion of the many standards, regulations, guidance documents, and policies that have been implemented globally to protect these systems. In addition, the chapter introduces the reader to the most basic premises of industrial security.

Of particular note, Chapter 2 also discusses the use of terminology within the book as it relates to the many applications of industrial networks (again, there is also an extensive Glossary included to cover the abundance of new acronyms and terms used in industrial control networks).