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
- Changes Made to the Second Addition

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** (**ICS**), while also taking into consideration a variety of common compliance controls. For the purposes of this book, a common definition of ICS will be used in lieu of the more specific **Supervisory Control and Data Acquisition** (**SCADA**) or **Distributed Control System** (**DCS**) terms. Note that these and many other specialized terms are used extensively throughout the book. While we have made an effort to define them all, an extensive glossary has also been included to provide a quick reference if needed. If a term is included in the glossary, it will be printed in bold type the first time that it is used.

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, references and readily available information security tools, there is little information available about how these apply to an industrial network. 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 be 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 Internet Protocol (IP) networking communications used ubiquitously in the enterprise, and the control and fieldbus protocols used to manage and/or operate automation systems.

As a result, this book possesses a bifurcated audience. For the plant operator with an advanced engineering degree and decades of programming experience for process 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 ICS.

There is an interesting dichotomy between the two that provides a further challenge. Enterprise security typically strives to protect digital information by securing the users and **hosts** on a network, while at the same time enabling 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, while always addressing the safety of the personnel, plant, and environment in which they operate. Only by giving the necessary consideration to both sides can the true objective be achieved—a secure industrial network architecture that supports safe and reliable operation while also providing business value to the larger enterprise. This latter concept is referred to as "operational integrity."

To further complicate matters, there is a third audience—the compliance officer who is mandated with meeting either certain regulatory standards or internal policies and procedures 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, and chemical 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 ICS architectures and their industrial networks across a very wide range of systems and suppliers. As a result, the diagrams will undoubtedly differ from real ICS designs and may exclude details specific to one particular industry while

including details that are specific to another. Their purpose is to 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 security requirements; 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, and so on, 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 *Applied Cyber Security and the Smart Grid* by Eric D. Knapp and Raj Samani (ISBN: 978-1-59749-998-9, Syngress).

HOW THIS BOOK IS ORGANIZED

This book is divided into a total of 13 chapters, followed by three appendices guiding the reader where to find additional information and resources about industrial protocols, standards and regulations, and relevant security guidelines and best practices (such as **NIST**, **ChemITC**, and **ISA**).

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 **security assessment** on an industrial network, begin with Chapter 8; 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 primer of industrial control systems, industrial networks, **critical infrastructure**, common cyber security guidelines, and other terminology specific to the lexicon of industrial cyber security. The goal of this chapter is to

provide a baseline of information from which topics can be explored in more detail in the following chapters (there is also an extensive Glossary included to cover the abundance of new acronyms and terms used in industrial control networks). Chapter 2 also covers some of the basic misperceptions about industrial cyber security, in an attempt to rectify any misunderstandings prior to the more detailed discussions that will follow.

CHAPTER 3: INDUSTRIAL CYBER SECURITY, HISTORY, AND TRENDS

Chapter 3 is a primer for industrial cyber security. It introduces industrial network cyber security in terms of its history and evolution, by examining the interrelations between "general" networking, industrial networking, and potentially critical infrastructures. Chapter 3 covers the importance of securing industrial networks, discusses the impact of a successful industrial attack, and provides examples of real historical incidents—including a discussion of the **Advanced Persistent Threat** and the implications of cyber war.

CHAPTER 4: INTRODUCTION TO ICS AND OPERATIONS

It is impossible to understand how to adequately secure an industrial control environment without first understanding the fundamentals of ICSs and operations. These systems use specialized devices, applications, and protocols because they perform functions that are different than enterprise networks, with different requirements, operational priorities, and security considerations. Chapter 4 discusses control system **assets**, operations, protocol basics, how control processes are managed, and common systems and applications with special emphasis on smart grid operations.

CHAPTER 5: ICS NETWORK DESIGN AND ARCHITECTURE

Industrial networks are built from a combination of Ethernet and IP networks (to interconnect general computing systems and servers) and at least one real-time network or fieldbus (to connect devices and process systems). These networks are typically nested deep within the enterprise architecture, offering some implied layers of protection against external threats. In recent years, the deployment of remote access and wireless networks within industrial systems have offered new entry points into these internal networks. Chapter 5 provides an overview of some of the more common industrial network designs and architectures, the potential risk they present, and some of the methods that can be used to select appropriate technologies and strengthen these critical industrial systems.

CHAPTER 6: INDUSTRIAL NETWORK PROTOCOLS

This chapter focuses on industrial network protocols, including **Modbus**, **DNP3**, **OPC**, **ICCP**, **CIP**, **Foundation Fieldbus HSE**, **Wireless HART**, **Profinet and Profibus**, and others. This chapter will also introduce vendor-proprietary industrial protocols, and the implications they have in securing industrial networks. The basics

of protocol operation, frame format, and security considerations are provided for each, with security recommendations being made where applicable. Where properly disclosed vulnerabilities or exploits are available, examples are provided to illustrate the importance of securing industrial communications.

CHAPTER 7: HACKING INDUSTRIAL SYSTEMS

Understanding effective cyber security requires a basic understanding of the threats that exist. Chapter 7 provides a high-level overview of common attack methodologies, and how industrial networks present a unique **attack surface** with common attack vectors to many critical areas.

CHAPTER 8: RISK AND VULNERABILITY ASSESSMENTS

Industrial control systems are often more susceptible to a cyber-attack, yet they are also more difficult to patch due to the extreme uptime and reliability requirements of operational systems. Chapter 8 focuses on risk and vulnerability assessment strategies that specifically address the unique challenges of assessing risk in industrial networks, in order to better understand—and therefore reduce—the vulnerabilities and threats facing these real-time systems.

CHAPTER 9: ESTABLISHING ZONES AND CONDUITS

A strong cyber security strategy requires the isolation of devices into securable groups. Chapter 9 looks at how to separate functional groups and where functional boundaries should be implemented, using the Zone and Conduit model originated by the Purdue Research Foundation in 1989 and later adapted by ISA 99 (now known as ISA/**IEC** 62443).

CHAPTER 10: IMPLEMENTING SECURITY AND ACCESS CONTROLS

Once the industrial architecture has been appropriately divided into defined zones and the associated communication conduits between these zones, it is necessary to deploy appropriate security controls to enforce network security. Chapter 10 discusses the vital activity of network segmentation and how network- and host-based security controls are implemented.

CHAPTER 11: EXCEPTION, ANOMALY, AND THREAT DETECTION

Awareness is the prerequisite of action, according to the common definition of **situational awareness**. Awareness in turn requires an ability to monitor for and detect threats. In this chapter, several contributing factors to obtaining situational awareness are discussed, including how to use anomaly detection, exception reporting, and information correlation for the purposes of threat detection and risk management.

CHAPTER 12: SECURITY MONITORING OF INDUSTRIAL CONTROL SYSTEMS

Completing the cycle of situational awareness requires further understanding and analysis of the threat indicators that you have learned how to detect in Chapter 11. Chapter 12 discusses how obtaining and analyzing broader sets of information can help you better understand what is happening, and make better decisions. This includes recommendations of what to monitor, why, and how. Information management strategies—including **log** and **event** collection, direct monitoring, and correlation using **security information and event management** (**SIEM**)—are discussed, including guidance on data collection, retention, and management.

CHAPTER 13: STANDARDS AND REGULATIONS

There are many regulatory compliance standards applicable to industrial network security, and most consist of a wide range of procedural controls that are not easily resolved using information technology. On top of this, there is an emergence of a large number of industrial standards that attempt to tailor many of the general-purpose IT standards to the uniqueness of ICS architectures. There are common cyber security controls (with often subtle but important variations), however, which reinforce the recommendations put forth in this book. Chapter 13 attempts to map those cyber security–related controls from some common standards—including **NERC CIP**, **CFATS**, NIST 800-53, **ISO/**IEC 27002:2005, ISA 62443, **NRC** RG 5.71, and NIST 800-82—to the security recommendations made within this book, making it easier for security analysts to understand the motivations of compliance officers, while compliance officers are able to see the security concerns behind individual controls.

CHANGES MADE TO THE SECOND EDITION

For readers of the Industrial Network Security, Securing Critical Infrastructure Networks for Smart grid, SCADA and Other Industrial Control Systems, First Edition, you will find new and updated content throughout the book. However, the largest changes that have been made include the following:

- Revised diagrams, designed to provide a more accurate representation of industrial systems so that the lessons within the book can be more easily applied in real life.
- Better organization of topics, including major revisions to introductory chapters that are intended to provide a more effective introduction of topics.
- The separation of "hacking methodologies" and "risk and vulnerability assessment" into two chapters, expanding each to provide significantly more detail to each very important subject.
- The inclusion of wireless networking technologies and how they are applied to industrial networks, including important differences between general-purpose IT and specific ICS technology requirements.

- Much greater depth on the subjects of industrial firewall implementation and industrial protocol filtering—important technologies that were in their infancy during the first edition but are now commercially available.
- The inclusion of real-life vulnerabilities, exploits, and defensive techniques throughout the book to provide a more realistic context around each topic, while also proving the reality of the threat against critical infrastructure.

CONCLUSION

Writing the first edition of this book was an education, an experience, and a challenge. In the months of research and writing, several historic moments occurred concerning ICS security, including the first ICS-targeted cyber weapon—Stuxnet. At the time, Stuxnet was the most sophisticated cyber-attack to date. Since then, its complexity and sophistication have been surpassed more than once, and the frequency of new threats continues to rise. There is a growing number of attacks, more relevant cyber security research (from both **blackhats** and **whitehats**), and new evidence of Advanced Persistent Threats, cyber espionage, nation-based cyber privacy concerns, and other socio-political concerns on what seems like a daily basis. It is for this reason that Eric D. Knapp (the original author) joined forces with Joel Langill, aka "SCADAhacker," for the second edition.

Hopefully, this book will be both informative and enjoyable, and it will facilitate the increasingly urgent need to strengthen the security of our industrial networks and automation systems. Even though the attacks themselves will continue to evolve, the methods provided herein should help to prepare against the inevitable advancement of industrial network threat.

A Note from Author Eric D. Knapp. Those readers who are familiar with my works will know that I have an ongoing agreement with Raj Samani, the technical editor of this book—if either of us mention a certain well-known cyber-attack by name we must donate $5 as a penance. While this is a rule that I try to live by, this book predates that agreement and it did not seem fair or appropriate to remove all mention of that incident. So, the pages herein are exempt. In fact, the incident-that-shall-not-be-named is mentioned twice in this chapter alone; sadly, no one will be getting $10.