Securing SCADA Systems

Ronald L. Krutz

WILEY
Wiley Publishing, Inc.

Securing SCADA Systems

Securing SCADA Systems

Ronald L. Krutz

WILEY
Wiley Publishing, Inc.

Securing SCADA Systems

Published by
Wiley Publishing, Inc.
10475 Crosspoint Boulevard
Indianapolis, IN 46256
www.wiley.com

Published simultaneously in Canada

ISBN-13: 978-0-7645-9787-9
ISBN-10: 0-7645-9787-6

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

1MA/RQ/RR/QV/IN

Library of Congress Cataloging-in-Publication Data

Krutz, Ronald L., 1938–
Securing SCADA systems / Ronald L. Krutz.
p. cm.
Includes bibliographical references and index.
ISBN-13: 978-0-7645-9787-9 (cloth : alk. paper)
ISBN-10: 0-7645-9787-6 (cloth : alk. paper)
1. Process control. 2. Data protection. 3. Computer security. I. Title.
TS156.8.K78 2005
670.42'7558—dc22
2005026371

To Emma Antoinette:

The latest Lady Love in my life—a precious beauty—
and only 18 months old.

Love
Grandpapa

About the Author

Ronald L. Krutz, Ph.D., P.E., CISSP, ISSEP, is a senior information security researcher for Lockheed Martin Information Technology. In this capacity, he works with a team responsible for advancing the state of the art in information systems security. He has more than 40 years of experience in distributed computing systems, computer architectures, real-time systems, information assurance methodologies, and information security training.

He has been an information security consultant at REALTECH Systems Corporation and BAE Systems, an associate director of the Carnegie Mellon Research Institute (CMRI), and a professor in the Carnegie Mellon University Department of Electrical and Computer Engineering. Dr. Krutz founded the CMRI Cybersecurity Center and was founder and director of the CMRI Computer, Automation, and Robotics Group. He is also a distinguished special lecturer in the Center for Forensic Computer Investigation at the University of New Haven, a part-time instructor in the University of Pittsburgh Department of Electrical and Computer Engineering, and a registered professional engineer.

Dr. Krutz is the author of seven best-selling publications in the area of information systems security, and is a consulting editor for John Wiley & Sons for its information security book series. He holds B.S., M.S., and Ph.D. degrees in electrical and computer engineering.

Credits

Executive Editor
Carol Long

Development Editor
Tom Dinse

Production Editor
Kathryn Duggan

Copy Editor
Maarten Reilingh

Editorial Manager
Mary Beth Wakefield

Production Manager
Tim Tate

Vice President and Executive Group Publisher
Richard Swadley

Vice President and Executive Publisher
Joseph B. Wikert

Project Coordinator
Ryan Steffen

Graphics and Production Specialists
Karl Brandt
Carrie A. Foster
Stephanie D. Jumper
Barbara Moore

Quality Control Technicians
Jessica Kramer
Robert Springer

Proofreading and Indexing
TECHBOOKS Production Services

Contents

Acknowledgments

Special thanks to my wife, Hilda, for her encouragement and support during yet another book project.

I also want to thank Carol A. Long, executive acquisitions editor, Networking and Security, Wiley Technology Publishing, for her support and advice on this text and Tom Dinse, development editor, Wiley Publishing, for his excellent editing efforts.

Special Acknowledgment

I want to express my appreciation to Dr. Eric Cole, chief scientist at Lockheed Martin Information Technologies, for his input to this text as a subject matter expert.

Dr. Cole is a renowned thought leader with over 15 years of experience in the network-security consulting market space, with clients including leading international banks, Fortune 500 companies, and the CIA. Eric is a member of the HoneyNet project and the CVE editorial board, and is a recognized author of several books, including *Hackers Beware* and *Hiding in Plain Sight.*

Introduction

Computer-based supervisory control and data acquisition (SCADA) systems have evolved over the past 40 years, from standalone, compartmentalized operations into networked architectures that communicate across large distances. In addition, their implementations have migrated from custom hardware and software to standard hardware and software platforms. These changes have led to reduced development, operational, and maintenance costs as well as providing executive management with real-time information that can be used to support planning, supervision, and decision making. These benefits, however, come with a cost. The once semi-isolated industrial control systems using proprietary hardware and software are now vulnerable to intrusions through external networks, including the Internet, as well as from internal personnel. These attacks take advantage of vulnerabilities in standard platforms, such as Windows, and PCs that have been adopted for use in SCADA systems.

This situation might be considered a natural progression of moderate concern—as in many other areas using digital systems—if it were not for the fact that these SCADA systems are controlling a large percentage of the United States' and the world's critical infrastructures, such as nuclear power plants, electricity generating plants, pipelines, refineries, and chemical plants. In addition, they are directly and indirectly involved in providing services to seaports, transportation systems, pipelines, manufacturing plants, and many other critical enterprises.

A large body of information-system security knowledge has accumulated concerning the protection of various types of computer systems and networks. The fundamental principles inherent in this knowledge provide a solid foundation for application to SCADA systems. However, some of the characteristics, performance requirements, and protocols of SCADA system components require adapting information-system security methods in industrial settings.

In order to present a complete view of SCADA system security concepts and their important role in the nation's critical infrastructure, this text begins by defining SCADA system components and functions, and providing illustrations of general SCADA systems architectures. With this background, specific SCADA implementations in a variety of critical applications are presented along with a determination of security concerns and potential harmful outcomes of attacks on these operations.

The text follows these illustrations with a detailed look at the evolution of SCADA protocols and an overview of the popular protocols in use today. Then the security issues and vulnerabilities associated with these protocols are examined.

With the criticality of SCADA system security established, the chapters that follow explore SCADA system vulnerabilities, risk issues, attacks, and attack routes, and they provide detailed guidance on countermeasures and other mechanisms that can be applied to effectively secure SCADA systems. In addition, related information, security standards, and reference documents are discussed. These publications provide extremely useful information for securing SCADA systems from cyberattacks.

The book concludes with an examination of the economics of implementing SCADA system security, organizational culture issues, perceptions (and misperceptions) of SCADA vulnerability, and current state of SCADA system security. This last topic is addressed in detail by examining SCADA security issues in the oil and gas industry, rail systems, and seaports. Finally, current advanced development programs, additional countermeasures, and legislation targeted to increase the effectiveness of SCADA security in the present and future are described.

CHAPTER

1

What Is a SCADA System?

Supervisory control and data acquisition (SCADA) systems are vital components of most nations' critical infrastructures. They control pipelines, water and transportation systems, utilities, refineries, chemical plants, and a wide variety of manufacturing operations.

SCADA provides management with real-time data on production operations, implements more efficient control paradigms, improves plant and personnel safety, and reduces costs of operation. These benefits are made possible by the use of standard hardware and software in SCADA systems combined with improved communication protocols and increased connectivity to outside networks, including the Internet. However, these benefits are acquired at the price of increased vulnerability to attacks or erroneous actions from a variety of external and internal sources.

This chapter explores the evolution of SCADA systems, their characteristics, functions, typical applications, and general security issues.

History of Critical Infrastructure Directives

In 1996, Presidential Executive Order 13010 established the President's Commission on Critical Infrastructure Protection (PCCIP) to explore means to address the vulnerabilities in the U.S. critical infrastructure. Internet-based attacks and physical attacks were two of the major concerns that were to be considered by the committee. As a result of the committee's efforts, the FBI National Infrastructure Protection Center (NIPC) and the Critical Infrastructure Assurance Office (CIAO) were established in May 1998 by Presidential Decision Directive 63 (PDD 63). The main function of the NIPC was to conduct investigations relating to attacks against the critical infrastructure and issue associated warnings, when appropriate. The CIAO was designated as the main entity for managing the U.S. critical infrastructure protection (CIP) efforts, including coordinating the efforts of the different commercial and industrial entities affected.

As a consequence of the CIAO activities, the Communications and Information Sector Working Group (CISWG) was established with the mission to "promote information sharing and coordinated action to mitigate CIP risk and vulnerabilities in all levels of the Information and Communications (I&C) Sector." In addition, companies in eight critical industry sectors established a related entity, the Partnership for Critical Infrastructure Security (PCIS). The PCIS was formed to mitigate the vulnerabilities caused by the interdependence of many commercial and industrial organizations.

In response to the September 11, 2001 attacks, the president, on October 8, 2001, established the President's Critical Infrastructure Board (PCIB), the Office of Homeland Security, and the Homeland Security Council with Executive Order 13228. Also in October 2001, the USA Patriot Act was passed to provide U.S. government law enforcement agencies with increased authority to perform searches, monitor Internet communications, and conduct investigations.

On the economic front, in February 2003, President George W. Bush appointed the 30-member National Infrastructure Advisory Council (NIAC) from the private sector, state and local governments, and academia. NIAC's charter is to advise the president on information system security issues related to the various U.S. business sectors. Around the same time, President Bush issued Executive Order 1327, which discontinued the PCIB. This action was necessary because the functions of the PCIB were assumed by the Department of Homeland Security.

President Bush, in December 2003, announced Homeland Security Presidential Directives HSPD-7 and HSPD-8. HSPD-7 is a modification of PDD 63 that delineates the national policy and responsibilities of the executive departments,