

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

Copyright © 2006 by Wiley Publishing, Inc., Indianapolis, Indiana

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

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600. Requests to the Publisher for permission should be addressed to the Legal Department, Wiley Publishing, Inc., 10475 Crosspoint Blvd., Indianapolis, IN 46256, (317) 572-3447, fax (317) 572-4355, or online at <http://www.wiley.com/go/permissions>.

Limit of Liability/Disclaimer of Warranty: The publisher and the author make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation warranties of fitness for a particular purpose. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If professional assistance is required, the services of a competent professional person should be sought. Neither the publisher nor the author shall be liable for damages arising herefrom. The fact that an organization or Website is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or Website may provide or recommendations it may make. Further, readers should be aware that Internet Websites listed in this work may have changed or disappeared between when this work was written and when it is read.

For general information on our other products and services or to obtain technical support, please contact our Customer Care Department within the U.S. at (800) 762-2974, outside the U.S. at (317) 572-3993 or fax (317) 572-4002.

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

Trademarks: Wiley, the Wiley logo, and related trade dress are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates, in the United States and other countries, and may not be used without written permission. All other trademarks are the property of their respective owners. Wiley Publishing, Inc., is not associated with any product or vendor mentioned in this book.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

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.



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

About the Author	vii
Acknowledgments	xvii
Introduction	xix
Chapter 1 What Is a SCADA System?	1
History of Critical Infrastructure Directives	1
SCADA System Evolution, Definitions, and Basic Architecture	3
SCADA Evolution	5
SCADA Definition	6
SCADA System Architecture	7
SCADA Applications	10
SCADA System Security Issues Overview	16
SCADA and IT Convergence	16
Conventional IT Security and Relevant SCADA Issues	17
Redundancy as a Component of SCADA Security	20
SCADA System Desirable Properties	20
Summary	22
Chapter 2 SCADA Systems in the Critical Infrastructure	23
Employment of SCADA Systems	23
Petroleum Refining	23
The Basic Refining Process	24
Possible Attack Consequences	26
Nuclear Power Generation	26
The Boiling Water Reactor	27
The Pressurized Water Reactor	28
Possible Attack Consequences	29

	Conventional Electric Power Generation	30
	Petroleum Wellhead Pump Control	32
	Water Purification System	34
	Crane Control	36
	SCADA in the Corporation	37
	Chemical Plant	38
	Benzene Production	38
	Embedded Systems	40
	Why We Should Worry about These Operations	40
	Summary	41
Chapter 3	The Evolution of SCADA Protocols	43
	Evolution of SCADA Protocols	43
	Background Technologies of the SCADA Protocols	44
	Overview of the OSI Model	44
	Overview of the TCP/IP Model	48
	SCADA Protocols	50
	The MODBUS Model	50
	The DNP3 Protocol	52
	UCA 2.0 and IEC61850 Standards	53
	Controller Area Network	54
	Control and Information Protocol	55
	DeviceNet	56
	ControlNet	57
	EtherNet/IP	57
	FFB	59
	Profibus	61
	The Security Implications of the SCADA Protocols	63
	Firewalls	63
	Packet-Filtering Firewalls	63
	Stateful Inspection Firewalls	65
	Proxy Firewalls	65
	Demilitarized Zone	65
	Single Firewall DMZ	66
	Dual Firewall DMZ	66
	General Firewall Rules for Different Services	66
	Virtual Private Networks	69
	Summary	71
Chapter 4	SCADA Vulnerabilities and Attacks	73
	The Myth of SCADA Invulnerability	73
	SCADA Risk Components	76
	Managing Risk	78
	Risk Management Components	79
	Assessing the Risk	79
	Mitigating the Risk	80

SCADA Threats and Attack Routes	81
Threats	81
SCADA Attack Routes	82
Typical Attacker Privilege Goals	83
SCADA Honeynet Project	85
Honeypots	85
Honeynet Project	86
SCADA Honeynet	86
Summary	87
Chapter 5 SCADA Security Methods and Techniques	89
SCADA Security Mechanisms	89
Improving Cybersecurity of SCADA Networks	90
Implementing Security Improvements	96
SCADA Intrusion Detection Systems	97
Types of Intrusion Detection Systems	98
Network-Based and Host-Based IDS	98
Signature-Based and Anomaly-Based IDS	99
Active-Response IDS	99
Passive-Response IDS	100
Processing of IDS Data	100
Vulnerability Scanning and Analysis	100
SCADA Audit Logs	102
Security Awareness	106
Summary	108
Chapter 6 SCADA Security Standards and Reference Documents	109
ISO/IEC 17799:2005 and BS 7799-2:2002	110
ISO/IEC 1779:2005	111
BS 7799-2:2002	112
ISA-TR99.00.01-2004, <i>Security Technologies for Manufacturing and Control Systems</i>	113
ISA-TR99.00.02-2004, <i>Integrating Electronic Security into the Manufacturing and Control Systems Environment</i>	114
GAO-04-140T, <i>Critical Infrastructure Protection, Challenges in Securing Control Systems</i>	115
NIST, <i>System Protection Profile for Industrial Control Systems (SPP ICS)</i>	117
Federal Information Processing Standards Publication (FIPS Pub) 199, <i>Standards for Security Categorization of Federal Information and Information Systems</i> , February 2004	117
Additional Useful NIST Special Publications	119
NIST Special Publication 800-37, <i>Guide for the Security Certification and Accreditation of Federal Information Systems</i>	119

	NIST Special Publication 800-53, <i>Recommended Security Controls for Federal Information Systems</i>	120
	NIST Special Publication 800-53A, <i>Guide for Assessing the Security Controls in Federal Information Systems</i>	121
	Summary	122
Chapter 7	SCADA Security Management Implementation Issues and Guidelines	123
	Management Impressions of SCADA Security	123
	SCADA Culture	124
	Unique Characteristics and Requirements of SCADA Systems	125
	Limitations of Current Technologies	126
	Guidance for Management in SCADA Security Investment	127
	Information-System Security Engineering	127
	Discover Information Protection Needs	128
	Define System Security Requirements	128
	Design System Security Architecture	128
	Develop Detailed Security Design	129
	Implement System Security	129
	Common Criteria Protection Profiles	130
	Defense-in-Depth	130
	People	131
	Technology	131
	Operations	132
	Defense-in-Depth Strategy	132
	The NIST SP 800-14, <i>Generally Accepted Principles and Practices for Securing Information Technology Systems</i>	134
	NIST Special Publication 800-26, <i>Security Self-Assessment Guide for Information Technology Systems</i>	136
	Summary	137
Chapter 8	Where We Stand Today	139
	The Status Today	139
	Human Issues	140
	Weakness of Standard Security Approaches	142
	The Oil and Gas Industry	142
	API Standard 1164	143
	AGA Report Number 12	144
	Interdependencies	144
	Rail System Security	145
	Port Security	146
	Legislation	148
	Threats to Seaports	148
	Countermeasures	149
	Conventional Countermeasures	149
	Advanced Countermeasures	150
	Security Controls That Can Be Put in Place Now	151
	Summary	152

Appendix A Acronyms and Abbreviations	153
Appendix B System Protection Profile – Industrial Control Systems	157
Appendix C Bibliography	195
Index	201



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.

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,