A PRACTICAL GUIDE TO

Security Engineering and Information Assurance

OTHER AUERBACH PUBLICATIONS

ABCs of IP Addressing
Gilbert Held
ISBN: 0-8493-1144-6

Application Servers for E-Business
Lisa M. Lindgren
ISBN: 0-8493-0827-5

Architectures for e-Business
Sanjiv Purba, Editor
ISBN: 0-8493-1161-6

A Technical Guide to IPSec Virtual Private Networks
James S. Tiller
ISBN: 0-8493-0876-3

Building an Information Security Awareness Program
Mark B. Desman
ISBN: 0-8493-0116-5

Computer Telephony Integration
William Yarberry, Jr.
ISBN: 0-8493-9995-5

Cyber Crime Field Handbook
Bruce Middleton
ISBN: 0-8493-1192-6

Enterprise Systems Architectures
Mark Goodyear, Editor
ISBN: 0-8493-9836-3

Enterprise Systems Integration, 2nd Edition
Judith Myerson
ISBN: 0-8493-1149-7

Information Security Architecture
Jan Killmeyer Tudor
ISBN: 0-8493-9988-2

Information Security Management Handbook, 4th Edition, Volume 2
Harold F. Tipton and Micki Krause, Editors
ISBN: 0-8493-0800-3

Information Security Management Handbook, 4th Edition, Volume 3
Harold F. Tipton and Micki Krause, Editors
ISBN: 0-8493-1127-6

Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security
Thomas Peltier
ISBN: 0-8493-1137-3

Information Security Risk Analysis
Thomas Peltier
ISBN: 0-8493-0880-1

Information Technology Control and Audit
Frederick Gallegos, Sandra Allen-Senft, and Daniel P. Manson
ISBN: 0-8493-9994-7

Integrating ERP, CRM, Supply Chain Management, and Smart Materials
Dimitris N. Chorafas
ISBN: 0-8493-1076-8

New Directions in Internet Management
Sanjiv Purba, Editor
ISBN: 0-8493-1160-8

New Directions in Project Management
Paul C. Tinnirello, Editor
ISBN: 0-8493-1190-X

Oracle Internals: Tips, Tricks, and Techniques for DBAs
Donald K. Burleson, Editor
ISBN: 0-8493-1139-X

Practical Guide to Security Engineering and Information Assurance
Debra Herrmann
ISBN: 0-8493-1163-2

TCP/IP Professional Reference Guide
Gilbert Held
ISBN: 0-8493-0824-0

Roadmap to the e-Factory
Alex N. Beavers, Jr.
ISBN: 0-8493-0099-1

Securing E-Business Applications and Communications
Jonathan S. Held
John R. Bowers
ISBN: 0-8493-0963-8

AUERBACH PUBLICATIONS
www.auerbach-publications.com
To Order: Call: 1-800-272-7737 • Fax: 1-800-374-3401
E-mail: orders@crcpress.com

A PRACTICAL GUIDE TO

Security Engineering and Information Assurance

DEBRA S. HERRMANN

AUERBACH PUBLICATIONS

A CRC Press Company

Boca Raton London New York Washington, D.C.

Library of Congress Cataloging-in-Publication Data

Herrmann, Debra S.
A practical guide to security engineering and information assurance / Debra S. Herrmann.
p. cm.
Includes bibliographical references and index.
ISBN 0-8493-1163-2 (alk. paper)
1. Computer security. 2. Data Protection. I. Title.

QA76.9.A25 H47 2001
005.8—dc21 2001037901
CIP

Visit the Auerbach Publications Web site at
www.auerbach-publications.com

International Standard Book Number 0-8493-1163-2
Library of Congress Card Number 2001037901
Printed in the United States of America 1 2 3 4 5 6 7 8 9 0
Printed on acid-free paper

Abstract

This book is a comprehensive yet practical guide to security engineering and the broader realm of information assurance (IA). This book fills an important gap in the professional literature. It is the first book to:

1. Examine the impact of both accidental and malicious intentional action and inaction on information security and IA
2. Explore the synergy between security, safety, and reliability engineering that is the essence of IA
3. Introduce the concept of IA integrity levels
4. Provide a complete methodology for security engineering and IA throughout the life of a system

The relationship between security engineering and IA and why both are needed is explained. Innovative long-term vendor, technology, and application-independent strategies demonstrate how to protect critical systems and data from accidental and intentional action and inaction that could lead to a system failure/compromise. These real-world strategies are applicable to all systems, from small systems supporting a home-based business to those of a multi-national corporation, government agency, or critical infrastructure system. Step-by-step, in-depth solutions take one from defining information security/IA goals through performing vulnerability/threat analyses, implementing and verifying the effectiveness of threat control measures, to conducting accident/incident investigations, whether internal, independent, regulatory, or forensic. A review of historical approaches to information security/IA puts the discussion in context for today's challenges. Extensive glossaries of information security/IA terms and 80 techniques are an added bonus.

This book is written for engineers, scientists, managers, regulators, academics, and policy-makers responsible for information security/IA. Those who have to comply with Presidential Decision Directive (PDD-63), which requires all government agencies to implement an IA program and certify mission-critical systems by May 2003, will find this book especially useful.

Dedication

This book is dedicated to the memory of Harry E. Murray, Edward P. Herrmann, and Chet and Telma Cherryholmes.

Other Books by the Author

Software Safety and Reliability: Techniques, Approaches, and Standards of Key Industrial Sectors, IEEE Computer Society Press, 1999.

Contents

List of Exhibits

Chapter 2

Chapter 3

Chapter 4

Chapter 5

Chapter 6

Chapter 7

Chapter 8

Appendix B

Appendix D