

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

This book contains information obtained from authentic and highly regarded sources. Reprinted material is quoted with permission, and sources are indicated. A wide variety of references are listed. Reasonable efforts have been made to publish reliable data and information, but the author and the publisher cannot assume responsibility for the validity of all materials or for the consequences of their use.

Neither this book nor any part may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, microfilming, and recording, or by any information storage or retrieval system, without prior permission in writing from the publisher.

All rights reserved. Authorization to photocopy items for internal or personal use, or the personal or internal use of specific clients, may be granted by CRC Press LLC, provided that \$1.50 per page photocopied is paid directly to Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923 USA. The fee code for users of the Transactional Reporting Service is ISBN 0-8493-1163-2/01/\$0.00+\$1.50. The fee is subject to change without notice. For organizations that have been granted a photocopy license by the CCC, a separate system of payment has been arranged.

The consent of CRC Press LLC does not extend to copying for general distribution, for promotion, for creating new works, or for resale. Specific permission must be obtained in writing from CRC Press LLC for such copying.

Direct all inquiries to CRC Press LLC, 2000 N.W. Corporate Blvd., Boca Raton, Florida 33431.

Trademark Notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation, without intent to infringe.

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

© 2002 by CRC Press LLC

Auerbach is an imprint of CRC Press LLC

No claim to original U.S. Government works

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 multinational 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. Hermann, 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

1 Introduction

- 1.1 Background
- 1.2 Purpose
- 1.3 Scope
- 1.4 Intended Audience
- 1.5 Organization

2 What Is Information Assurance, How Does It Relate To Information Security, and Why Are Both Needed?

- 2.1 Definition
- 2.2 Application Domains
- 2.3 Technology Domains
- 2.4 Importance
- 2.5 Stakeholders
- 2.6 Summary
- 2.7 Discussion Problems

3 Historical Approaches To Information Security and Information Assurance

- 3.1 Physical Security
- 3.2 Communications Security (COMSEC)
- 3.3 Computer Security (COMPUSEC)
- 3.4 Information Security (INFOSEC)
- 3.5 Operations Security (OPSEC)
- 3.6 System Safety
- 3.7 System Reliability
- 3.8 Summary
- 3.9 Discussion Problems

4 Define the System Boundaries

- 4.1 Determine What is Being Protected and Why
- 4.2 Identify the System
- 4.3 Characterize System Operation
- 4.4 Ascertain What One Does and Does Not Have Control Over
- 4.5 Summary
- 4.6 Discussion Problems

5 Perform Vulnerability and Threat Analyses

- 5.1 Definitions
- 5.2 Select/Use IA Analysis Techniques
- 5.3 Identify Vulnerabilities, Their Type, Source, and Severity
- 5.4 Identify Threats, Their Type, Source, and Likelihood
- 5.5 Evaluate Transaction Paths, Critical Threat Zones, and Risk Exposure
- 5.6 Summary
- 5.7 Discussion Problems

6 Implement Threat Control Measures

- 6.1 Determine How Much Protection Is Needed
- 6.2 Evaluate Controllability, Operational Procedures, and In-Service Considerations
- 6.3 Contingency Planning and Disaster Recovery
- 6.4 Perception Management
- 6.5 Select/Implement IA Design Features and Techniques
- 6.6 Summary
- 6.7 Discussion Problems

7 Verify Effectiveness of Threat Control Measures

- 7.1 Select/Employ IA Verification Techniques
- 7.2 Determine Residual Risk Exposure
- 7.3 Monitor Ongoing Risk Exposure, Responses, and Survivability
- 7.4 Summary
- 7.5 Discussion Problems

8 Conduct Accident/Incident Investigations

- 8.1 Analyze Cause, Extent, and Consequences of Failure/Compromise
- 8.2 Initiate Short-Term Recovery Mechanisms
- 8.3 Report Accident/Incident
- 8.4 Deploy Long-Term Remedial Measures
- 8.5 Evaluate Legal Issues
- 8.6 Summary
- 8.7 Discussion Problems

Annex A Glossary of Terms

Annex B Glossary of Techniques

- B.1 IA Analysis Techniques
- B.2 IA Design Techniques/Features
- B.3 IA Verification Techniques
- B.4 IA Accident/Incident Investigation Techniques

Annex C Additional Resources

- C.1 Standards
- C.2 Publications
- C.3 Online Resources

Annex D Summary of Components, Activities, and Tasks of an Effective Information Security/IA Program

List of Exhibits

Chapter 2

- Exhibit 1 [Interaction and Interdependency Among Infrastructure Systems](#)
- Exhibit 2 [Interaction and Interdependency Between Infrastructure Systems, Mission-Critical Systems, and Business-Critical Systems](#)
- Exhibit 3 [Illustration of the Technology Domains Involved in Information Assurance Using an Online Purchase as an Example](#)
- Exhibit 4 [The Importance of IA in the Real World](#)
- Exhibit 5 [Sample Identification of Transaction Paths](#)
- Exhibit 6 [Sample Identification of Transaction Paths \(continued\)](#)
- Exhibit 7 [Sample Correlation of Vulnerabilities, Threats, Transaction Paths, and Consequences](#)

Chapter 3

- Exhibit 1 [Traditional Physical Security Perimeters](#)
- Exhibit 2 [Historical COMSEC Architecture](#)
- Exhibit 3 [Simple Illustration of the Steps Involved in Encryption](#)
- Exhibit 4 [Summary of Orange Book Trusted Computer System Evaluation Criteria \(TCSEC\) Divisions](#)
- Exhibit 5 [Summary of Orange Book Trusted Computer System Evaluation Criteria \(TCSEC\)](#)
- Exhibit 6 [Orange Book Testing Requirements](#)
- Exhibit 7 [ISO/IEC 15408-2 Functional Security Classes and Families](#)
- Exhibit 8 [ISO/IEC 15408-3 Security Assurance Classes and Families](#)
- Exhibit 9 [Summary of Common Criteria for IT Security Evaluation Assurance Levels \(EALs\)](#)
- Exhibit 10 [Examples of Items to Address in OPSEC Procedures](#)
- Exhibit 11 [Software as a Component of System Safety](#)
- Exhibit 12 [System Safety Tasks and Activities Required by MIL-STD-882D](#)
- Exhibit 13 [Summary of the Different Roles Played by Historical Approaches to Information Security/IA](#)
- Exhibit 14 [Summary of the Techniques Used by Historical Approaches to Information Security/IA](#)

Chapter 4

- Exhibit 1 Sample Statement of IA Goals
- Exhibit 2 Standard Hierarchy Used in System Definition
- Exhibit 3 Sample High-Level System Definition
- Exhibit 4 Sample High-Level System Definition
- Exhibit 5 Sample High-Level System Operation Characterization
- Exhibit 6 Sample High-Level System Entity Control Analysis
- Exhibit 7 Summary of Activities Involved in Defining System Boundaries

Chapter 5

- Exhibit 1 Interaction Between Vulnerabilities, Hazards, Threats, and Risk
- Exhibit 2 Information Assurance Analysis Techniques
 - Legend for Exhibit 5.2
- Exhibit 3 Analysis Role of IA Techniques
- Exhibit 4 Vulnerability Identification Process
- Exhibit 5 Correlation of Failure Points, Failure Scenarios, and Vulnerabilities
- Exhibit 6 Classification of IA Vulnerabilities
- Exhibit 7 Identification of Vulnerability Types
- Exhibit 8 Identification of Vulnerability Sources
- Exhibit 9 Identification of Vulnerability Severity
- Exhibit 10 Potential COTS Vulnerabilities
- Exhibit 11 Vulnerability Characterization Summary: Online Banking System
- Exhibit 12 Characterization of IA Threats
- Exhibit 13 Threat Identification: Online Banking System
- Exhibit 14 Threat Characterization Summary: Online Banking System
- Exhibit 15 Correlation of Threat Likelihood and Vulnerability Severity to Prioritize Threat Control Measures
- Exhibit 16 High-Level Depiction of the Logical Operation of an ATC System
- Exhibit 17 Potential Transaction Paths Leading to the Compromise of a Hypothetical ATC System
- Exhibit 18 Potential Transaction Paths Leading to the Compromise of a Hypothetical ATC System (continued)
- Exhibit 19 Potential Transaction Paths Leading to the Compromise of a Hypothetical ATC System (continued)
- Exhibit 20 Potential Transaction Paths Leading to the Compromise of a Hypothetical ATC System (continued)
- Exhibit 21 Potential Transaction Paths Leading to the Compromise of a Hypothetical ATC System (continued)
- Exhibit 22 Potential Transaction Paths Leading to the Compromise of a Hypothetical ATC System (continued)
- Exhibit 23 Potential Transaction Paths Leading to the Compromise of a Hypothetical ATC System (continued)
- Exhibit 24 Potential Transaction Paths Leading to the Compromise of a Hypothetical ATC System (continued)
- Exhibit 25 Potential Transaction Paths Leading to the Compromise of a Hypothetical ATC System (continued)
- Exhibit 26 System Compromises Examined from Different Threat Perspectives
- Exhibit 27 Components of Risk Exposure and Their Interaction
- Exhibit 28 Summary of the Activities Involved in Performing Vulnerability and Threat Analyses

Chapter 6

- Exhibit 1 Proactive Responses to Common Accident/Incident Precursors
- Exhibit 2 Chronology of Threat Control Measures
- Exhibit 3 Summary of the Activities Involved in Determining the Level of Protection Needed
- Exhibit 4 High-Level Identification of Entity Criticality
- Exhibit 5 High-Level Identification of MWFs and MNWFs
- Exhibit 6 Relationship Between Controllability and IA Integrity Levels
- Exhibit 7 Contingency Planning Process
- Exhibit 8 Contingency Planning Process (continued)
- Exhibit 9 Contingency Planning Checklist (partial)
- Exhibit 10 IA Design Techniques and Features
Legend for the codes used in Exhibit 6.10
- Exhibit 11 Comparison of ISO OSI Information/Communications and TCP/IP Internet Reference Models
- Exhibit 12 Assignment of Common Vulnerabilities and Threats to ISO OSI and TCP/IP Reference Model Layers
- Exhibit 13 Assignment of IA Techniques and Features to ISO OSI and TCP/IP Reference Model Layers
- Exhibit 14 Comparison of Methods for Specifying Access Control Rules
- Exhibit 15 How to Account for All Possible Logic States
- Exhibit 16 Use of Audit Trail Data to Maintain and Improve IA Integrity
- Exhibit 17 Illustration of Block Recovery Logic
- Exhibit 18 Illustration of Defense in Depth
- Exhibit 19 Key Decisions to Make when Implementing Encryption
- Exhibit 20 Potential Encryption Points in a Typical Information Architecture
Legend for Exhibit 6.20
- Exhibit 21 Sample Formal Specifications
- Exhibit 22 Summary of Activities Involved in Implementing Threat Control Measures
- Exhibit 23 Correlation of IA Design Techniques/Features to the Chronology of Threat Control Measures
- Exhibit 24 Assignment of IA Design Techniques/Features to Common Vulnerabilities and Threats

Chapter 7

- Exhibit 1 IA Verification Techniques
Legend for Exhibit 7.1
- Exhibit 2 Verification Role of IA Techniques
- Exhibit 3 Sample High-Level Test Scenarios for Verifying the Effectiveness of Threat Control Measures: The Radiation Therapy System
- Exhibit 4 Sample High-Level Test Scenarios for Verifying the Effectiveness of Threat Control Measures: The ATC System
- Exhibit 5 Sample High-Level Test Scenarios for Verifying the Effectiveness of Threat Control Measures: The Online Banking System
- Exhibit 6 Checklist for Verifying the Effectiveness of Three Threat Control Measures
- Exhibit 7 Threat Control Effectiveness Assessment
- Exhibit 8 Threat Control Effectiveness Summary
- Exhibit 9 Structure of an IA Integrity Case
- Exhibit 10 Summary of Activities Involved in Verifying the Effectiveness of Threat Control Measures

Chapter 8

- Exhibit 1 [Comparison of Legal and Engineering Cause Categories](#)
- Exhibit 2 [Generic Accident/Incident Evidence Sources](#)
- Exhibit 3 [IA Accident/Incident Investigation Techniques](#)
[Legend for Exhibit 8.3](#)
- Exhibit 4 [Accident/Incident Investigation Role of IA Techniques](#)
- Exhibit 5 [Barrier Analysis Concept](#)
- Exhibit 6 [Barrier Analysis Report](#)
- Exhibit 7 [Event and Causal Factor Chart](#)
- Exhibit 8 [Standard STEP Investigation System Symbols and Notation](#)
- Exhibit 9 [STEP Investigation Diagram](#)
- Exhibit 10 [STEP Investigation Diagram \(continued\)](#)
- Exhibit 11 [STEP Investigation Diagram \(continued\)](#)
[Legend for Exhibits 9 through 11](#)
- Exhibit 12 [TLA Graphs](#)
- Exhibit 13 [Warning Time Analysis Report](#)
- Exhibit 14 [Interaction Between Accident/Incident Investigation Techniques](#)
- Exhibit 15 [Accident/Incident Recovery Steps](#)
- Exhibit 16 [Accident/Incident Report: Part I](#)
- Exhibit 17 [Accident/Incident Report: Part II](#)
- Exhibit 18 [Information Flow Between Accident/Incident Investigations, Reports, and Remedial Measures](#)
- Exhibit 19 [Summary of Activities Involved in Conducting Accident/Incident Investigations](#)
- Exhibit 20 [Summary of Activities Involved in Conducting Accident/Incident Investigations \(continued\)](#)

Appendix B

- Exhibit 1 [Legend for Exhibits B.2 through B.5](#)
- Exhibit 2 [Information Assurance Analysis Techniques](#)
- Exhibit 3 [Information Assurance Design Techniques and Features](#)
- Exhibit 4 [Information Assurance Verification Techniques](#)
- Exhibit 5 [Information Assurance Accident/Incident Investigation Techniques](#)

Appendix D

- Exhibit 1 [Interaction Between Components of an Effective Computer Security/IA Program](#)
- Exhibit 2 [Summary of the Components, Activities, and Tasks of an Effective Information Security/IA Program](#)