AUERBACH

USING the COMMON CRITERIA for IT SECURITY EVALUATION

DEBRA S. HERRMANN

USING the COMMON CRITERIA for IT SECURITY EVALUATION

OTHER AUERBACH PUBLICATIONS

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

The ABCs of TCP/IP
Gilbert Held
ISBN: 0-8493-1463-1

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

Building a Wireless Office
Gilbert Held
ISBN: 0-8493-1271-X

The Complete Book of Middleware
Judith Myerson
ISBN: 0-8493-1272-8

Computer Telephony Integration, 2nd Edition
William A. Yarberry, Jr.
ISBN: 0-8493-1438-0

Cyber Crime Investigator's Field Guide
Bruce Middleton
ISBN: 0-8493-1192-6

Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes
Albert J. Marcella and Robert S. Greenfield, Editors
ISBN: 0-8493-0955-7

Global Information Warfare: How Businesses, Governments, and Others Achieve Objectives and Attain Competitive Advantages
Andy Jones, Gerald L. Kovacich,
and Perry G. Luzwick
ISBN: 0-8493-1114-4

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

Information Security Management Handbook, 4th Edition, Volume 1
Harold F. Tipton and Micki Krause, Editors
ISBN: 0-8493-9829-0

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 Management Handbook, 4th Edition, Volume 4
Harold F. Tipton and Micki Krause, Editors
ISBN: 0-8493-1518-2

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

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

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

The Privacy Papers: Managing Technology and Consumers, Employee, and Legislative Action
Rebecca Herold
ISBN: 0-8493-1248-5

Secure Internet Practices: Best Practices for Securing Systems in the Internet and e-Business Age
Patrick McBride, Jody Patilla,
Craig Robinson, Peter Thermos,
and Edward P. Moser
ISBN: 0-8493-1239-6

Securing and Controlling Cisco Routers
Peter T. Davis
ISBN: 0-8493-1290-6

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

Securing Windows NT/2000: From Policies to Firewalls
Michael A. Simonyi
ISBN: 0-8493-1261-2

Six Sigma Software Development
Christine B. Tayntor
ISBN: 0-8493-1193-4

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

Telecommunications Cost Management
Brian DiMarsico, Thomas Phelps IV,
and William A. Yarberry, Jr.
ISBN: 0-8493-1101-2

AUERBACH PUBLICATIONS

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

USING the COMMON CRITERIA for IT SECURITY EVALUATION

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.
Using the Common Criteria for IT security evaluation / Debra S. Herrmann.
p. cm.
Includes bibliographical references and index.
ISBN 0-8493-1404-6 (alk. paper)
1. Telecommunication—Security measures—Standards. 2. Computer security—Standards. 3. Information technology—Standards. I. Title.

TK5102.85 .H47 2002
005.8—dc21 2002033250
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.

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.

No claim to original U.S. Government works
International Standard Book Number 0-8493-1404-6
Library of Congress Card Number 2002033250
Printed in the United States of America 1 2 3 4 5 6 7 8 9 0
Printed on acid-free paper

Dedication

This book is dedicated to the victims of terrorist attacks
in Israel, New York City, Pennsylvania, and Washington, D.C.

Other Books by the Author

A Practical Guide to Security Engineering and Information Assurance (Auerbach Publications, 2001)

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

Table of Contents

Chapter 4 Designing a Security Architecture: The Security Target 125

List of Exhibits

Chapter 2

Chapter 3

Chapter 4

Chapter 5

Chapter 1

Introduction

1.0 Background

In December 1999, ISO/IEC 15408, Parts 1–3 (Criteria for IT Security Evaluation), was approved as an international standard. The Common Criteria (CC) are considered *the* international standard for information technology (IT) security and provide a complete methodology, notation, and syntax for specifying security requirements, designing a security architecture, and verifying the security integrity of an "as built" product, system, or network. Roles and responsibilities for a variety of stakeholders are defined, such as:

- *Customers* — corporations, government agencies, and other organizations who want to acquire security products, systems, and networks
- *Developers* — (a) system integrators who implement or manage security systems and networks for customers, and (b) vendors who manufacture and sell commercial "off the shelf" (COTS) security products
- *Evaluators* — accredited Common Criteria Testing Laboratories, which perform an independent evaluation of the security integrity of a product, system, or network

Many organizations and government agencies require the use of CC-certified products and systems and use the CC methodology in their acquisition process. For example, in the United States, NSTISSP #11 (National Information Assurance Acquisition Policy)[75] mandated the use of CC-evaluated IT security products in critical infrastructure systems starting in July 2002.

Like ISO 9000, the Common Criteria have a mutual recognition agreement so that products certified in one country are recognized in another. As of June 2002, 15 countries have signed the mutual recognition agreement: Australia, Canada, Finland, France, Germany, Greece, Israel, Italy, the Netherlands, New Zealand, Norway, Spain, Sweden, the United Kingdom, and the United States.

1.1 Purpose

This book is a user's guide for the Criteria for IT Security Evaluation. It explains in detail how to understand, interpret, apply, and employ the Common Criteria methodology throughout the life of a system, including the acquisition and certification and accreditation (C&A) processes.

1.2 Scope

This book is limited to a discussion of ISO/IEC 15408, Parts 1–3 (Criteria for IT Security Evaluation) and how to use the Common Criteria within a generic system-development lifecycle and a generic procurement process. The terminology, concepts, techniques, activities, roles, and responsibilities comprising the Common Criteria methodology are emphasized.

1.3 Intended Audience

This book is written for program managers, product development managers, acquisition managers, security engineers, and system engineers responsible for the specification, design, development, integration, test and evaluation, or acquisition of IT security products and systems. A basic understanding of security engineering concepts and terminology is assumed; however, extensive security engineering experience is not expected.

The Common Criteria define three generic categories of stakeholders: customers, developers, and evaluators. In practice, these categories are further refined into customers or end users, IT product vendors, sponsors, Common Criteria Testing Laboratories (CCTLs), National Evaluation Authorities, and the Common Criteria Implementation Management Board (CCIMB). All six perspectives are captured in this book.

1.4 Organization

This book is organized into six chapters. Chapter 1 puts the book in context by explaining the purpose for which the book was written. Limitations on the scope of the subject matter of the book, the intended audience for whom the book was written, and the organization of the book are explained.

Chapter 2 introduces the Common Criteria (CC) by:

- Describing the historical events that led to their development
- Delineating the purpose and intended use of the CC and, conversely, situations not covered by the CC
- Explaining the major concepts and components of the CC methodology and how they work

- Illustrating how the CC relate to other well-known national and international standards
- Discussing the CC user community and stakeholders
- Looking at the future of the CC

Chapter 3 explains how to express security requirements through the instrument of a Protection Profile (PP) using the CC standardized methodology, syntax, and notation. The required content and format of a PP are discussed section by section. The perspective from which to read and interpret PPs is defined. In addition, the purpose, scope, and development of a PP are mapped to both a generic system lifecycle and a generic procurement process.

Chapter 4 explains how to design a security architecture, in response to a PP, through the instrument of a Security Target (ST) using the CC standardized methodology, syntax, and notation. The required content and format of an ST are discussed section by section. The perspective from which to read and interpret STs is defined. In addition, the purpose, scope, and development of an ST are mapped to both a generic system lifecycle and a generic procurement sequence.

Chapter 5 explains how to verify a security solution, whether a system or COTS product, using the CC/CEM (Common Evaluation Methodology). The conduct of security assurance activities is examined in detail, particularly why, how, when, and by whom these activities are conducted. Guidance is provided on how to interpret the results of security assurance activities. The relationship between these activities and a generic system lifecycle, as well as a generic procurement process, is explained. Finally, the role of security assurance activities during ongoing system operations and maintenance is highlighted.

Chapter 6 explores new and emerging concepts within the CC/CEM that are under discussion within the CC user community. These concepts have not yet been formally incorporated into the standard or methodology but are likely to be so in the near future.

Six informative annexes are also provided. Annex A is a glossary of acronyms and terms related to the Common Criteria. Annex B lists the sources that were consulted during the development of this book and provides pointers to other resources that may be of interest to the reader. Annex B is organized in three parts: (1) standards, regulations, and policy; (2) publications; and (3) online resources. Annex C cites the participants who have signed the Common Criteria Recognition Agreement (CCRA) and provides contact information for each country's National Evaluation Authority. Annex D lists organizations that are currently recognized as certified CCTLs in Australia and New Zealand, Canada, France, Germany, the United Kingdom, and the United States. Annex E lists organizations that are currently certified to operate Cryptographic Module Validation Program (CMVP) laboratories in Canada and the United States. Annex F is a glossary of CC three-character class and family mnemonics.