Computer and Information Security Handbook

The Morgan Kaufmann Series in Computer Security

Computer and Information Security Handbook
John Vacca

Disappearing Cryptography: Information Hiding: Steganography & Watermarking, Third Edition
Peter Wayner

Network Security: Know It All
James Joshi, et al.

Digital Watermarking and Steganography, Second Edition
Ingemar Cox, Matthew Miller, Jeffrey Bloom, Jessica Fridrich, and Ton Kalker

Information Assurance: Dependability and Security in Networked Systems
Yi Qian, David Tipper, Prashant Krishnamurthy, and James Joshi

Network Recovery: Protection and Restoration of Optical, SONET-SDH, IP, and MPLS
Jean-Philippe Vasseur, Mario Pickavet, and Piet Demeester

For further information on these books and for a list of forthcoming titles,
please visit our Web site at http://www.elsevierdirect.com

Computer and Information Security Handbook

Edited by
John R. Vacca

ELSEVIER

AMSTERDAM • BOSTON • HEIDELBERG • LONDON • NEW YORK
OXFORD • PARIS • SAN DIEGO • SAN FRANCISCO
SINGAPORE • SYDNEY • TOKYO

Morgan Kaufmann Publishers is an imprint of Elsevier

MORGAN KAUFMANN
PUBLISHERS

Morgan Kaufmann Publishers is an imprint of Elsevier.
30 Corporate Drive, Suite 400, Burlington, MA 01803, USA

This book is printed on acid-free paper.

Library of Congress Cataloging-in-Publication Data
Application submitted

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library.

ISBN: 978-0-12-374354-1

Printed in the United States of America
09 10 11 12 13 5 4 3 2 1

This book is dedicated to my wife, Bee.

Contents

Part IV
Privacy and Access Management

Foreword

The Computer and Information Security Handbook is an essential reference guide for professionals in all realms of computer security. Researchers in academia, industry, and government as well as students of security will find the *Handbook* helpful in expediting security research efforts. The *Handbook* should become a part of every corporate, government, and university library around the world.

Dozens of experts from virtually every industry have contributed to this book. The contributors are the leading experts in computer security, privacy protection and management, and information assurance. They are individuals who will help others in their communities to address the immediate as well as long-term challenges faced in their respective computer security realms.

These important contributions make the *Handbook* stand out among all other security reference guides. I know and have worked with many of the contributors and can testify to their experience, accomplishments, and dedication to their fields of work.

John Vacca, the lead security consultant and managing editor of the *Handbook*, has worked diligently to see that this book is as comprehensive as possible. His knowledge, experience, and dedication have combined to create a book of more than 1400 pages covering every important aspect of computer security and the assurance of the confidentiality, integrity, and availability of information.

The depth of knowledge brought to the project by all the contributors assures that this comprehensive handbook will serve as a professional reference and provide a complete and concise view of computer security and privacy. The *Handbook* provides in-depth coverage of computer security theory, technology, and practice as it relates to established technologies as well as recent advancements in technology. Above all, the *Handbook* explores practical solutions to a wide range of security issues.

Another important characteristic of the *Handbook* is that it is a vendor-edited volume with chapters written by leading experts in industry and academia who do not support any specific vendor's products or services. Although there are many excellent computer security product and service companies, these companies often focus on promoting their offerings as one-and-only, best-on-the-market solutions. Such bias can lead to narrow decision making and product selection and thus was excluded from the *Handbook*.

Michael Erbschloe
Michael Erbschloe teaches information security courses at Webster University in St. Louis, Missouri.

Preface

This comprehensive handbook serves as a professional reference to provide today's most complete and concise view of computer security and privacy available in one volume. It offers in-depth coverage of computer security theory, technology, and practice as they relate to established technologies as well as recent advancements. It explores practical solutions to a wide range of security issues. Individual chapters are authored by leading experts in the field and address the immediate and long-term challenges in the authors' respective areas of expertise.

The primary audience for this handbook consists of researchers and practitioners in industry and academia as well as security technologists and engineers working with or interested in computer security. This comprehensive reference will also be of value to students in upper-division undergraduate and graduate-level courses in computer security.

ORGANIZATION OF THIS BOOK

The book is organized into eight parts composed of 43 contributed chapters by leading experts in their fields, as well as 10 appendices, including an extensive glossary of computer security terms and acronyms.

Part 1: Overview of System and Network Security: A Comprehensive Introduction

Part 1 discusses how to build a secure organization; generating cryptography; how to prevent system intrusions; UNIX and Linux security; Internet and intranet security; LAN security; wireless network security; cellular network security, and RFID security. For instance:

Chapter 1, "Building a Secure Organization," sets the stage for the rest of the book by presenting insight into where to start building a secure organization.

Chapter 2, "A Cryptography Primer," provides an overview of cryptography. It shows how communications may be encrypted and transmitted.

Chapter 3, "Preventing System Intrusions," discusses how to prevent system intrusions and where an unauthorized penetration of a computer in your enterprise or an address in your assigned domain can occur.

Chapter 4, "Guarding Against Network Intrusions," shows how to guard against network intrusions by understanding the variety of attacks, from exploits to malware and social engineering.

Chapter 5, "UNIX and Linux Security," discusses how to scan for vulnerabilities; reduce denial-of-service (DoS) attacks; deploy firewalls to control network traffic; and build network firewalls.

Chapter 6, "Eliminating the Security Weakness of Linux and UNIX Operating Systems," presents an introduction to securing UNIX in general and Linux in particular, providing some historical context and describing some fundamental aspects of the secure operating system architecture.

Chapter 7, "Internet Security," shows you how cryptography can be used to address some of the security issues besetting communications protocols.

Chapter 8, "The Botnet Problem," describes the botnet threat and the countermeasures available to network security professionals.

Chapter 9, "Intranet Security," covers internal security strategies and tactics; external security strategies and tactics; network access security; and Kerberos.

Chapter 10, "Local Area Network Security," discusses network design and security deployment as well as ongoing management and auditing.

Chapter 11, "Wireless Network Security," presents an overview of wireless network security technology; how to design wireless network security and plan for wireless network security; how to install, deploy, and maintain wireless network security; information warfare countermeasures: the wireless network security solution; and wireless network security solutions and future directions.

Chapter 12, "Cellular Network Security," addresses the security of the cellular network; educates readers on the current state of security of the network and its vulnerabilities; outlines the cellular network specific attack taxonomy, also called *three-dimensional attack taxonomy*; discusses the vulnerability assessment tools for cellular networks; and provides

insights into why the network is so vulnerable and why securing it can prevent communication outages during emergencies.

Chapter 13, "RFID Security," describes the RFID tags and RFID reader and back-end database in detail.

Part 2: Managing Information Security

Part 2 discusses how to protect mission-critical systems; deploy security management systems, IT security, ID management, intrusion detection and prevention systems, computer forensics, network forensics, firewalls, and penetration testing; and conduct vulnerability assessments. For instance:

Chapter 14, "Information Security Essentials for IT Managers: Protecting Mission-Critical Systems," discusses how security goes beyond technical controls and encompasses people, technology, policy, and operations in a way that few other business objectives do.

Chapter 15, "Security Management Systems," examines documentation requirements and maintaining an effective security system as well as conducting assessments.

Chapter 16, "Information Technology Security Management," discusses the processes that are supported with enabling organizational structure and technology to protect an organization's information technology operations and IT assets against internal and external threats, intentional or otherwise.

Chapter 17, "Identity Management," presents the evolution of identity management requirements. It also surveys how the most advanced identity management technologies fulfill present-day requirements. It discusses how mobility can be achieved in the field of identity management in an ambient intelligent/ubiquitous computing world.

Chapter 18, "Intrusion Prevention and Detection Systems," discusses the nature of computer system intrusions, the people who commit these attacks, and the various technologies that can be utilized to detect and prevent them.

Chapter 19, "Computer Forensics," is intended to provide an in-depth familiarization with computer forensics as a career, a job, and a science. It will help you avoid mistakes and find your way through the many aspects of this diverse and rewarding field.

Chapter 20, "Network Forensics," helps you determine the path from a victimized network or system through any intermediate systems and communication pathways, back to the point of attack origination or the person who should be held accountable.

Chapter 21, "Firewalls," provides an overview of firewalls: policies, designs, features, and configurations. Of course, technology is always changing, and network firewalls are no exception. However, the intent of this chapter is to describe aspects of network firewalls that tend to endure over time.

Chapter 22, "Penetration Testing," describes how testing differs from an actual "hacker attack" as well as some of the ways penetration tests are conducted, how they're controlled, and what organizations might look for when choosing a company to conduct a penetration test for them.

Chapter 23, "What Is Vulnerability Assessment?" covers the fundamentals: defining vulnerability, exploit, threat, and risk; analyzing vulnerabilities and exploits; and configuring scanners. It also shows you how to generate reports, assess risks in a changing environment, and manage vulnerabilities.

Part 3: Encryption Technology

Part 3 discusses how to implement data encryption, satellite encryption, public key infrastructure, and instant-messaging security. For instance:

Chapter 24, "Data Encryption," is about the role played by cryptographic technology in data security.

Chapter 25, "Satellite Encryption," proposes a method that enhances and complements satellite encryption's role in securing the information society. It also covers satellite encryption policy instruments; implementing satellite encryption; misuse of satellite encryption technology; and results and future directions.

Chapter 26, "Public Key Infrastructure," explains the cryptographic background that forms the foundation of PKI systems; the mechanics of the X.509 PKI system (as elaborated by the Internet Engineering Task Force); the practical issues surrounding the implementation of PKI systems; a number of alternative PKI standards; and alternative cryptographic strategies for solving the problem of secure public key distribution.

Chapter 27, "Instant-Messaging Security," helps you develop an IM security plan, keep it current, and make sure it makes a difference.

Part 4: Privacy and Access Management

Part 4 discusses Internet privacy, personal privacy policies, virtual private networks, identity theft, and VoIP security. For instance:

Chapter 28, "Net Privacy," addresses the privacy issues in the digital society from various points of view, investigating the different aspects related to the notion of privacy and the debate that the intricate essence of privacy has stimulated; the most common privacy threats and the possible economic aspects that may influence the way privacy is (and especially is not currently) managed in most firms; the efforts in the computer science community to face privacy threats, especially in the context of mobile and database systems; and the network-based technologies available to date to provide anonymity when communicating over a private network.

Chapter 29, "Personal Privacy Policies," begins with the derivation of policy content based on privacy legislation, followed by a description of how a personal privacy policy may be constructed semiautomatically. It then shows how to additionally specify policies so that negative unexpected outcomes can be avoided. Finally, it describes the author's Privacy Management Model, which explains how to use personal privacy policies to protect privacy, including what is meant by a "match" of consumer and service provider policies and how nonmatches can be resolved through negotiation.

Chapter 30, "Virtual Private Networks," covers VPN scenarios, VPN comparisons, and information assurance requirements. It also covers building VPN tunnels; applying cryptographic protection; implementing IP security; and deploying virtual private networks.

Chapter 31, "Identity Theft," describes the importance of understanding the human factor of ID theft security and details the findings from a study on deceit.

Chapter 32, "VoIP Security," deals with the attacks targeted toward a specific host and issues related to social engineering.

Part 5: Storage Security

Part 5 covers storage area network (SAN) security and risk management. For instance:

Chapter 33, "SAN Security," describes the following components: protection rings; security and protection; restricting access to storage; access control lists (ACLs) and policies; port blocks and port prohibits; and zoning and isolating resources.

Chapter 34, "Storage Area Networking Security Devices," covers all the issues and security concerns related to SAN security.

Chapter 35, "Risk Management," discusses physical security threats, environmental threats, and incident response.

Part 6: Physical Security

Part 6 discusses physical security essentials, biometrics, homeland security, and information warfare. For instance:

Chapter 36, "Physical Security Essentials," is concerned with physical security and some overlapping areas of premises security. It also looks at physical security threats and then considers physical security prevention measures.

Chapter 37, "Biometrics," discusses the different types of biometrics technology and verification systems and how the following work: biometrics eye analysis technology; biometrics facial recognition technology; facial thermal imaging; biometrics finger-scanning analysis technology; biometrics geometry analysis technology; biometrics verification technology; and privacy-enhanced, biometrics-based verification/authentication as well as biometrics solutions and future directions.

Chapter 38, "Homeland Security," describes some principle provisions of U.S. homeland security-related laws and Presidential directives. It gives the organizational changes that were initiated to support homeland security in the United States. The chapter highlights the 9/11 Commission that Congress charted to provide a full account of the circumstances surrounding the 2001 terrorist attacks and to develop recommendations for corrective measures that could be taken to prevent future acts of terrorism. It also details the Intelligence Reform and Terrorism Prevention Act of 2004 and the Implementation of the 9/11 Commission Recommendations Act of 2007.

Chapter 39, "Information Warfare," defines information warfare (IW) and discusses its most common tactics, weapons, and tools as well as comparing IW terrorism with conventional warfare and addressing the issues of liability and the available legal remedies under international law.

Part 7: Advanced Security

Part 7 discusses security through diversity, online reputation, content filtering, and data loss protection. For instance:

Chapter 40, "Security Through Diversity," covers some of the industry trends in adopting diversity in hardware, software, and application deployments. This chapter also covers the risks of uniformity, conformity, and the ubiquitous impact of adopting standard organizational principals without the consideration of security.

Chapter 41, "Reputation Management," discusses the general understanding of the human notion of reputation. It explains how this concept of reputation fits into computer security. The chapter presents the state of the art of attack-resistant reputation computation. It also gives an overview of the current market of online reputation services. The chapter concludes by underlining the need to standardize online reputation for increased adoption and robustness.

Chapter 42, "Content Filtering," examines the many benefits and justifications of Web-based content filtering such as legal liability risk reduction, productivity gains, and bandwidth usage. It also explores the downside and unintended consequences and risks that improperly deployed or misconfigured systems create. The chapter also looks into methods to subvert and bypass these systems and the reasons behind them.

Chapter 43, "Data Loss Protection," introduces the reader to a baseline understanding of how to investigate and evaluate DLP applications in the market today.

John R. Vacca
Editor-in-Chief
jvacca@frognet.net
www.johnvacca.com

Acknowledgments

There are many people whose efforts on this book have contributed to its successful completion. I owe each a debt of gratitude and want to take this opportunity to offer my sincere thanks.

A very special thanks to my senior acquisitions editor, Rick Adams, without whose continued interest and support this book would not have been possible. Assistant editor Heather Scherer provided staunch support and encouragement when it was most needed. Thanks to my production editor, A. B. McGee_and copyeditor, Darlene Bordwell, whose fine editorial work has been invaluable. Thanks also to my marketing manager, Marissa Hederson, whose efforts on this book have been greatly appreciated. Finally, thanks to all the other people at Computer Networking and Computer and Information Systems Security, Morgan Kaufmann Publishers/Elsevier Science & Technology Books, whose many talents and skills are essential to a finished book.

Thanks to my wife, Bee Vacca, for her love, her help, and her understanding of my long work hours. Also, a very, very special thanks to Michael Erbschloe for writing the Foreword. Finally, I wish to thank all the following authors who contributed chapters that were necessary for the completion of this book: John Mallery, Scott R. Ellis, Michael West, Tom Chen, Patrick Walsh, Gerald Beuchelt, Mario Santana, Jesse Walker, Xinyuan Wang, Daniel Ramsbrock, Bill Mansoor, Dr. Pramod Pandya, Chunming Rong, Prof. Erdal Cayirci, Prof. Gansen Zhao, Liang Yan, Peng Liu, Thomas F La Porta, Kameswari Kotapati, Albert Caballero, Joe Wright, Jim Harmening, Rahul Bhaskar, Prof. Bhushan Kapoor, Dr. Jean-Marc Seigneur, Christopher W. Day, Yong Guan, Dr. Errin W. Fulp, Sanjay Bavisi, Almantas Kakareka, Daniel S. Soper, Terence Spies, Samuel JJ Curry, Marco Cremonini, Chiara Braghin, Claudio Agostino Ardagna, Dr. George Yee, Markus Jacobsson, Alex Tsow, Sid Stamm, Chris Soghoian, Harsh Kupwade Patil, Dan Wing, Jeffrey S. Bardin, Robert Rounsavall, Sokratis K. Katsikas, William Stallings, Luther Martin, Jan Eloff, Anna Granova, Kevin Noble, Peter Nicoletti, and Ken Perkins.

About the Editor

John Vacca is an information technology consultant and bestselling author based in Pomeroy, Ohio. Since 1982 John has authored 60 books. Some of his most recent works include *Biometric Technologies and Verification Systems* (Elsevier, 2007); *Practical Internet Security* (Springer, 2006); *Optical Networking Best Practices Handbook* (Wiley-Interscience, 2006); *Guide to Wireless Network Security* (Springer, 2006); *Computer Forensics: Computer Crime Scene Investigation, 2nd Edition* (Charles River Media, 2005); *Firewalls: Jumpstart for Network and Systems Administrators* (Elsevier, 2004); *Public Key Infrastructure: Building Trusted Applications and Web Services (*Auerbach, 2004); *Identity Theft* (Prentice Hall/PTR, 2002); *The World's 20 Greatest Unsolved Problems* (Pearson Education, 2004); and more than 600 articles in the areas of advanced storage, computer security, and aerospace technology. John was also a configuration management specialist, computer specialist, and the computer security official (CSO) for NASA's space station program (Freedom) and the International Space Station Program from 1988 until his early retirement from NASA in 1995.

Contributors

Claudio Agostino Ardagna (Chapter 28), Dept. of Information Technology, University of Milan, Crema, Italy

Jeffrey S. Bardin (Chapter 33), Independent Security Consultant, Barre, Massachusetts 01005

Jay Bavisi (Chapter 22), President, EC-Council, Albuquerque, New Mexico 87109

Gerald Beuchelt (Chapter 5), Independent Security Consultant, Burlington, Massachusetts 01803

Rahul Bhaskar (Chapter 38), Department of Information Systems and Decision Sciences, California State University, Fullerton, California 92834

Rahul Bhaskar (Chapter 16), Department of Information Systems and Decision Sciences, California State University, Fullerton, California 92834

Chiara Braghin (Chapter 28), Dept. of Information Technology, University of Milan, Crema, Italy

Albert Caballero CISSP, GSEC (Chapter 14), Security Operations Center Manager, Terremark Worldwide, Inc., Bay Harbor Islands, Florida 33154

Professor Erdal Cayirci (Chapters 11, 13), University of Stavanger, N-4036 Stavanger, Norway

Tom Chen (Chapter 4), Swansea University, Singleton Park, SA2 8PP, Wales, United Kingdom

Marco Cremonini (Chapter 28), Dept. of Information Technology, University of Milan, Crema, Italy

Sam Curry (Chapter 27), VP Product Management, RSA, the Security Division of EMC, Bedford, Massachusetts 01730

Christopher Day, CISSP, NSA:IEM (Chapter 18), Senior Vice President, Secure Information Systems, Terremark Worldwide, Inc., Miami, Florida 33131

Scott R. Ellis, EnCE (Chapters 2, 19), RGL – Forensic Accountants & Consultants, Forensics and Litigation Technology, Chicago, Illinois 60602

Jan H. P. Eloff (Chapter 39), Extraordinary Professor, Information & Computer Security Architectures Research Group, Department of Computer Science, University of Pretoria, and Research Director SAP Meraka UTD/SAP Research CEC, Hillcrest, Pretoria, South Africa, 0002

Michael Erbschloe (Foreword), Teaches Information Security courses at Webster University, St. Louis, Missouri 63119

Errin W. Fulp (Chapter 21), Department of Computer Science, Wake Forest University, Winston-Salem, North Carolina 27109

Anna Granova (Chapter 39), Advocate of the High Court of South Africa, Member of the Pretoria Society of Advocates, University of Pretoria, Computer Science Department, Hillcrest, Pretoria, South Africa, 0002

Yong Guan (Chapter 20), Litton Assistant Professor, Department of Electrical and Computer Engineering, Iowa State University, Ames, Iowa 50011

James T. Harmening (Chapters 15, 30), Computer Bits, Inc., Chicago, Illinois 60602

Markus Jakobsson (Chapter 31), Principal Scientist, CSL, Palo Alto Research Center, Palo Alto, California 94304

Almantas Kakareka (Chapter 23), Terremark World Wide Inc., Security Operations Center, Miami, Florida 33132

Bhushan Kapoor (Chapters 16, 24, 38), Department of Information Systems and Decision Sciences, California State University, Fullerton, California 92834

Sokratis K. Katsikas (Chapter 35), Department of Technology Education & Digital Systems, University of Piraeus, Piraeus 18532, Greece

Larry Korba (Chapter 29), Ottawa, Ontario, Canada K1G 5N7.

Kameswari Kotapati (Chapter 12), Department of Computer Science and Engineering, The Pennsylvania State University, University Park, Pennsylvania 16802

Thomas F. LaPorta (Chapter 12), Department of Computer Science and Engineering, The Pennsylvania State University, University Park, Pennsylvania 16802

Peng Liu (Chapter 12), College of Information Sciences and Technology, The Pennsylvania State University, University Park, Pennsylvania 16802

Tewfiq El Maliki (Chapter 17), Telecommunications labs, University of Applied Sciences of Geneva, Geneva, Switzerland

John R. Mallery (Chapter 1), BKD, LLP, Kansas City, Missouri 64105-1936

Bill Mansoor (Chapter 9), Information Systems Audit and Control Association (ISACA), Rancho Santa Margarita, California 92688-8741

Luther Martin (Chapter 37), Voltage Security, Palo Alto, California 94304

John McDonald (Chapter 33), EMC Corporation, Hopkinton, Massachusetts 01748

John McGowan (Chapter 33), EMC Corporation, Hopkinton, Massachusetts 01748

Peter F. Nicoletti (Chapter 42), Secure Information Systems, Terremark Worldwide, Miami, Florida

Kevin Noble, CISSP GSEC (Chapter 40), Director, Secure Information Services, Terremark Worldwide Inc., Miami, Florida 33132

Pramod Pandya (Chapters 10, 24), Department of Information Systems and Decision Sciences, California State University, Fullerton, California 92834

Harsh Kupwade Patil (Chapter 32), Department of Electrical Engineering, Southern Methodist University, Dallas, Texas 75205

Ken Perkins (Chapter 43), CIPP (Certified Information Privacy Professional), Sr. Systems Engineer, Blazent Incorporated, Denver, Colorado 80206

Daniel Ramsbrock (Chapter 8), Department of Computer Science, George Mason University, Fairfax, Virginia 22030

Chunming Rong (Chapters 11, 13), Professor, Ph.D., Chair of Computer Science Section, Faculty of Science and Technology, University of Stavanger, N-4036 Stavanger, Norway

Robert Rounsavall (Chapter 34), GCIA, GCWN**,** Director, SIS – SOC, Terremark Worldwide, Inc., Miami, Florida 33131

Mario Santana (Chapter 6), Terremark, Dallas, Texas 75226

Jean-Marc Seigneur (Chapters 17, 41), Department of Social and Economic Sciences, University of Geneva, Switzerland

Daniel S. Soper (Chapter 25), Information and Decision Sciences Department, Mihaylo College of Business and Economics, California State University, Fullerton, California 92834-6848

Terence Spies (Chapter 26), Voltage Security, Inc., Palo Alto, California 94304

William Stallings (Chapter 36), Independent consultant, Brewster Massachusetts 02631

Alex Tsow (Chapter 31), The MITRE Corporation, Mclean, Virginia 22102

Jesse Walker (Chapter 7), Intel Corporation, Hillboro, Oregon 97124

Patrick J. Walsh (Chapter 4), eSoft Inc., Broomfield, Colorado 80021

Xinyuan Wang (Chapter 8), Department of Computer Science, George Mason University, Fairfax, Virginia 22030

Michael A. West (Chapter 3), Independent Technical Writer, Martinez, California 94553

Dan Wing (Chapter 32), Security Technology Group, Cisco Systems, San Jose, California 95123

Joe Wright (Chapters 15, 30), Computer Bits, Inc., Chicago, Illinois 60602

George O.M. Yee (Chapter 29), Information Security Group, Institute for Information Technology, National Research Council Canada, Ottawa, Canada K1A 0R6