

HANDBOOK — OF — INFORMATION SECURITY

**Information Warfare; Social,
Legal, and International Issues;
and Security Foundations**

Volume 2

Hossein Bidgoli

Editor-in-Chief

California State University

Bakersfield, California



John Wiley & Sons, Inc.

HANDBOOK — OF — INFORMATION SECURITY

**Information Warfare; Social,
Legal, and International Issues;
and Security Foundations**

Volume 2

Hossein Bidgoli

Editor-in-Chief

California State University

Bakersfield, California



John Wiley & Sons, Inc.

This book is printed on acid-free paper. ☺

Copyright © 2006 by John Wiley & Sons, Inc. All rights reserved.

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

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 Section 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, Inc., 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600, or on the web at www.copyright.com. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at <http://www.wiley.com/go/permissions>.

Limit of Liability/Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. The publisher is not engaged in rendering professional services, and you should consult a professional where appropriate. Neither the publisher nor author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

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

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books. For more information about Wiley products, visit our web site at www.Wiley.com.

Library of Congress Cataloging-in-Publication Data:

The handbook of information security / edited by Hossein Bidgoli.
p. cm.

Includes bibliographical references and index.

ISBN-13: 978-0-471-64830-7, ISBN-10: 0-471-64830-2 (CLOTH VOL 1 : alk. paper)

ISBN-13: 978-0-471-64831-4, ISBN-10: 0-471-64831-0 (CLOTH VOL 2 : alk. paper)

ISBN-13: 978-0-471-64832-1, ISBN-10: 0-471-64832-9 (CLOTH VOL 3 : alk. paper)

ISBN-13: 978-0-471-22201-9, ISBN-10: 0-471-22201-1 (CLOTH SET : alk. paper)

1. Internet--Encyclopedias. I. Bidgoli, Hossein.

TK5105.875.I57I5466 2003

004.67'8'03--dc21

2002155552

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

To so many fine memories of my mother, Ashraf, my father,
Mohammad, and my brother, Mohsen, for their uncompromising
belief in the power of education.

About the Editor-in-Chief

Hossein Bidgoli, Ph.D., is professor of Management Information Systems at California State University. Dr. Bidgoli helped set up the first PC lab in the United States. He is the author of 43 textbooks, 27 manuals and over five dozen technical articles and papers on various aspects of computer applications, information systems and network security, e-commerce and decision support systems published and presented throughout the world. Dr. Bidgoli also serves as the editor-in-chief of *The*

Internet Encyclopedia and the *Encyclopedia of Information Systems*.

The *Encyclopedia of Information Systems* was the recipient of one of the *Library Journal's* Best Reference Sources for 2002 and *The Internet Encyclopedia* was recipient of one of the PSP Awards (Professional and Scholarly Publishing), 2004. Dr. Bidgoli was selected as the California State University, Bakersfield's 2001–2002 Professor of the Year.

Editorial Board

Dorothy E. Denning

Naval Postgraduate School

James E. Goldman

Purdue University

Sushil Jajodia

George Mason University

Ari Juels

RSA Laboratories

Raymond R. Panko

University of Hawaii, Manoa

Dennis M. Powers

Southern Oregon University

Pierangela Samarati

Università di Milano, Italy

E. Eugene Schultz

University of California-Berkeley Lab

Lee S. Sproull

New York University

Rebecca N. Wright

Stevens Institute of Technology

Avishai Wool

Tel Aviv University, Israel

Contents

Contributors	xv	Extranets: Applications, Development, Security, and Privacy	215
Preface	xxiii	<i>Stephen W. Thorpe</i>	
Guide to the Handbook of Information Security	xxvi	Business-to-Business Electronic Commerce	226
Reviewers List	911	<i>Julian J. Ray</i>	
Volume Index	919	Click-and-Brick Electronic Commerce	242
		<i>Charles Steinfield</i>	
		Mobile Commerce	254
		<i>Vijay Atluri</i>	
		E-Education and Information Privacy and Security	268
		<i>William K. Jackson</i>	
		Security in E-Learning	279
		<i>Edgar R. Weippl</i>	
		E-Government	294
		<i>Shannon Schelin and G. David Garson</i>	
		E-Government Security Issues and Measures	306
		<i>William C. Barker</i>	
		International Security Issues of E-Government	318
		<i>Karin Geiselhart</i>	
Volume I: Key Concepts, Infrastructure, Standards, and Protocols		Part 2: Infrastructure for the Internet, Computer Networks, and Secure Information Transfer	
Part 1: Key Concepts and Applications Related to Information Security		Conducted Communications Media	337
Internet Basics	3	<i>Thomas L. Pigg</i>	
<i>Hossein Bidgoli</i>		Routers and Switches	350
Digital Economy	15	<i>Hans-Peter Dommel</i>	
<i>Nirvikar Singh</i>		Radio Frequency and Wireless Communications Security	363
Online Retail Banking: Security Concerns, Breaches, and Controls	37	<i>Okechukwu Ugweje</i>	
<i>Kent Belasco and Siaw-Peng Wan</i>		Wireless Channels	387
Digital Libraries: Security and Preservation Considerations	49	<i>P. M. Shankar</i>	
<i>Cavan McCarthy</i>		Security in Circuit, Message, and Packet Switching	400
E-Mail and Instant Messaging	77	<i>Robert H. Greenfield and Daryle P. Niedermayer</i>	
<i>Bhagyavati</i>		Digital Communication	415
Internet Relay Chat	87	<i>Robert W. Heath Jr., William Bard, and Atul A. Salvekar</i>	
<i>Paul L. Witt</i>		Local Area Networks	428
Online Communities	97	<i>Wayne C. Summers</i>	
<i>Lee Sproull</i>		Wide Area and Metropolitan Area Networks	444
Groupware: Risks, Threats, and Vulnerabilities in the Internet Age	110	<i>Lynn A. DeNoia</i>	
<i>Pierre Balthazard and John Warren</i>		Home Area Networking	460
Search Engines: Security, Privacy, and Ethical Issues	126	<i>Sherali Zeadally, Priya Kubher, and Nadeem Ansari</i>	
<i>Raymond Wisman</i>			
Web Services	151		
<i>Akhil Sahai, Sven Graupner, and Wooyoung Kim</i>			
Electronic Commerce	164		
<i>Charles Steinfield</i>			
EDI Security	179		
<i>Matthew K. McGowan</i>			
Electronic Payment Systems	189		
<i>Indrajit Ray</i>			
Intranets: Principals, Privacy, and Security Considerations	205		
<i>William T. Schiano</i>			

Public Network Technologies and Security*Dale R. Thompson and Amy W. Apon***Client/Server Computing: Principles and Security Considerations***Daniel J. McFarland***Peer-to-Peer Security***Allan Friedman and L. Jean Camp***Security Middleware***Linda Volonino and Richard P. Volonino***Internet Architecture***Graham Knight***TCP/IP Suite***Prabhaker Mateti***Voice-over Internet Protocol (VoIP)***Roy Morris***Security and Web Quality of Service***Tarek F. Abdelzhaer and Chengdu Huang***Mobile Devices and Protocols***Min Song***Bluetooth Technology***Brent A. Miller***Wireless Local Area Networks***M. S. Obaidat, G. I. Papadimitriou,
and S. Obeidat***Security in Wireless Sensor Networks***Mohamed Eltoweissy, Stephan Olariu,
and Ashraf Wadaa***Cellular Networks***Jingyuan Zhang and Ivan Stojmenovic***Mobile IP***M. Farooque Mesiya***IP Multicast and Its Security***Emilia Rosti***TCP over Wireless Links***Mohsen Guizani and Anupama Raju***Air Interface Requirements for Mobile Data Services***Harald Haas***Wireless Internet: A Cellular Perspective***Abbas Jamalipour***Security of Satellite Networks***Michele Luglio and Antonio Saitto***Security of Broadband Access Networks***Peter L. Heinzmann***Ad Hoc Network Security***Pietro Michiardi and Refik Molva***Part 3: Standards and Protocols for Secure Information Transfer****Standards for Product Security Assessment** 809*István Zsolt Berta, Levente Buttyán, and István Vajda***Digital Certificates** 823*Albert Levi***Internet E-Mail Architecture** 836*Robert Gezelter***PKI (Public Key Infrastructure)** 852*Radia Perlman***S/MIME (Secure MIME)** 859*Steven J. Greenwald***PGP (Pretty Good Privacy)** 868*Stephen A. Weis***SMTP (Simple Mail Transfer Protocol)** 878*Vladimir V. Riabov***Internet Security Standards** 901*Raymond R. Panko***Kerberos** 920*William Stallings***IPsec: AH and ESP** 932*A. Meddeb, N. Boudriga, and M. S. Obaidat***IPsec: IKE (Internet Key Exchange)** 944*Charlie Kaufman***Secure Sockets Layer (SSL)** 952*Robert J. Boncella***PKCS (Public Key Cryptography Standards)** 966*Yongge Wang***Public Key Standards: Secure Shell** 979*Xukai Zou***Security and the Wireless Application Protocol** 995*Lillian N. Cassel and Cynthia Pandolfo***Wireless Network Standards and Protocol (802.11)** 1007*Prashant Krishnamurthy***P3P (Platform for Privacy Preferences Project)** 1023*Lorrie Faith Cranor***Volume II: Information Warfare; Social, Legal, and International Issues; and Security Foundations****Part 1: Information Warfare****Cybercrime and the U.S. Criminal Justice System** 3*Susan W. Brenner***Cyberterrorism and Information Security** 16*Charles Jaeger***Online Stalking** 40*David J. Loundy*

	CONTENTS	xi
Electronic Attacks	47	Trademark Law and the Internet 381
<i>Thomas M. Chen, Jimi Thompson, and Matthew C. Elder</i>		<i>Ray Everett-Church</i>
Wireless Information Warfare	59	Online Contracts 392
<i>Randall K. Nichols</i>		<i>G. E. Evans</i>
Computer Network Operations (CNO)	89	Electronic Speech 408
<i>Andrew Blyth</i>		<i>Seth Finkelstein</i>
Electronic Protection	101	Software Piracy 418
<i>Neil C. Rowe</i>		<i>Robert K. Moniot</i>
Information Assurance	110	Internet Gambling 428
<i>Peng Liu, Meng Yu, and Jiwu Jing</i>		<i>Susanna Frederick Fischer</i>
Part 2: Social and Legal Issues		The Digital Millennium Copyright Act 446
The Legal Implications of Information Security:		<i>Seth Finkelstein</i>
Regulatory Compliance and Liability	127	Digital Courts, the Law and Evidence 459
<i>Blaze D. Waleski</i>		<i>Robert Slade</i>
Hackers, Crackers, and Computer Criminals	154	
<i>David Dittrich and Kenneth Einar Himma</i>		Part 3: Foundations of Information, Computer and Network Security
Hacktivism	172	Encryption Basics 469
<i>Paul A. Taylor and Jan L. Harris</i>		<i>Ari Juels</i>
Corporate Spying: The Legal Aspects	183	Symmetric Key Encryption 479
<i>William A. Zucker and Scott Nathan</i>		<i>Jonathan Katz</i>
Law Enforcement and Computer Security Threats and Measures	200	Data Encryption Standard (DES) 491
<i>Mathieu Deflem and J. Eagle Shutt</i>		<i>Mike Speciner</i>
Combating the Cybercrime Threat: Developments in Global Law Enforcement	210	The Advanced Encryption Standard 498
<i>Roderic Broadhurst</i>		<i>Duncan A. Buell</i>
Digital Identity	223	Hashes and Message Digests 510
<i>Drummond Reed and Jerry Kindall</i>		<i>Magnus Daum and Hans Dobbertin</i>
Digital Divide	238	Number Theory for Information Security 532
<i>Jaime J. Davila</i>		<i>Duncan A. Buell</i>
Legal, Social, and Ethical Issues of the Internet	247	Public Key Algorithms 548
<i>Kenneth Einar Himma</i>		<i>Bradley S. Rubin</i>
Anonymity and Identity on the Internet	265	Elliptic Curve Cryptography 558
<i>Jonathan Wallace</i>		<i>N. P. Smart</i>
Spam and the Legal Counter Attacks	275	IBE (Identity-Based Encryption) 575
<i>Charles Jaeger</i>		<i>Craig Gentry</i>
Cyberlaw: The Major Areas, Development, and Information Security Aspects	297	Cryptographic Protocols 593
<i>Dennis M. Powers</i>		<i>Markus Jakobsson</i>
Global Aspects of Cyberlaw	319	Quantum Cryptography 606
<i>Julia Alpert Gladstone</i>		<i>G. Massimo Palma</i>
Privacy Law and the Internet	336	Key Lengths 617
<i>Ray Everett-Church</i>		<i>Arjen K. Lenstra</i>
Internet Censorship	349	Key Management 636
<i>Richard A. Spinello</i>		<i>Xukai Zou and Amandeep Thukral</i>
Copyright Law	357	Secure Electronic Voting Protocols 647
<i>Randy Canis</i>		<i>Helger Lipmaa</i>
Patent Law	369	Digital Evidence 658
<i>Gerald Bluhm</i>		<i>Robin C. Stuart</i>

Digital Watermarking and Steganography <i>M. A. Suhail, B. Sadoun, and M. S. Obaidat</i>	664	Hacking Techniques in Wireless Networks <i>Prabhaker Mateti</i>	83
Law Enforcement and Digital Evidence <i>J. Philip Craiger, Jeff Swauger, and Mark Pollitt</i>	679	Computer Viruses and Worms <i>Robert Slade</i>	94
Forensic Computing <i>Mohamed Hamdi, Noureddine Boudriga, and M. S. Obaidat</i>	702	Trojan Horse Programs <i>Adam L. Young</i>	107
Computer Forensics Procedures and Methods <i>J. Philip Craiger</i>	715	Hoax Viruses and Virus Alerts <i>Robert Slade</i>	119
Computer Forensics—Computer Media Reviews in Classified Government Agencies <i>Michael R. Anderson</i>	750	Hostile Java Applets <i>David Evans</i>	126
Forensic Analysis of UNIX Systems <i>Dario V. Forte</i>	763	Spyware <i>Tom S. Chan</i>	136
Forensic Analysis of Windows Systems <i>Steve J. Chapin and Chester J. Maciag</i>	781	Mobile Code and Security <i>Song Fu and Cheng-Zhong Xu</i>	146
Operating System Security <i>William Stallings</i>	796	Wireless Threats and Attacks <i>Robert J. Boncella</i>	165
UNIX Security <i>Mark Shacklette</i>	806	WEP Security <i>Nikita Borisov</i>	176
Linux Security <i>A. Justin Wilder</i>	822	Bluetooth Security <i>Susanne Wetzel</i>	184
OpenVMS Security <i>Robert Gezelter</i>	853	Cracking WEP <i>Pascal Meunier</i>	198
Windows 2000 Security <i>E. Eugene Schultz</i>	870	Denial of Service Attacks <i>E. Eugene Schultz</i>	207
Software Development and Quality Assurance <i>Pascal Meunier</i>	885	Network Attacks <i>Edward Amoroso</i>	220
The Common Criteria <i>J. McDermott</i>	897	Fault Attacks <i>Hamid Choukri and Michael Tunstall</i>	230
		Side-Channel Attacks <i>Pankaj Rohatgi</i>	241

Volume III: Threats, Vulnerabilities, Prevention, Detection, and Management

Part 1: Threats and Vulnerabilities to Information and Computing Infrastructures

Internal Security Threats <i>Marcus K. Rogers</i>	3
Physical Security Threats <i>Mark Michael</i>	18
Fixed-Line Telephone System Vulnerabilities <i>Mak Ming Tak, Xu Yan, and Zenith Y. W. Law</i>	30
E-Mail Threats and Vulnerabilities <i>David Harley</i>	40
E-Commerce Vulnerabilities <i>Sviatoslav Braynov</i>	57
Hacking Techniques in Wired Networks <i>Qijun Gu, Peng Liu, and Chao-Hsien Chu</i>	70

Part 2: Prevention: Keeping the Hackers and Crackers at Bay

Physical Security Measures <i>Mark Michael</i>	263
RFID and Security <i>Stephen A. Weis</i>	289
Cryptographic Privacy Protection Techniques <i>Markus Jakobsson</i>	300
Cryptographic Hardware Security Modules <i>Nicko van Someren</i>	311
Smart Card Security <i>Michael Tunstall, Sebastien Petit, and Stephanie Porte</i>	326
Client-Side Security <i>Charles Border</i>	342
Server-Side Security <i>Slim Rekhis, Noureddine Boudriga, and M. S. Obaidat</i>	355
Protecting Web Sites <i>Dawn Alexander and April Giles</i>	370

Database Security <i>Michael Gertz and Arnon Rosenthal</i>	380	Part 3: Detection, Recovery, Management, and Policy Considerations	
Medical Records Security <i>Normand M. Martel</i>	395	Intrusion Detection Systems Basics <i>Peng Ning and Sushil Jajodia</i>	685
Access Control: Principles and Solutions <i>S. De Capitani di Vimercati, S. Paraboschi, and Pierangela Samarati</i>	406	Host-Based Intrusion Detection System <i>Giovanni Vigna and Christopher Kruegel</i>	701
Password Authentication <i>Jeremy L. Rasmussen</i>	424	Network-Based Intrusion Detection Systems <i>Marco Cremonini</i>	713
Computer and Network Authentication <i>Patrick McDaniel</i>	439	The Use of Agent Technology for Intrusion Detection <i>Dipankar Dasgupta</i>	730
Antivirus Technology <i>Matthew Schmid</i>	450	Contingency Planning Management <i>Marco Cremonini and Pierangela Samarati</i>	744
Biometric Basics and Biometric Authentication <i>James L. Wayman</i>	459	Computer Security Incident Response Teams (CSIRTs) <i>Raymond R. Panko</i>	760
Issues and Concerns in Biometric IT Security <i>Philip Statham</i>	471	Implementing a Security Awareness Program <i>K. Rudolph</i>	766
Firewall Basics <i>James E. Goldman</i>	502	Risk Management for IT Security <i>Rick Kazman, Daniel N. Port, and David Klappholz</i>	786
Firewall Architectures <i>James E. Goldman</i>	515	Security Insurance and Best Practices <i>Selahattin Kuru, Onur Ihsan Arsun, and Mustafa Yildiz</i>	811
Packet Filtering and Stateful Firewalls <i>Avishai Wool</i>	526	Auditing Information Systems Security <i>S. Rao Vallabhaneni</i>	829
Proxy Firewalls <i>John D. McLaren</i>	537	Evidence Collection and Analysis Tools <i>Christopher L. T. Brown</i>	840
E-Commerce Safeguards <i>Mark S. Merkow</i>	552	Information Leakage: Detection and Countermeasures <i>Phil Venables</i>	853
Digital Signatures and Electronic Signatures <i>Raymond R. Panko</i>	562	Digital Rights Management <i>Renato Iannella</i>	865
E-Mail Security <i>Jon Callas</i>	571	Web Hosting <i>Doug Kaye</i>	879
Security for ATM Networks <i>Thomas D. Tarman</i>	584	Managing a Network Environment <i>Jian Ren</i>	893
VPN Basics <i>G. I. Papadimitriou, M. S. Obaidat, C. Papazoglou, and A. S. Pomportsis</i>	596	E-Mail and Internet Use Policies <i>Nancy J. King</i>	908
VPN Architecture <i>Stan Kurkovsky</i>	612	Forward Security Adaptive Cryptography: Time Evolution <i>Gene Itkis</i>	927
IP-Based VPN <i>David E. McDysan</i>	624	Security Policy Guidelines <i>Mohamed Hamdi, Nouredine Boudriga, and M. S. Obaidat</i>	945
Identity Management <i>John Linn</i>	636	Asset-Security Goals Continuum: A Process for Security <i>Margarita Maria Lenk</i>	960
The Use of Deception Techniques: Honeypots and Decoys <i>Fred Cohen</i>	646	Multilevel Security <i>Richard E. Smith</i>	972
Active Response to Computer Intrusions <i>David Dittrich and Kenneth Einar Himma</i>	664		

Multilevel Security Models <i>Mark Stamp and Ali Hushyar</i>	987	Security Policy Enforcement <i>Cynthia E. Irvine</i>	1026
Security Architectures <i>Nicole Graf and Dominic Kneeshaw</i>	998	Guidelines for a Comprehensive Security System <i>Hossein Bidgoli</i>	1041
Quality of Security Service: Adaptive Security <i>Timothy E. Levin, Cynthia E. Irvine, and Evdoxia Spyropoulou</i>	1016		

Contributors

Tarek F. Abdelzhaer

University of Virginia
Security and Web Quality of Service

Dawn Alexander

University of Maryland
Protecting Web Sites

Edward Amoroso

AT&T Laboratories
Network Attacks

Michael R. Anderson

SCERC
*Computer Forensics—Computer Media Reviews
in Classified Government Agencies*

Nadeem Ansari

Wayne State University
Home Area Networking

Amy W. Apon

University of Arkansas
Public Network Technologies and Security

Onur Ihsan Arsun

Isik University, Turkey
Security Insurance and Best Practices

Vijay Atluri

Rutgers University
Mobile Commerce

Pierre Balthazard

Arizona State University
*Groupware: Risks, Threats, and Vulnerabilities
in the Internet Age*

William Bard

The University of Texas, Austin
Digital Communication

William C. Barker

National Institute of Standards and Technology
E-Government Security Issues and Measures

Kent Belasco

First Midwest Bank
*Online Retail Banking: Security Concerns, Breaches,
and Controls*

István Zsolt Berta

Budapest University of Technology and Economics,
Hungary
Standards for Product Security Assessment

Bhagyavati

Columbus State University
E-Mail and Instant Messaging

Hossein Bidgoli

California State University, Bakersfield
*Guidelines for a Comprehensive Security System
Internet Basics*

Gerald Bluhm

Tyco Fire & Security
Patent Law

Andrew Blyth

University of Glamorgan, Pontypridd, UK
Computer Network Operations (CNO)

Robert J. Boncella

Washburn University
*Secure Sockets Layer (SSL)
Wireless Threats and Attacks*

Charles Border

Rochester Institute of Technology
Client-Side Security

Nikita Borisov

University of California, Berkeley
WEP Security

Noureddine Boudriga

National Digital Certification Agency and University
of Carthage, Tunisia
*Forensic Computing
IPsec: AH and ESP
Security Policy Guidelines
Server-Side Security*

Sviatoslav Braynov

University of Illinois, Springfield
E-Commerce Vulnerabilities

Susan W. Brenner

University of Dayton School of Law
Cybercrime and the U.S. Criminal Justice System

Roderic Broadhurst

Queensland University of Technology
*Combating the Cybercrime Threat: Developments
in Global Law Enforcement*

Christopher L. T. Brown

Technology Pathways
Evidence Collection and Analysis Tools

Duncan A. Buell

University of South Carolina
*Number Theory for Information Security
The Advanced Encryption Standard*

Levente Buttyán

Budapest University of Technology and Economics,
Hungary
Standards for Product Security Assessment

Jon Callas

PGP Corporation
E-Mail Security

L. Jean Camp

Harvard University
Peer-to-Peer Security

Randy Canis

Greensfelder, Hemker & Gale, P.C.
Copyright Law

Lillian N. Cassel

Villanova University
Security and the Wireless Application Protocol

Tom S. Chan

Southern New Hampshire University
Spyware

Steve J. Chapin

Syracuse University
Forensic Analysis of Windows Systems

Thomas M. Chen

Southern Methodist University
Electronic Attacks

Hamid Choukri

Gemplus & University of Bordeaux, France
Fault Attacks

Chao-Hsien Chu

Pennsylvania State University
Hacking Techniques in Wired Networks

Fred Cohen

University of New Haven
The Use of Deception Techniques: Honeypots and Decoys

J. Philip Craiger

University of Central Florida
Computer Forensics Procedures and Methods
Law Enforcement and Digital Evidence

Lorrie Faith Cranor

Carnegie Mellon University
P3P (Platform for Privacy Preferences Project)

Marco Cremonini

University of Milan, Italy
Contingency Planning Management
Network-Based Intrusion Detection Systems

Dipankar Dasgupta

University of Memphis
The Use of Agent Technology for Intrusion Detection

Magnus Daum

Ruhr University Bochum, Germany
Hashes and Message Digests

Jaime J. Davila

Hampshire College
Digital Divide

S. De Capitani di Vimercati

Università di Milano, Italy
Access Control: Principles And Solutions

Mathieu Deflem

University of South Carolina
Law Enforcement and Computer Security
Threats and Measures

Lynn A. DeNoia

Rensselaer Polytechnic Institute
Wide Area and Metropolitan Area Networks

David Dittrich

University of Washington
Active Response to Computer Intrusions
Hackers, Crackers, and Computer Criminals

Hans Dobbertin

Ruhr University Bochum, Germany
Hashes and Message Digests

Hans-Peter Dommel

Santa Clara University
Routers and Switches

Matthew C. Elder

Symantec Corporation
Electronic Attacks

Mohamed Eltoweissy

Virginia Tech
Security in Wireless Sensor Networks

David Evans

University of Virginia
Hostile Java Applets

G. E. Evans

Queen Mary Intellectual Property
Research Institute, UK
Online Contracts

Ray Everett-Church

PrivacyClue LLC
Privacy Law and the Internet
Trademark Law and the Internet

Seth Finkelstein

SethF.com
Electronic Speech
The Digital Millennium Copyright Act

Susanna Frederick Fischer

Columbus School of Law, The Catholic University
of America
Internet Gambling

Dario V. Forte

University of Milan, Crema, Italy
Forensic Analysis of UNIX Systems

Allan Friedman

Harvard University
Peer-to-Peer Security

Song Fu

Wayne State University
Mobile Code and Security

G. David Garson

North Carolina State University
E-Government

Karin Geiselhart

University of Canberra and Australian National
University, Canberra, Australia
International Security Issues of
E-Government

Craig Gentry

DoCoMo USA Labs
IBE (Identity-Based Encryption)

Michael Gertz

University of California, Davis
Database Security

Robert Gezelter

Software Consultant
Internet E-Mail Architecture
OpenVMS Security

April Giles

Johns Hopkins University
Protecting Web Sites

Julia Alpert Gladstone

Bryant University
Global Aspects of Cyberlaw

James E. Goldman

Purdue University
Firewall Architectures
Firewall Basics

Nicole Graf

University of Cooperative Education,
Germany
Security Architectures

Sven Graupner

Hewlett-Packard Laboratories
Web Services

Robert H. Greenfield

Computer Consulting
Security in Circuit, Message, and Packet Switching

Steven J. Greenwald

Independent Information Security Consultant
S/MIME (Secure MIME)

Qijun Gu

Pennsylvania State University
Hacking Techniques in Wired Networks

Mohsen Guizani

Western Michigan University
TCP over Wireless Links

Harald Haas

International University Bremen (IUB),
Germany
*Air Interface Requirements for Mobile Data
Services*

Mohamed Hamdi

National Digital Certification Agency, Tunisia
*Forensic Computing
Security Policy Guidelines*

David Harley

NHS Connecting for Health, UK
E-Mail Threats and Vulnerabilities

Jan Ll. Harris

University of Salford, UK
Hacktivism

Robert W. Heath Jr.

The University of Texas, Austin
Digital Communication

Peter L. Heinzmann

University of Applied Sciences, Eastern Switzerland
Security of Broadband Access Networks

Kenneth Einar Himma

Seattle Pacific University
*Active Response to Computer Intrusions
Legal, Social, and Ethical Issues of the Internet
Hackers, Crackers, and Computer Criminals*

Chengdu Huang

University of Virginia
Security and Web Quality of Service

Ali Hushyar

San Jose State University
Multilevel Security Models

Renato Iannella

National ICT, Australia (NICTA)
Digital Rights Management

Cynthia E. Irvine

Naval Postgraduate School
*Quality of Security Service: Adaptive Security
Security Policy Enforcement*

Gene Itkis

Boston University
*Forward Security Adaptive Cryptography: Time
Evolution*

William K. Jackson

Southern Oregon University
E-Education and Information Privacy and Security

Charles Jaeger

Southern Oregon University
*Cyberterrorism and Information Security
Spam and the Legal Counter Attacks*

Sushil Jajodia

George Mason University
Intrusion Detection Systems Basics

Markus Jakobsson

Indiana University, Bloomington
*Cryptographic Privacy Protection Techniques
Cryptographic Protocols*

Abbas Jamalipour

University of Sydney, Australia
Wireless Internet: A Cellular Perspective

Jiwu Jing

Chinese Academy of Sciences, Beijing, China
Information Assurance

Ari Juels

RSA Laboratories
Encryption Basics

Jonathan Katz

University of Maryland
Symmetric Key Encryption

Charlie Kaufman

Microsoft Corporation
IPsec: IKE (Internet Key Exchange)

Doug Kaye

IT Conversations
Web Hosting

Rick Kazman

University of Hawaii, Manoa
Risk Management for IT Security

Wooyoung Kim

University of Illinois, Urbana-Champaign
Web Services

Nancy J. King

Oregon State University
E-Mail and Internet Use Policies

Jerry Kindall

Epok, Inc.
Digital Identity

Dominic Kneeshaw

Independent Consultant, Germany
Security Architectures

David Klappholz

Stevens Institute of Technology
Risk Management for IT Security

Graham Knight

University College, London, UK
Internet Architecture

Prashant Krishnamurthy

University of Pittsburgh
Wireless Network Standards and Protocol (802.11)

Christopher Kruegel

Technical University, Vienna, Austria
Host-Based Intrusion Detection

Priya Kubher

Wayne State University
Home Area Networking

Stan Kurkovsky

Central Connecticut State University
VPN Architecture

Selahattin Kuru

Isik University, Turkey
Security Insurance and Best Practices

Zenith Y. W. Law

JustSolve Consulting, Hong Kong
Fixed-Line Telephone System Vulnerabilities

Margarita Maria Lenk

Colorado State University
Asset-Security Goals Continuum: A Process for Security

Arjen K. Lenstra

Lucent Technologies Bell Laboratories
 and Technische Universiteit Eindhoven
Key Lengths

Albert Levi

Sabancı University, Turkey
Digital Certificates

Timothy E. Levin

Naval Postgraduate School
Quality of Security Service: Adaptive Security

John Linn

RSA Laboratories
Identity Management

Helger Lipmaa

Cybernetica AS and University of Tartu, Estonia
Secure Electronic Voting Protocols

Peng Liu

Pennsylvania State University
Hacking Techniques in Wired Networks
Information Assurance

David J. Loundy

Devon Bank University College of Commerce
Online Stalking

Michele Luglio

University of Rome Tor Vergata, Italy
Security of Satellite Networks

Chester J. Maciag

Air Force Research Laboratory
Forensic Analysis of Windows Systems

Normand M. Martel

Medical Technology Research Corp.
Medical Records Security

Prabhaker Mateti

Wright State University
Hacking Techniques in Wireless Networks
TCP/IP Suite

Cavan McCarthy

Louisiana State University
Digital Libraries: Security and Preservation
Considerations

Patrick McDaniel

Pennsylvania State University
Computer and Network Authentication

J. McDermott

Center for High Assurance Computer System, Naval
 Research Laboratory
The Common Criteria

David E. McDysan

MCI Corporation
IP-Based VPN

Daniel J. McFarland

Rowan University
Client/Server Computing: Principles and Security
Considerations

Matthew K. McGowan

Bradley University
EDI Security

John D. McLaren

Murray State University
Proxy Firewalls

A. Meddeb

National Digital Certification Agency and University
 of Carthage, Tunisia
IPsec: AH and ESP

Mark S. Merkow

University of Phoenix Online
E-Commerce Safeguards

M. Farooque Mesiya

Rensselaer Polytechnic Institute
Mobile IP

Pascal Meunier

Purdue University
Cracking WEP
Software Development and Quality Assurance

Mark Michael

Research in Motion Ltd., Canada
Physical Security Measures
Physical Security Threats

Pietro Michiardi

Institut Eurecom, France
Ad Hoc Network Security

Brent A. Miller

IBM Corporation
Bluetooth Technology

Refik Molva

Institut Eurecom, France
Ad Hoc Network Security

Robert K. Moniot

Fordham University
Software Piracy

Roy Morris

Capitol College
Voice-over Internet Protocol (VoIP)

Scott Nathan

Independent Consultant
Corporate Spying: The Legal Aspects

Randall K. Nichols

The George Washington University & University of
 Maryland University College
Wireless Information Warfare

Daryle P. Niedermayer

CGI Group Inc.
Security in Circuit, Message, and Packet Switching

Peng Ning

North Carolina State University
Intrusion Detection Systems Basics

M. S. Obaidat

Monmouth University
Digital Watermarking and Steganography
Forensic Computing
IPsec: AH and ESP
Security Policy Guidelines

Server-Side Security
Wireless Local Area Networks
VPN Basics

S. Obeidat

Arizona State University
Wireless Local Area Networks

Stephan Olariu

Old Dominion University
Security in Wireless Sensor Networks

G. Massimo Palma

Università degli Studi di Milano, Italy
Quantum Cryptography

Cynthia Pandolfo

Villanova University
Security and the Wireless Application Protocol

Raymond R. Panko

University of Hawaii, Manoa
Computer Security Incident Response Teams (CSIRTs)
Digital Signatures and Electronic Signatures
Internet Security Standards

G. I. Papadimitriou

Aristotle University, Greece
VPN Basics
Wireless Local Area Networks

C. Papazoglou

Aristotle University, Greece
VPN Basics

S. Paraboschi

Università di Bergamo, Italy
Access Control: Principles and Solutions

Radia Perlman

Sun Microsystems Laboratories
PKI (Public Key Infrastructure)

Sebastien Petit

Gemplus, France
Smart Card Security

Thomas L. Pigg

Jackson State Community College
Conducted Communications Media

Mark Pollitt

DigitalEvidencePro
Law Enforcement and Digital Evidence

A. S. Pomportsis

Aristotle University, Greece
VPN Basics

Daniel N. Port

University of Hawaii, Manoa
Risk Management for IT Security

Stephanie Porte

Gemplus, France
Smart Card Security

Dennis M. Powers

Southern Oregon University
Cyberlaw: The Major Areas, Development, and Information Security Aspects

Anupama Raju

Western Michigan University
TCP over Wireless Links

Jeremy L. Rasmussen

Sypris Electronics, LLC
Password Authentication

Indrajit Ray

Colorado State University
Electronic Payment Systems

Julian J. Ray

University of Redlands
Business-to-Business Electronic Commerce

Drummond Reed

OneName Corporation
Digital Identity

Slim Rekhis

National Digital Certification Agency and University of Carthage, Tunisia
Server-Side Security

Jian Ren

Michigan State University, East Lansing
Managing A Network Environment

Vladimir V. Riabov

Rivier College
SMTP (Simple Mail Transfer Protocol)

Marcus K. Rogers

Purdue University
Internal Security Threats

Pankaj Rohatgi

IBM T. J. Watson Research Center
Side-Channel Attacks

Arnon Rosenthal

The MITRE Corporation
Database Security

Emilia Rosti

Università degli Studi di Milano, Italy
IP Multicast and Its Security

Neil C. Rowe

U.S. Naval Postgraduate School
Electronic Protection

Bradley S. Rubin

University of St. Thomas
Public Key Algorithms

K. Rudolph

Native Intelligence, Inc.
Implementing a Security Awareness Program

B. Sadoun

Al-Balqa' Applied University, Jordan
Digital Watermarking and Steganography

Akhil Sahai

Hewlett-Packard Laboratories
Web Services

Antonio Saitto

Telespazio, Italy
Security of Satellite Networks

Atul A. Salvekar

Intel Corporation
Digital Communication

Pierangela Samarati

Università di Milano, Italy
Access Control: Principles and Solutions
Contingency Planning Management

Shannon Schelin

The University of North Carolina, Chapel Hill
E-Government

William T. Schiano

Bentley College
Intranets: Principals, Privacy, and Security Considerations

Matthew Schmid

Cigital, Inc.
Antivirus Technology

E. Eugene Schultz

University of California–Berkeley Lab
Windows 2000 Security
Denial of Service Attacks

Mark Shacklette

The University of Chicago
UNIX Security

P. M. Shankar

Drexel University
Wireless Channels

J. Eagle Shutt

University of South Carolina
Law Enforcement and Computer Security
Threats and Measures

Nirvikar Singh

University of California, Santa Cruz
Digital Economy

Robert Slade

Vancouver Institute for Research into User Security, Canada
Computer Viruses and Worms
Digital Courts, the Law and Evidence
Hoax Viruses and Virus Alerts

Nigel Smart

University of Bristol, UK
Elliptic Curve Cryptography

Richard E. Smith

University of St. Thomas
Multilevel Security

Min Song

Old Dominion University
Mobile Devices and Protocols

Mike Speciner

Independent Consultant
Data Encryption Standard (DES)

Richard A. Spinello

Boston College
Internet Censorship

Lee Sproull

New York University
Online Communities

Evdoxia Spyropoulou

Technical Vocational Educational School of Computer Science of Halandri, Greece
Quality of Security Service: Adaptive Security

William Stallings

Independent Consultant
Kerberos
Operating System Security

Mark Stamp

San Jose State University
Multilevel Security Models

Philip Statham

CESG, Cheltenham, Gloucestershire, UK
Issues and Concerns in Biometric IT Security

Charles Steinfield

Michigan State University
Click-and-Brick Electronic Commerce
Electronic Commerce

Ivan Stojmenovic

University of Ottawa, Canada
Cellular Networks

Robin C. Stuart

Digital Investigations Consultant
Digital Evidence

M. A. Suhail

University of Bradford, UK
Digital Watermarking and Steganography

Wayne C. Summers

Columbus State University
Local Area Networks

Jeff Swauger

University of Central Florida
Law Enforcement and Digital Evidence

Mak Ming Tak

Hong Kong University of Science and Technology, Hong Kong
Fixed-Line Telephone System Vulnerabilities

Thomas D. Tarman

Sandia National Laboratories
Security for ATM Networks

Paul A. Taylor

University of Leeds, UK
Hacktivism

Dale R. Thompson

University of Arkansas
Public Network Technologies and Security

Jimi Thompson

Southern Methodist University
Electronic Attacks

Stephen W. Thorpe

Neumann College
Extranets: Applications, Development, Security, and Privacy

Amandeep Thukral

Purdue University
Key Management

Michael Tunstall

Gemplus & Royal Holloway University, France
Fault Attacks
Smart Card Security

Okechukwu Ugweje

The University of Akron
Radio Frequency and Wireless Communications Security

István Vajda

Budapest University of Technology and Economics, Hungary
Standards for Product Security Assessment

S. Rao Vallabhaneni

SRV Professional Publications
Auditing Information Systems Security

Nicko van Someren

nCipher Plc., UK
Cryptographic Hardware Security Modules

Phil Venables

Institute of Electrical and Electronics Engineers
Information Leakage: Detection and Countermeasures

Giovanni Vigna

Reliable Software Group
Host-Based Intrusion Detection Systems

Linda Volonino

Canisius College
Security Middleware

Richard P. Volonino

Canisius College
Security Middleware

Ashraf Wadaa

Old Dominion University
Security in Wireless Sensor Networks

Blaze D. Waleski

Fulbright & Jaworski LLP
The Legal Implications of Information Security: Regulatory Compliance and Liability

Jonathan Wallace

DeCoMo USA Labs
Anonymity and Identity on the Internet

Siaw-Peng Wan

Elmhurst College
Online Retail Banking: Security Concerns, Breaches, and Controls

Yongge Wang

University of North Carolina, Charlotte
PKCS (Public-Key Cryptography Standards)

John Warren

University of Texas, San Antonio
Groupware: Risks, Threats, and Vulnerabilities in the Internet Age

James L. Wayman

San Jose State University
Biometric Basics and Biometric Authentication

Edgar R. Weippl

Vienna University of Technology, Austria
Security in E-Learning

Stephen A. Weis

MIT Computer Science and Artificial Intelligence Laboratory
PGP (Pretty Good Privacy)
RFID and Security

Susanne Wetzel

Stevens Institute of Technology
Bluetooth Security

A. Justin Wilder

Telos Corporation
Linux Security

Raymond Wisman

Indiana University Southeast
Search Engines: Security, Privacy, and Ethical Issues

Paul L. Witt

Texas Christian University
Internet Relay Chat

Avishai Wool

Tel Aviv University, Israel
Packet Filtering and Stateful Firewalls

Cheng-Zhong Xu

Wayne State University
Mobile Code and Security

Xu Yan

Hong Kong University of Science and Technology, Hong Kong
Fixed-Line Telephone System Vulnerabilities

Mustafa Yildiz

Isik University, Turkey
Security Insurance and Best Practices

Adam L. Young

Cigital, Inc.
Trojan Horse Programs

Meng Yu

Monmouth University
Information Assurance

Sherali Zeadally

Wayne State University
Home Area Networking

Jingyuan Zhang

University of Alabama
Cellular Networks

Xukai Zou

Purdue University
Key Management
Public Key Standards: Secure Shell

William A. Zucker

Gadsby Hannah LLP
Corporate Spying: The Legal Aspects

Preface

The Handbook of Information Security is the first comprehensive examination of the core topics in the security field. *The Handbook of Information Security*, a 3-volume reference work with 207 chapters and 3300+ pages, is a comprehensive coverage of information, computer, and network security.

The primary audience is the libraries of 2-year and 4-year colleges and universities with computer science, MIS, CIS, IT, IS, data processing, and business departments; public, private, and corporate libraries throughout the world; and reference material for educators and practitioners in the information and computer security fields.

The secondary audience is a variety of professionals and a diverse group of academic and professional course instructors.

Among the industries expected to become increasingly dependent upon information and computer security and active in understanding the many issues surrounding this important and fast-growing field are: government, military, education, library, health, medical, law enforcement, accounting, legal, justice, manufacturing, financial services, insurance, communications, transportation, aerospace, energy, biotechnology, retail, and utility.

Each volume incorporates state-of-the-art, core information, on computer security topics, practical applications and coverage of the emerging issues in the information security field.

This definitive 3-volume handbook offers coverage of both established and cutting-edge theories and developments in information, computer, and network security.

This handbook contains chapters by global academic and industry experts. This handbook offers the following features:

- 1) Each chapter follows a format including title and author, outline, introduction, body, conclusion, glossary, cross-references, and references. This format allows the reader to pick and choose various sections of a chapter. It also creates consistency throughout the entire series.
- 2) The handbook has been written by more than 240 experts and reviewed by more than 1,000 academics and practitioners from around the world. These experts have created a definitive compendium of both established and cutting-edge theories and applications.
- 3) Each chapter has been rigorously peer-reviewed. This review process assures accuracy and completeness.
- 4) Each chapter provides extensive online and off-line references for additional readings, which will enable the reader to learn more on topics of special interest.
- 5) The handbook contains more than 1,000 illustrations and tables that highlight complex topics for further understanding.
- 6) Each chapter provides extensive cross-references, leading the reader to other chapters related to a particular topic.
- 7) The handbook contains more than 2,700 glossary items. Many new terms and buzzwords are included to provide a better understanding of concepts and applications.
- 8) The handbook contains a complete and comprehensive table of contents and index.
- 9) The series emphasizes both technical as well as managerial, social, legal, and international issues in the field. This approach provides researchers, educators, students, and practitioners with a balanced perspective and background information that will be helpful when dealing with problems related to security issues and measures and the design of a sound security system.
- 10) The series has been developed based on the current core course materials in several leading universities around the world and current practices in leading computer, security, and networking corporations.

We chose to concentrate on fields and supporting technologies that have widespread applications in the academic and business worlds. To develop this handbook, we carefully reviewed current academic research in the security field from leading universities and research institutions around the world.

Computer and network security, information security and privacy, management information systems, network design and management, computer information systems (CIS), decision support systems (DSS), and electronic commerce curriculums, recommended by the Association of Information Technology Professionals (AITP) and the Association for Computing Machinery (ACM) were carefully investigated. We also researched the current practices in the security field carried out by leading security and IT corporations. Our research helped us define the boundaries and contents of this project.

TOPIC CATEGORIES

Based on our research, we identified nine major topic categories for the handbook.

- Key Concepts and Applications Related to Information Security
- Infrastructure for the Internet, Computer Networks, and Secure Information Transfer
- Standards and Protocols for Secure Information Transfer
- Information Warfare
- Social, Legal, and International Issues

- Foundations of Information, Computer, and Network Security
- Threats and Vulnerabilities to Information and Computing Infrastructures
- Prevention: Keeping the Hackers and Crackers at Bay
- Detection, Recovery, Management, and Policy Considerations

Although these topics are related, each addresses a specific concern within information security. The chapters in each category are also interrelated and complementary, enabling readers to compare, contrast, and draw conclusions that might not otherwise be possible.

Though the entries have been arranged logically, the light they shed knows no bounds. The handbook provides unmatched coverage of fundamental topics and issues for successful design and implementation of a sound security program. Its chapters can serve as material for a wide spectrum of courses such as:

Information and Network Security
 Information Privacy
 Social Engineering
 Secure Financial Transactions
 Information Warfare
 Infrastructure for Secure Information Transfer
 Standards and Protocols for Secure Information Transfer
 Network Design and Management
 Client/Server Computing
 E-commerce

Successful design and implementation of a sound security program requires a thorough knowledge of several technologies, theories, and supporting disciplines. Security researchers and practitioners have had to consult many resources to find answers. Some of these resources concentrate on technologies and infrastructures, some on social and legal issues, and some on managerial concerns. This handbook provides all of this information in a comprehensive, three-volume set with a lively format.

Key Concepts and Applications Related to Information Security

Chapters in this group examine a broad range of topics. Theories, concepts, technologies, and applications that expose either a user, manager, or an organization to security and privacy issues and/or create such security and privacy concerns are discussed. Careful attention is given to those concepts and technologies that have widespread applications in business and academic environments. These areas include e-banking, e-communities, e-commerce, e-education, and e-government.

Infrastructure for the Internet, Computer Networks, and Secure Information Transfer

Chapters in this group concentrate on the infrastructure, popular network types, key technologies, and principles

for secure information transfer. Different types of communications media are discussed followed by a review of a variety of networks including LANs, MANs, WANs, mobile, and cellular networks. This group of chapters also discusses important architectures for secure information transfers including TCP/IP, the Internet, peer-to-peer, and client/server computing.

Standards and Protocols for Secure Information Transfer

Chapters in this group discuss major protocols and standards in the security field. This topic includes important protocols for online transactions, e-mail protocols, Internet protocols, IPsec, and standards and protocols for wireless networks emphasizing 802.11.

Information Warfare

This group of chapters examines the growing field of information warfare. Important laws within the United States criminal justice system, as they relate to cybercrime and cyberterrorism, are discussed. Other chapters in this group discuss cybercrime, cyberfraud, cyber stalking, wireless information warfare, electronic attacks and protection, and the fundamentals of information assurance.

Social, Legal, and International Issues

Chapters in this group explore social, legal, and international issues relating to information privacy and computer security. Digital identity, identity theft, censorship, and different types of computer criminals are also explored. The chapters in this group also explain patent, trademark, and copyright issues and offer guidelines for protecting intellectual properties.

Foundations of Information, Computer, and Network Security

These chapters cover four different but complementary areas including encryption, forensic computing, operating systems and the common criteria and the principles for improving the security assurance.

Threats and Vulnerabilities to Information and Computing Infrastructures

The chapters in this group investigate major threats to, and vulnerabilities of, information and computing infrastructures in wired and wireless environments. The chapters specifically discuss intentional, unintentional, controllable, partially controllable, uncontrollable, physical, software and hardware threats and vulnerabilities.

Prevention: Keeping the Hackers and Crackers at Bay

The chapters in this group present several concepts, tools, techniques, and technologies that help to protect information, keep networks secure, and keep the hackers and computer criminals at bay. Some of the topics discussed include physical security measures; measures

for protecting client-side, server-side, database, and medical records; different types of authentication techniques; and preventing security threats to e-commerce and e-mail transactions.

Detection, Recovery, Management, and Policy Considerations

Chapters in this group discuss concepts, tools, and techniques for detection of security breaches, offer techniques and guidelines for recovery, and explain principles for managing a network environment. Some of the topics highlighted in this group include intrusion detection, contingency planning, risk management, auditing, and guidelines for effective security management and policy implementation.

Acknowledgments

Many specialists have helped to make the handbook a resource for experienced and not-so-experienced readers. It is to these contributors that I am especially grateful. This remarkable collection of scholars and practitioners has distilled their knowledge into a fascinating and enlightening one-stop knowledge base in information, computer, and network security that “talks” to readers. This has been a massive effort, as well as a most rewarding experience. So many people have played a role, it is difficult to know where to begin.

I would like to thank the members of the editorial board for participating in the project and for their expert advice on selection of topics, recommendations of authors, and review of the materials. Many thanks to the more than

1,000 reviewers who provided their advice on improving the coverage, accuracy, and comprehensiveness of these materials.

I thank my senior editor, Matt Holt, who initiated the idea of the handbook. Through a dozen drafts and many reviews, the project got off the ground and then was managed flawlessly by Matt and his professional team. Many thanks to Matt and his team for keeping the project focused and maintaining its lively coverage.

Tamara Hummel, editorial coordinator, assisted the contributing authors and me during the initial phases of development. I am grateful for all her support. When it came time for the production phase, the superb Wiley production team took over. Particularly, I want to thank Deborah Schindlar, senior production editor. I am grateful for all her hard work. I thank Michelle Patterson, our marketing manager, for her impressive marketing campaign launched on behalf of the handbook.

Last, but not least, I want to thank my wonderful wife, Nooshin, and my two children, Mohsen and Morvareed, for being so patient during this venture. They provided a pleasant environment that expedited the completion of this project. Mohsen and Morvareed assisted me in sending out thousands of e-mail messages to authors and reviewers. Nooshin was a great help in designing and maintaining the authors’ and reviewers’ databases. Their efforts are greatly appreciated. Also, my two sisters, Azam and Akram, provided moral support throughout my life. To this family, any expression of thanks is insufficient.

Hossein Bidgoli
California State University, Bakersfield

Guide to The Handbook of Information Security

The Handbook of Information Security is a comprehensive coverage of the relatively new and very important field of information, computer, and network security. This reference work consists of three separate volumes and 207 different chapters on various aspects of this field. Each chapter in the handbook provides a comprehensive overview of the selected topic, intended to inform a broad spectrum of readers, ranging from computer and security professionals and academicians to students to the general business community.

This guide is provided to help the reader easily locate information throughout *The Handbook of Information Security*. It explains how the information within it can be located.

Organization

This is organized for maximum ease of use, with the chapters arranged logically in three volumes. While one can read individual volumes (or articles) one will get the most out of the handbook by becoming conversant with all three volumes.

Table of Contents

A complete table of contents of the entire handbook appears in the front of each volume. This list of chapter titles represents topics that have been carefully selected by the editor-in-chief, Dr. Hossein Bidgoli, and his colleagues on the editorial board.

Index

A subject index for each individual volume is located at the end of each volume.

Chapters

The author's name and affiliation are displayed at the beginning of the chapter.

All chapters in the handbook are organized in the same format:

Title and author

Outline

Introduction

Body

Conclusion

Glossary

Cross-References

References

Outline

Each chapter begins with an outline that provides a brief overview of the chapter, as well as highlighting important subtopics. For example, the chapter "Internet Basics" includes sections for Information Superhighway and the World Wide Web, Domain Name Systems, Navigational Tools, Search Engines, and Directories. In addition, second-level and third-level headings will be found within the chapter.

Introduction

Each chapter begins with an introduction that defines the topic under discussion and summarizes the chapter, in order to give the reader a general idea of what is to come.

Body

The body of the chapter fills out and expands upon items covered in the outline.

Conclusion

The conclusion provides a summary of the chapter, highlighting issues and concepts that are important for the reader to remember.

Glossary

The glossary contains terms that are important to an understanding of the chapter and that may be unfamiliar to the reader. Each term is defined in the context of the particular chapter in which it is used. Thus the same term may be defined in two or more chapters with the detail of the definition varying slightly from one chapter to another. The handbook includes approximately 2,700 glossary terms. For example, the chapter "Internet Basics" includes the following glossary entries:

Extranet A secure network that uses the Internet and Web technology to connect two or more intranets of trusted business partners, enabling business-to-business, business-to-consumer, consumer-to-consumer, and consumer-to-business communications.

Intranet A network within the organization that uses Web technologies (TCP/IP, HTTP, FTP, SMTP, HTML, XML, and its variations) for collecting, storing, and disseminating useful information throughout the organization.

Cross-References

All chapters have cross-references to other chapters that contain further information on the same topic. They

appear at the end of the chapter, preceding the references. The cross-references indicate related chapters that can be consulted for further information on the same topic. The handbook contains more than 1,400 cross-references in all. For example, the chapter “Computer Viruses and Worms” has the following cross references:

Hackers, Crackers and Computer Criminals, Hoax Viruses and Virus Alerts, Hostile Java Applets, Spyware, Trojan Horse Programs.

References

The references in this handbook are for the benefit of the reader, to provide references for further research on the given topic. Review articles and research papers that are important to an understanding of the topic are also listed. The references typically consist of a dozen to two dozen entries, and do not include all material consulted by the author in preparing the chapter.

