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. ♾

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

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

Contents

Part 3: Standards and Protocols for Secure Information Transfer

Volume II: Information Warfare; Social, Legal, and International Issues; and Security Foundations

Part 1: Information Warfare

Part 2: Social and Legal Issues

Part 3: Foundations of Information, Computer and Network Security

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

Part 1: Threats and Vulnerabilities to Information and Computing Infrastructures

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

Part 3: Detection, Recovery, Management, and Policy Considerations

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
Sabanci 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 Univesity
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, Cananda
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 commence 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 summarized 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.