Mc Graw Hill Osborne

Includes a Security Dictionary and contributions from topical experts!

The Complete Reference

Network Security

Examine and implement security strategies and discover proven techniques

Secure Windows®, Linux/ UNIX, Novell and Wireless Security networks with logical, concise information

Understand legal issues and HIPPA legislation

Roberta Bragg
CISSP, MCSE: Security, Security+

Mark Rhodes-Ousley
CISSP

Keith Strassberg
CPA, CISSP

MORE THAN 20 CO-AUTHORS AND TECHNICAL REVIEWERS

Network Security: The Complete Reference

Roberta Bragg
Mark Phodes-Ousley
Keith Strassberg

with Brian Buege, Glen Carty,
Bernard Chapple, Anil Desai,
Nick Efford, Thaddeus Fortenberry,
Christian Genetski, Roger Grimes,
Michael Howard, Michael Judd,
Thomas Knox, Ken Pfeil,
Ben Rothke, Andrew Vladimirov,
and Barak Weichselbaum

McGraw-Hill/Osborne
New York Chicago San Francisco
Lisbon London Madrid Mexico City
Milan New Delhi San Juan
Seoul Singapore Sydney Toronto

The McGraw-Hill Companies

McGraw-Hill/Osborne
2100 Powell Street, 10th Floor
Emeryville, California 94608
U.S.A.

To arrange bulk purchase discounts for sales promotions, premiums, or fund-raisers, please contact **McGraw-Hill**/Osborne at the above address. For information on translations or book distributors outside the U.S.A., please see the International Contact Information page immediately following the index of this book.

Network Security: The Complete Reference

1234567890 DOC DOC 0198765432

ISBN 0-07-222697-8

Publisher
Brandon A. Nordin

Vice President & Associate Publisher
Scott Rogers

Editorial Director
Tracy Dunkelberger

Executive Project Editor
Mark Karmendy

Senior Project Editor
Betsy Manini

Acquisitions Coordinator
Athena Honore

Copy Editors
Andy Carroll, Bob Campbell, Emily Rader

Proofreader
Stefany Otis

Technical Editors
Robert Clugston, Ole Drews Jensen
Curtis Karnow, Jim Keogh, Rob Kraft
Eric Maiwald, Michael O'Dea
Gary Prendergast, Curtis W. Rose
Ben Rothke, Steven Thomas
Barak Weichselbaum, Steve Wright

Indexer
Valerie Perry

Composition
Tara Davis, Lucie Ericksen

Illustrators
Kathleen Edwards, Melinda Lytle, Michael Mueller

Series Design
Peter F. Hancik, Lyssa Wald

This book was composed with Corel VENTURA™ Publisher.

Network Security: The Complete Reference

For all of you who struggle
to make the digital world more secure,
this one's for you.
—Roberta Bragg

This book is dedicated to my wife
Marjorie and my son Trent,
both of whom were very helpful
and supportive during the two years
of intense effort required of me to produce
a work of this magnitude.
—Mark Rhodes-Ousley

To Nancy, whose love and support
made this all possible.
There aren't words for what you mean to me.
And also to my family and friends—
you still mean the world to me.
—Keith Strassberg

About the Contributors and Technical Editors

Brian Buege is responsible for developing application security frameworks for a large domestic airline. He has more than ten years of software development experience and has been developing large-scale, enterprise Java applications since 1998. He lives in McKinney, Texas, with his wife and his three-year-old son, who enjoys dinosaurs, ostriches, and hot dogs.

Glen Carty, CCIE, is a data and telecommunications specialist working in the networking industry since the early 1980s. He has held positions with IBM Global Network and AT&T and is the author of the book entitled *Broadband Networking* (McGraw-Hill/Osborne, 2002), which explores the current and emerging high-speed technologies facilitating the convergence of voice, video, and data. Glen is also a contributing author to several books including Stephen Bigelow's *Troubleshooting, Maintaining and Repairing Networks* (McGraw-Hill/Osborne, 2002). Glen wrote the Novell Security chapter for this book.

Bernard Chapple has almost 30-years experience in Information Technology and Data Center Management, including 17 years in Disaster Recovery and Business Continuity. He has developed security policies and procedures for several Fortune 500 companies, including U.S. Trust Corp., PNC Corporation, Merrill Lynch, Bombardier Capital Mortgage, and Southeast Toyota. Bernard was trained at Florida A&M University, Disaster Recovery Institute, American Institute of Banking, Hewlett-Packard, and IBM.

Bernard speaks at user group symposiums and conferences around the country on subjects such as Data Mirroring and Terrorism. He is published in *Contingency Planning & Management* magazine and serves on its Editorial Advisory Board. He sits on the Executive Committee of the Northeast Florida e-Commerce User Group. He is also on the faculty of the International Disaster Recovery Association. He is a member of the Northeast Florida Chapter of the Association of Contingency Planners, the Business Sustainability subcommittee of Duval Prepares, and the City of Jacksonville's CERT (Community Emergency Response Team) program.

Robert Clugston is an information technology security consultant for Foundstone, Inc. He has over six years of experience in systems administration, network security, and web production engineering. Prior to joining Foundstone, Robert worked as a systems administrator for an Internet service provider. His responsibilities included deploying,

maintaining, and securing business-critical systems to include web servers, routers, DNS servers, mail servers, and additional Internet delivery devices and systems. Before that, Robert also worked briefly as an independent contractor specializing in Perl/PHP web development to create online shopping carts. Robert initially joined Foundstone to design and secure Foundstone's web site, and he is now focused on delivering those services to Foundstone's clients. Robert holds a MCSE in Windows NT.

Anil Desai (MCSE, MCSA, MCSD, MCDBA) is an independent consultant based in Austin, Texas. He specializes in evaluating, developing, implementing, and managing solutions based on Microsoft technologies. He has worked extensively with Microsoft's server products and the .NET platform. Anil is the author of several other technical books, including *MCSE/MCSA Managing and Maintaining a Windows Server 2003 Environment Study Guide Exam 70-290* (McGraw-Hill/Osborne, 2003), *Windows 2000 Directory Services Administration Study Guide* (McGraw-Hill/Osborne, 2001), *Windows NT Network Management: Reducing Total Cost of Ownership* (New Riders, 1999), and *SQL Server 2000 Backup and Recovery* (McGraw-Hill/Osborne, 2001). He has made dozens of conference presentations at national events and is also a contributor to magazines.

When he's not busy doing techie-type things, Anil enjoys cycling in and around Austin, playing electric guitar and drums, and playing video games. For more information, you can contact him at anil@austin.rr.com.

Dr. Nick Efford is a senior teaching fellow in the School of Computing at the University of Leeds in the United Kingdom, where he currently teaches object-oriented software engineering, distributed systems, and computer security. His previous published work includes a book on digital image processing using Java.

Thaddeus Fortenberry (MCSE, MCT) is a senior member technical staff and the remote access architect for employee access at HP. For the past year, he has been working on the consolidation of the remote access solutions for the merged Compaq and HP environments. Thaddeus specializes in complete security plans for remote deployments that address real-world issues and protection.

Christian Genetski is a partner in the Washington, DC, office of Sonnenschein Nath & Rosenthal LLP, where he is the vice-chair of the firm's Information Security and Anti-Piracy practice group. Mr. Genetski is a former prosecutor in the Department of Justice Computer Crime Section, where he coordinated the investigations of several prominent computer crime cases, including the widely publicized denial of service attacks that hit e-commerce sites eBay, Amazon.com, and others in February 2000. In private practice, he counsels clients on compliance with information security regulations, conducts investigations into computer security breaches or other hostile network activity, and represents clients in civil litigation or criminal referrals arising from network incidents. Mr. Genetski graduated from the Vanderbilt University School of Law, Order of the Coif. He regularly lectures to a wide variety of audiences on computer crime and information security issues, and he serves as an adjunct professor at the Georgetown University Law Center. Christian would like to thank David Tonisson for his thoughtful contributions to Chapter 30 on legal issues.

Roger A. Grimes (CPA, MCSE NT/2000, CNE 3/4, A+) is the author of *Malicious Mobile Code: Virus Protection for Windows* (O'Reilly, 2001) and the upcoming *Honeypots for Windows*

(Apress, 2004), and he has been fighting malware since 1987. He has consulted for some of the world's largest companies, universities, and the U.S. Navy. Roger has written dozens of articles for national computer magazines, such as *Windows & .NET Magazine, Microsoft Certified Professional Magazine,* and *Network Magazine,* and *Newsweek* covered his work fighting computer viruses. You can contact him at rogerg@cox.net.

Michael Howard is a senior program manager, a founding member of the Secure Windows Initiative group at Microsoft Corp., and a coauthor of *Writing Secure Code* (Microsoft Press International, 2001). He focuses on the short- and long-term goals of designing, building, testing, and deploying applications to withstand attack and yet to still be usable by millions of nontechnical users.

Ole Drews Jensen started in 1987 as a programmer for the U.S. Navy but soon got involved with administering servers and networks. Today Ole is the systems network manager for an enterprise company with several subsidiaries in the recruiting industry. Ole holds CCNP, MCSE, and MCP+I certifications and is currently pursuing CCSP.

Michael Judd (a.k.a. Judd) is a customer training specialist for Sun Microsystems. Over the last six years, he has taught and developed technical courseware on subjects ranging from Java syntax, object-oriented analysis and design, patterns, and distributed programming, to Java security and J2EE. He lives in Plano, Texas, with his wife, three dogs, and a cat.

Curtis Karnow is a partner at the law firm of Sonnenschein Nath & Rosenthal LLP, and a member of the firm's e-commerce, security and privacy, and intellectual property groups. He is the author of *Future Codes: Essays in Advanced Computer Technology and the Law* (Artech House, 1997) and he represents Sun Microsystems in the landmark technology antitrust litigation *Sun Microsystems v. Microsoft*. Karnow has counseled on public key infrastructure policies, electronic contracting, and digital signatures. Formerly assistant U.S. attorney in the Criminal Division, Karnow's responsibilities included prosecution of all federal crimes, including complex white-collar fraud, from investigation and indictment through jury verdict and appeal. Since then, he has represented defendants indicted for unauthorized access to federal interest computers, defended against a criminal grand jury investigation into high tech export actions, represented clients before federal grand juries investigating alleged antitrust conspiracies and securities violations, brought legal actions against Internet-mediated attacks on client networks, and in a state criminal investigation represented a computer professional framed by a colleague in a complex computer sabotage. He has also advised on jurisdictional issues arising out of a federal criminal Internet-related indictment, and he advises on liability and policy issues (including interfacing with law enforcement authorities) arising from computer security breaches and Internet privacy matters. He occasionally sits as a temporary judge in the California state court system. He can be contacted at ckarnow@sonnenschein.com.

Jim Keogh introduced PC programming nationally in his column for *Popular Electronics* magazine in 1982, four years after Apple Computer started in a garage. He was a team member who built one of the first Windows applications by a Wall Street firm, featured by Bill Gates in 1986. Keogh has spent about two decades developing computer systems for Wall Street firms such as Salomon Inc. and Bear, Stearns & Co. Inc.

Keogh is on the faculty of Columbia University where he teaches technology courses including the Java Development lab. He developed and chaired the electronic commerce track at Columbia University. He is the author of *J2EE: The Complete Reference* (McGraw-Hill/Osborne, 2002) and *J2ME: The Complete Reference* (McGraw-Hill/Osborne, 2003), and more than 55 other titles, including *Linux Programming for Dummies, Unix Programming for Dummies and Java Database Programming for Dummies, Essential Guide to Networking, Essential Guide to Computer Hardware, C++ Programmer's Notebook,* and *E-Mergers.* He is also a member of the Java Community Process.

Thomas Knox has done Unix administration for more years than he wants to admit. He is a systems engineer for Amazon.com and can be reached at tknox@mac.com. His thanks go to his wife Gisela for all her love and support.

Rob Kraft works for KCX, Inc. as a project manager. He has coauthored books on Microsoft SQL Server, taught numerous classes as a Microsoft certified trainer, and is a microsoft certified solution developer (MCSD). Rob has presented on SQL, Visual Basic, and Internet Security at many seminars. He also has experience as an administrator and developer with DB2, Oracle, Informix, Sybase, Access, and DBase. He can be contacted at www.robkraft.org.

Eric Maiwald is the director of product management and support for Bluefire Security Technologies. He has over 15 years of experience in information security, including work in both the government and commercial sectors. Eric has performed assessments, developed policies, and implemented security solutions for large financial institutions, healthcare firms, and manufacturers. He holds a bachelor of science degree in electrical engineering from Rensselaer Polytechnic Institute and a master of engineering in electrical engineering from Stevens Institute of Technology, and he is a certified information systems security professional (CISSP). He is a named inventor on patent numbers 5,577,209, "Apparatus and Method for Providing Multi-Level Security for Communications among Computers and Terminals on a Network," and 5,872,847, "Using Trusted Associations to Establish Trust in a Computer Network." Eric is a regular presenter at a number of well-known security conferences. He wrote *Security Planning and Disaster Recovery* with William Sieglein (McGraw-Hill/Osborne, 2002) and is a contributing author for *Hacking Exposed Linux, 2nd Edition* (McGraw-Hill/Osborne, 2002) and *Hacker's Challenge 2* (McGraw-Hill/Osborne, 2002).

Michael O'Dea is project manager of Product Services for the security firm Foundstone, Inc. Michael has been immersed in information technology for over 10 years, working with technologies such as enterprise data encryption, virus defense, firewalls, and proxy service solutions on a variety of UNIX and Windows platforms. Currently, Michael develops custom integration solutions for the Foundstone Enterprise vulnerability management product line. Before joining Foundstone, Michael worked as a senior analyst supporting Internet security for Disney Worldwide Services, Inc. (the data services arm of the Walt Disney Company) and as a consultant for Network Associates, Inc. Michael has contributed to many security publications, including *Hacking Exposed: Fourth Edition* (McGraw-Hill/Osborne, 2003) and *Special Ops: Internal Network Security.*

Ken Pfeil is chief security officer at Capital IQ, a web-based financial information service company headquartered in New York City. Previously, Ken worked at Avaya, where he was

responsible for the Enterprise Security Consulting Practice, North East Region. He has two decades of IT and security experience, including positions at Microsoft, Dell, Identix, and Merrill Lynch. Ken has written extensively on security topics and is coauthor of *Hack-Proofing Your Network, Second Edition* (Syngress), and *Stealing the Network: How to Own the Box* (Syngress), and he is a contributing author to *Security Planning and Disaster Recovery* (McGraw-Hill/Osborne, 2002). He participates in ISSA, CSI, NYECTF, IEEE, and IETF groups and serves as a subject matter expert for CompTIA's Security+ certification as well as ISSA's International Privacy Advisory Board.

Gary Prendergast graduated with a BSc (with Honors) in electronic and computer engineering from the University of Leeds, U.K. He has spent the past eight years working in sales-focused engineering roles with a variety of companies, including Ford Motor Company, EMC Corp., KANA Software, and NativeMinds, Inc. He is currently a senior systems engineer for a market-leading WLAN security and detection company and is pursuing the certified wireless security professional (CWSP) qualification.

Curtis W. Rose is the director of investigations and forensics for SYTEX, Inc. Rose, a former senior counterintelligence special agent, is a well-recognized forensics and incident response expert. He has provided investigative support and training for the U.S. Department of Justice, the FBI's National Infrastructure Protection Center, the Air Force Office of Special Investigations, the U.S. Army, state and local law enforcement, and corporate entities. He has developed specialized software to identify, monitor, and track computer hackers, and he has written affidavits and testified as an expert witness in U.S. Federal Court. He was a contributing author to the *Anti-Hacker Toolkit, Second Edition* (McGraw-Hill/Osborne, 2003) and technical editor for *Incident Response: Investigating Computer Crime, Second Edition* (McGraw-Hill/Osborne, 2003).

Ben Rothke (CISSP) is a New York City–based senior security consultant with ThruPoint, Inc., and he has more than 15 years of industry experience in the area of information systems security. His areas of expertise are in PKI, HIPAA, 21 CFR Part 11, design and implementation of systems security, encryption, firewall configuration and review, cryptography, and security policy development. Prior to joining ThruPoint, Ben was with Baltimore Technologies, Ernst & Young, and Citicorp, and he has provided security solutions to many Fortune 500 companies. Ben is also the lead mentor in the ThruPoint, Inc. CISSP preparation program, preparing security professionals to take the rigorous CISSP examination.

Ben has written numerous articles for such computer periodicals as the *Journal of Information Systems Security, PC Week, Network World, Information Security, SC, Windows NT Magazine, InfoWorld,* and the *Computer Security Journal.* Ben writes for *Unix Review* and *Security Management* and is a former columnist for *Information Security* and *Solutions Integrator* magazine; he is also a frequent speaker at industry conferences. Ben is a certified information systems security professional (CISSP) and certified confidentiality officer (CCO), and a member of HTCIA, ISSA, ICSA, IEEE, ASIS, and CSI.

While not busy making corporate America a more secure place, Ben enjoys spending time with his family, and he is preparing to run in the 2003 Marine Corps Marathon for the Leukemia and Lymphoma Society's Team in Training, the world's largest endurance sports training program.

Steven B. Thomas is president and chief technical officer of Meridian Networks, a network system integration and consulting firm in West End, North Carolina. Recently, he spent five years as a full-time faculty member at Sandhills Community College in Pinehurst, North Carolina, where he taught Microsoft, Cisco, and general networking and system administration topics. Steve holds most major networking certifications, including the MCSE, MCP, MCSA, MCT, Network+, CCNP, CCNA, and CCDA. Steve is also the author of several books on various Microsoft and networking topics, including *Windows NT 4.0 Registry: A Professional Reference* (McGraw-Hill/Osborne, 1998), which despite now being three versions back on Windows remains a useful reference. In his spare time, Steve glories in Windows tips, tricks, and administrivia, and his love for the subject shows in everything he writes. You can contact Steve at sthomas@meridiannetworks.com.

Dr. Andrew A. Vladimirov (CISSP, CCNP, CCDP, CWNA, TIA Linux+) currently holds the position of chief security manager for Arhont Ltd. (www.arhont.com), a fast-growing information security company based in Bristol, U.K. Vladimirov is a graduate of King's College London and University of Bristol. He is a researcher with wide interests, ranging from cryptography and network security to bioinformatics and neuroscience. He published his first scientific paper at the age of 13 and dates his computing experience back to the release of Z80. He was one of the cofounders of Arhont Ltd., which was established in 2000 as a pro-open-source information security company with attitude. Over the years, Vladimirov has participated in Arhont's contributions to the security community via publications at BugTraq and other security-related public e-mail lists, network security articles for various IT magazines, and statistical research.

Vladimirov's wireless networking and security background predates the emergence of the 802.11 standard and includes hands-on experience designing, installing, configuring, penetrating, securing, and troubleshooting wireless LANs, Bluetooth PANs, and infrared links implemented using a wide variety of operating systems and hardware architectures. Vladimirov was one of the first U.K. IT professionals to obtain the CWNA certification, and he is currently in charge of the wireless consultancy service provided by Arhont Ltd. He participates in wireless security equipment beta-testing for major wireless hardware and firmware vendors, such as Proxim, Belkin, and Netgear. You can reach Vladimirov at andrew@arhont.com (please use the public key available at http://gpg.arhont.com).

Barak Weichselbaum, a network and security consultant, started his career in the Israeli armed defense forces and served in the intelligence corps. He spearheaded the development of numerous network security products and solutions, including B2B, P2P, IPS, and IDS from the ground up to the deployment and integration stage. You can contact him at www.komodia.com.

Steve Wright (MCSD, MCDBA, MCSE, MCSA, MCAD) is a senior architect with plaNet Consulting in Omaha, Nebraska. He has been developing mission-critical and line-of-business systems for the last 15 years. Steve leads development teams in the financial, healthcare, insurance, and transportation industries. Steve started his career at IBM working on AIX, but today he works mostly on the Microsoft platform with .NET, BizTalk, and SQL Server.

About the Authors

Roberta Bragg (CISSP, MCSE: Security; Security+, ETI Client Server, Certified Technical Trainer, IBM Certified Trainer, DB2-UDB, Citrix Certified Administrator) has been a Security Advisor columnist for *Microsoft Certified Professional Magazine* for five years, is a Security Expert for SearchWin2000.com, and writes for the "SecurityWatch" newsletter, which has over 55,000 subscribers. Roberta designed, planned, produced, and participated in the first Windows Security Summit, held in Seattle, Washington, in 2002. Also in 2002 at TechMentor San Diego, Roberta gave the first production of "Security Academy," a three-day hands-on secure network-building workshop, and it was subsequently scheduled for five repeat presentations in 2003. In September and October of 2002, Roberta was an instructor for four sessions of SANS Gold Standard Windows 2000 Training. Roberta has participated in numerous security audits and is a security evangelist traveling all over the world consulting, assessing, and training on network and Windows security. Roberta has served as adjunct faculty at Seattle Pacific University and at Johnson County Community College teaching courses on Windows 2000 Security Design and Network Security Design. Roberta is the lead author of the upcoming *MCSE 70-298 Designing Windows Server 2003 Security*, and *Windows Server 2003 Security Administrators Companion,* both from Microsoft Press. She has written on SQL Server 2000, CISSP, and Windows Security for QUE and New Riders.

Mark Rhodes-Ousley (CISSP) has been a practicing security professional for more than ten years. Mark has advised, designed, and installed security technologies and policies for dozens of companies, including Fortune 500 companies such as Clorox and Gap, Inc., large companies such as Sun Microsystems and Hitachi Data Systems, medium-sized companies such as Metricom and Watkins-Johnson, and many small companies such as Napster and Internex. All this experience with companies in different stages of growth leads to a unique perspective on how to manage security for a growing company—where to begin, what to do when moving forward, and how to plan for future growth.

Mark's focus is strategic as well as tactical. Believing that business processes are even more important than technical configurations, Mark has specialized in defense instead of hacking. Much of the work he has done in the field of information security has been groundbreaking. He has worked with some of the top figures in the industry and has trained others, and some of his security philosophies show up in publications by individuals and companies where he has left his mark. Mark holds certifications from the International

Information Systems Security Certification Consortium, known as (ISC)^2, Cisco Systems, Security Dynamics, Raptor Systems, Hewlett-Packard, and Digital Equipment Corporation, along with a bachelor's degree in applied mathematics and electrical engineering from the University of California, San Diego (UCSD).

Keith Strassberg (CPA, CISSP) is an independent security consultant with over seven years of experience in information security. Most recently, he worked as a senior security engineer for a mid-sized technology consulting company. Prior to that, Keith was part of the computer risk management group at Arthur Andersen, LLP. Keith's professional experiences cover all facets of information security, including, but not limited to, designing and deploying secure infrastructures, implementing firewalls and intrusion-detection systems, performing computer forensic investigations, developing policies and procedures, and performing vulnerability testing.

His publications include authoring *Firewalls: The Complete Reference* (McGraw-Hill/Osborne, 2002) as well as contributing to other popular books, such as *Security Architecture: Design, Deployment, and Operation* (McGraw-Hill/Osborne, 2001), and *Troubleshooting, Maintaining & Repairing Networks* (McGraw-Hill/Osborne, 2002).

Keith has a BS in accounting from Binghamton University, and he can be reached at kstrassberg@yahoo.com

Acknowledgments

Thanks to Athena Honore, without whom all the pieces of this book would have been scattered. I honestly don't know how she kept 28 authors' and reviewers' materials straight and on track. Thanks to Tracy Dunkelberger, who pushed this book forward in spite of seemingly insurmountable odds. Thanks to the other authors who put up with this cranky old lady and her fussy requests for "more," "better," "sharper." Thank goodness for the Internet, without which we'd still be tracking down manuscripts in mailing envelopes and blaming the delivery mechanism (and using it for an excuse too).

—Roberta Bragg

I would like to acknowledge those who established, developed, and documented the information security industry and upon whose efforts this work is built: Bruce Schneier, Bill Cheswick, Steve Bellovin, Winn Schwartau, Simson Garfinkel, Gene Spafford, Sun Tzu, Miyamoto Musashi, Cliff Stoll, Ben Rothke, Charles Cresson Wood, Brent Chapman, Elizabeth Zwicky, William Stallings, and Phil Zimmerman, among many others too numerous to list.

—Mark Rhodes-Ousley

I'd like to take this opportunity to thank all my official and unofficial mentors over the years who patiently taught me so much about the world of Information Security. Also, a big thank-you to the people who made this book happen: Roberta and Mark, the ever-diligent people at McGraw-Hill/Osborne, Tracy Dunkelberger and Athena Honore and all the other editors who made sure the i's were dotted and the t's were crossed.

—Keith Strassberg

Introduction

You hold in your hands a testimony to the practice and passion of a multitude of hearts. Network security is an incredibly complicated and vast topic area, which is why it was unthinkable to imagine that three authors could effectively write on all the critical issues associated with it. We went beyond ourselves and enlisted the best and brightest minds in the industry to help us create what is intended to be the definitive guide to network security: the book you go to first, the one you trust. We've taken this opportunity to present realistic and useful information on the most relevant topics that IT professionals face every day. We wish with our very being that we could impart to you *all* the knowledge that we have gained through study, through experiment, and through practical responses to the realities of defending real-world networks, yet we know that such information transfer might not even be possible in a 15-volume set.

This is not a book that will scare you into some crazed exercise of response to wanton tales of horror. It won't tell you the magic ten things to do to secure your networks, harden your server, or rid the world of worms and spam. What it will do is provide both the big picture and the intimate details of 30 different areas of network security. This book spans the spectrum: from physical security to the legal implications of recent laws; from authentication, authorization, and auditing to defense, deterrence, and detection; from disaster recovery to configuring security on a Cisco router; from Windows to Linux and back again. Each author is an expert in his or her field. Each wants you to be. Inside this book you'll find their best work.

The book is divided into six sections that broadly define the subdomains of network security.

Part I: Network Security Foundations

This part of the book provides an overview of network security and defines the major management issues and organizational structures of information security. If you are a technical person by education or by experience, these chapters may, at first, appear to be something you can skip, or leave until last. Don't. Just as you need to understand how a computer works and how program instructions are executed in order to write good code; just as you need to know the seven layers of the OSI model to understand networking; just as you need to know the technical foundations, you need to know the things that form the basis of information security in order to apply them.

This part introduces risk analysis and security policies, and it defines how security management is organized in the enterprise.

Risk analysis is used to identify which systems should be secured first and which should get the budget dollars to do so. Do you have ideas for improving security by purchasing equipment, by implementing changes in the password policy, by providing security training for IT pros? Perhaps the corporate risk analysis can provide you the leverage you need to obtain the funds.

Security policy dictates what you can do and what you can't, both in your use of information systems *and* in your administration of them. Would you like to audit the password database and find users who aren't using good judgment in their selection of passwords? Better make sure you know what the password policy is, according to the written security policy, and better still, check whether you have the right to audit the database.

Security organization is a formal structure in many organizations, and it should be in others. Where do you fit in? Where would you like to?

Part II: Access Control

If no one were able to access the computing systems, we'd not have any problems. However, we need to be able to read and manipulate data, visit remote sites, and run applications. We need to use computers to do things. We have to sit at them, connect to them, log on to them, repair them, add new features, install new software, patch them, carry them with us, and leave them in hotel rooms.

How do we protect them? We can begin to enforce computer security by controlling access to computers and to the data and applications that are on them. Controlling access means many things to many people, but most will agree that it encompasses physical security, authentication (proving you are who you say you are), authorization (identifying what you can do once you have authenticated), and data and security management architectures. These chapters contain practical tips and the methodologies forged by experts to deal with the data center and traditional desktop deployments, as well as information on how to deal with the rapid accumulation and use of mobile computing devices. Security architects have had a long time to think about access controls; your authors will provide you with their insights.

Part III: Network Architecture

Cabling systems together and sticking a firewall between them and the Internet is not the way to secure a network—it's only a start. To be secure, a network must have an underlying infrastructure that is designed with security considerations at every juncture. Where should equipment closets be placed, and how should they be secured? Are switches more secure than routers? What type of firewall should you use? Do new intrusion-prevention devices make intrusion detection obsolete? Just what are the designs and devices that can mean the difference between a network that is secure and one that never can be?

In these chapters, you will find succinct definitions and copious advice on what makes a secure network. You'll find security devices, such as firewalls and IDSs, explained, as well as the steps to secure them. You'll discover best practices for using and securing VPNs,

designing secure networks, and securely integrating wireless networks. You'll find an excellent treatment of how to ensure the integrity of the network and the data it supports, as well as the need to support redundancy and recoverability.

No discussion of network infrastructure security would be complete without information on how to secure the various roles that computers play. Mail servers, fax servers, file and print servers, and others are integral parts of the network, and they need to be secured from attack and to be prevented from becoming the vector of an attack.

Part IV: Operating System Security

The basis for the security of applications that run on clients and servers connected to your network is the operating system. Before you can consider securing the applications that run in your network, you need to harden the underlying programs that provide the services on which the applications rely. The first thing that should be understood about operating system security is that, just as there are principles and models that define the services, such as networking, file system, and user interfaces, there are operating system security models. This section explains them in its first chapter. You should read the subsequent chapters on Unix, Linux, Windows, and Novell while thinking about them.

Part V: Application Security

For most people, applications are computers. They don't care about operating systems, networks, or such things. It's just important for them to be able to get their e-mail, play a game, write a report, use a spreadsheet, enter an order, or print the payroll checks. To many networking professionals, applications are second-class citizens and fall just above end-users in their hierarchy of importance. Applications, however, and the processes used to create them, run them, and manage their data, are the crux of information security today. No other element spans the spectrum. Ordinary people interface with applications, extraordinary people create them, evil people attempt to break them.

Applications are the e-mail clients, games, and data entry systems we know and use, but in some sense they are also the building blocks of operating systems, servers, and network devices. All of these programs are built using the same tools, the same languages, the same imperfect human minds. On a daily basis, we ask that these complex systems be created without flaws and that they never break down. When they do not meet our expectations, we cry foul.

How can this situation be changed? For many years, computer scientists have preached methodologies for making better programs. For many years, commercial software companies have not followed them. That is changing. This part of the book provides a detailed look at the principles and practices of writing secure software, no matter the specific technology you use and no matter the type of program. Complementary chapters on using Windows .NET and J2EE are also included. The section ends with a chapter on securing databases—repositories of data and their applications.