INTERNET SECURITY

Professional Reference

Derek Atkins
Paul Buis
Chris Hare
Robert Kelley
Carey Nachenberg
Anthony B. Nelson
Paul Phillips
Tim Ritchey
William Steen

New Riders Publishing, Indianapolis, IN

Internet Security Professional Reference

By Derek Atkins, Paul Buis, Chris Hare, Robert Kelley, Carey Nachenberg, Anthony B. Nelson, Paul Phillips, Tim Ritchey, and William Steen

Published by:
New Riders Publishing
201 West 103rd Street
Indianapolis, IN 46290 USA

Printed in the United States of America 1 2 3 4 5 6 7 8 9 0

Warning and Disclaimer

This book is designed to provide information about Internet security. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an "as is" basis. The authors and New Riders Publishing shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the disks or programs that may accompany it.

Publisher	Don Fowley
Publishing Manager	Emmett Dulaney
Marketing Manager	Ray Robinson
Managing Editor	Carla Hall

Acquisitions Editor
Mary Foote

Development Editor
Ian Sheeler

Project Editor
John Sleeva

Copy Editors
Peter Kuhns
Catherine Manship
Angie Trzepacz
Phil Worthington

Technical Editors
John Fisher
Paul Nelson
Tom Peltier
Michael Van Biesbrouck

Associate Marketing Manager
Tamara Apple

Acquisitions Coordinator
Stacia Mellinger

Publisher's Assistant
Karen Opal

Cover Designer
Karen Ruggles

Book Designer
Sandra Schroeder

Production Manager
Kelly D. Dobbs

Production Team Supervisor
Laurie Casey

Graphics Image Specialists
Clint Lahnen
Laura Robbins

Production Analysts
Jason Hand
Bobbi Satterfield

Production Team

Heather Butler, Angela Calvert, Kim Cofer, Tricia Flodder, Aleata Howard, Erika Millen, Beth Rago, Regina Rexrode, Erich Richter, Jenny Shoemake, Christine Tyner, Karen Walsh

Indexers
Christopher Cleveland
Tom Dinse

About the Authors

Derek Atkins grew up in Beachwood, Ohio, and graduated from Beachwood City Schools. He followed that with schooling at MIT in Cambridge, Massachusetts. While working toward his B.S. degree, Derek became interested in computer security. He started working with Kerberos, PGP, and other security systems before he graduated. After receiving his degree, he went to the MIT Media Laboratory for his M.S. degree in Media Arts and Sciences. His security background was used in his thesis, a payment system based on digital movie tickets. Today, Derek works at Sun Microsystems, programming the next generation of system security applications.

Paul Buis started life in Kalamazoo, Michigan, moved about in the midwest, and met his wife-to-be in a high school German class. Paul attended Hope College in Holland, Michigan, where he majored in Physics and Mathematics. Hope graduated him magna cum laude and elected him to Phi Beta Kappa, a Liberal Arts honorary; Sigma Pi Sigma, a Physics honorary; and Pi Mu Epsilon, a Mathematics honorary. After marrying his wife, Barbara, Paul went to Purdue University where he received M.S. degrees in both Mathematics and Computer Science.

While attending Purdue, Paul was the software architect for a firm that sold veterinary cardiology systems to automatically diagnose heart problems in dogs and cats. Eventually, Paul completed his doctoral work in computer science at Purdue and got a real job as a professor in the Computer Science Department at Ball State University in Muncie, Indiana. He is also an instructor for the Technology Exchange Company, located in Reading, Massachusetts, which sends him around the country to give workshops on TCP/IP networking, the X Window system, C++ programming, and Unix system administration.

Paul and Barbara are the parents of three delightful children: Daniel, Jennifer, and Thomas.

Chris Hare is the Production Services Manager for a Canadian national Internet Service Provider, iSTAR internet. He started working in computer-based technology in 1986, after studying health sciences. Since that time, he has worked in programming, system administration, quality assurance, training, network management, consulting, and technical management positions.

Chris has taught Unix courses all over the world, for his previous employers and for SCO. As a professional writer, Chris has authored almost 20 articles for *Sys Admin* magazine, and coauthored several books for New Riders, including *Inside Unix*, *Internet Firewalls and Network Security*, and *Building an Internet Server with Linux*.

Chris lives in Ottawa, Canada, with his wife Terri and their children Meagan and Matthew.

Robert Kelley is currently a software engineer in the networking lab of Hewlett-Packard, supporting network security and Internet services. He has held a variety of positions in marketing, support, and development. His educational background includes a B.S. degree in Electrical Engineering from San Jose State University, an M.S. degree in Computer Science from California State University at Hayward, and graduate work at Santa Clara University. Mr. Kelley has written a number of white papers on topics ranging from disk drive manufacturing to microwave communications. He has created and presented training to classes in Asia, Europe, and the United States, including video productions and live broadcast seminars. He created the security-alert@hp.com mail alias and has written many of HP's security bulletins. His current interests include compilers, cryptography, and data compression.

Carey Nachenberg is a senior software engineer at Symantec Corporation. He researches, designs, and develops new antivirus technologies for the award-winning Norton Antivirus line of products. Mr. Nachenberg has worked at Symantec for five years as a software engineer and architect on Norton Commander, Norton Desktop for DOS, and Norton Antivirus. He holds B.S. and M.S. degrees in Computer Science and Engineering from the University of California at Los Angeles. His master's thesis covers the topic of polymorphic computer virus detection.

Anthony B. Nelson is a management consultant specializing in information security and business automation. A regular contributor to the IT security industry, Mr. Nelson has 26 years of experience in the field, including regular speaking engagements at international conferences on information security and auditing issues. He has worked with a wide range of applications, from business and government accounting to technical applications such as Electronic and Mechanical Computer Assisted Drafting. He has worked on a variety of standard and proprietary platforms, including Unix, Microsoft Windows NT, PC DOS, Windows, and various networks.

Mr. Nelson has been involved in the security architecture design for a major West Coast utility. In addition, he designed their information security policy and developed their security implementation. The environment is an integrated network running Banyan Vines, TCP/IP, DecNet, Appletalk, and SNA. Other security projects have included disaster recovery projects, internetwork file transfer security, and reviews of security for, and intrusion testing of, Internet firewalls.

Recently, Mr. Nelson has been involved with corporate internal audit departments investigating IT-related problems. These have involved intrusion tracing to determine the source of system crashes, file damage, as well as fraud investigations in which the computer was the main point of attack. He has been involved in intrusion testing of client/server applications to determine the security holes that must be protected. Where companies have been involved in remote communication, he has reviewed remote dial up security, and looked into single-point of sign on solutions. Finally, he recently reviewed SCADA application security for master stations connected to the corporate LAN/WAN.

Mr. Nelson also has software project management experience. Project supervision has ranged from the initial systems analysis to programming, debugging, implementation, training, and after sales support for the applications. Direct participation in each of the phases has resulted in a firm understanding of the problems and pitfalls throughout the entire development cycle. In these projects, Mr. Nelson has been involved with implementing security at the computer hardware level, the operating systems level, and at the applications level.

Paul Phillips is a programmer and author currently residing in San Diego, California.

Tim Ritchey received his honors B.S. from Ball State University in Physics and Anthropology and is currently working toward his Ph.D. in Archaeology from Cambridge University, England. He has worked on artificial intelligence, high-performance parallel architectures, and computer vision. His honors thesis was the development of an inexpensive 3D scanner using structured lighting. Present interests include artificial intelligence, distributing computing, VRML, and Java. His Ph.D. includes adapting non-linear dynamics and artificial intelligence techniques to archaeological theory. In addition to computing and archaeology, he enjoys scuba diving, flying, and riding his Harley Davidson motorcycle.

William Steen owns and operates a consulting firm specializing in networking small businesses and local governmental agencies. He also works for BI Inc. as a senior customer support representative. He is the author of *Managing the NetWare 3.x Server* and *NetWare Security*, and a contributing author for *Implementing Internet Security*, published by New Riders.

Trademark Acknowledgments

Contents at a Glance

Table of Contents

INTRODUCTION

The staff of New Riders Publishing is committed to bringing you the very best in computer reference material. Each New Riders book is the result of months of work by authors and staff who research and refine the information contained within its covers.

As part of this commitment to you, the NRP reader, New Riders invites your input. Please let us know if you enjoy this book, if you have trouble with the information and examples presented, or if you have a suggestion for the next edition.

Please note, though: New Riders staff cannot serve as a technical resource for Internet security or for questions about software- or hardware-related problems.

If you have a question or comment about any New Riders book, there are several ways to contact New Riders Publishing. We will respond to as many readers as we can. Your name, address, or phone number will never become part of a mailing list or be used for any purpose other than to help us continue to bring you the best books possible. You can write us at the following address:

New Riders Publishing
Attn: Publisher
201 W. 103rd Street
Indianapolis, IN 46290

If you prefer, you can fax New Riders Publishing at (317) 581-4670.

You can also send e-mail to New Riders at the following Internet address:

`edulaney@newriders.mcp.com`

NRP is an imprint of Macmillan Computer Publishing. To obtain a catalog or information, or to purchase any Macmillan Computer Publishing book, call (800) 428-5331.

Thank you for selecting *Internet Security Professional Reference!*