

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 Richey, and William Steen

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

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the publisher, except for the inclusion of brief quotations in a review.

Copyright © 1996 by New Riders Publishing

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

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. New Riders Publishing cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Contents at a Glance

| | |
|---|-----|
| Introduction | 1 |
| Part I: Managing Internet Security | |
| 1 Understanding TCP/IP | 5 |
| 2 Understanding and Creating Daemons..... | 49 |
| 3 Using UUCP | 95 |
| 4 Audit Trails | 145 |
| 5 RFC 1244—The Site Security Handbook | 169 |
| Part II: Gaining Access and Securing the Gateway | |
| 6 IP Spoofing and Sniffing | 257 |
| 7 How to Build a Firewall | 317 |
| 8 SATAN and the Internet Inferno | 429 |
| 9 Kerberos | 535 |
| Part III: Messaging: Creating a Secure Channel | |
| 10 Encryption Overview | 615 |
| 11 PGP | 633 |
| Part IV: Modern Concerns | |
| 12 Java Security | 693 |
| 13 CGI Security | 731 |
| 14 Viruses | 751 |
| Part V: Appendixes | |
| A Security Information Sources | 845 |
| B Internet Security References | 849 |
| Index..... | 855 |

Table of Contents

| | |
|--------------|---|
| Introduction | 1 |
|--------------|---|

Part I: Managing Internet Security

| | | |
|----------|---|----------|
| 1 | Understanding TCP/IP | 5 |
| | The History of TCP/IP | 6 |
| | Exploring Addresses, Subnets, and Hostnames | 7 |
| | Address Classes | 8 |
| | Subnets | 9 |
| | Hostnames | 12 |
| | Working with Network Interfaces | 14 |
| | Configuration Using ifconfig | 15 |
| | Reviewing the Network Configuration Files | 17 |
| | The /etc/hosts File | 17 |
| | The /etc/ethers File | 18 |
| | The /etc/networks File | 18 |
| | The /etc/protocols File | 19 |
| | The /etc/services File | 19 |
| | The /etc/inetd.conf File | 20 |
| | Understanding the Network Access Files | 21 |
| | /etc/hosts.equiv File | 21 |
| | The .rhosts File | 21 |
| | User and Host Equivalency | 21 |
| | Examining TCP/IP Daemons | 23 |
| | The slink Daemon | 23 |
| | The ldsocket Daemon | 23 |
| | The cpd Daemon | 23 |
| | The Line Printer Daemon (lpd) | 23 |
| | The SNMP Daemon (snmpd) | 24 |
| | The RARP Daemon (rarpd) | 24 |
| | The BOOTP Daemon (bootpd) | 24 |
| | The ROUTE Daemon (routed) | 24 |
| | The Domain Name Service Daemon (named) | 25 |
| | The System Logger Daemon (syslogd) | 26 |
| | Inetd—The Super-Server | 26 |
| | The RWHO Daemon (rwhod) | 26 |

| | |
|---|-----------|
| Exploring TCP/IP Utilities | 26 |
| Administration Commands | 27 |
| User Commands | 40 |
| 2 Understanding and Creating Daemons | 49 |
| What Is a Daemon? | 50 |
| Examining the System Daemons | 55 |
| init | 55 |
| swapper | 55 |
| update and bdf flush | 55 |
| lpd | 56 |
| lpsched | 56 |
| cpd and sco_cpd (SCO) | 56 |
| cron | 56 |
| syslog | 57 |
| sendmail | 58 |
| getty | 59 |
| rlogind | 59 |
| deliver | 59 |
| inetd | 59 |
| routed | 59 |
| nfsd | 60 |
| mountd | 60 |
| pcnfsd | 60 |
| statd, rpc.statd | 60 |
| lockd, rpc.lockd | 60 |
| Creating Daemons with the Bourne Shell | 61 |
| Handling Input and Output | 61 |
| Handling Messages | 62 |
| Handling Signals | 62 |
| The dfmon Program | 64 |
| Creating Daemons with PERL | 65 |
| Handling Input and Output | 66 |
| Handling Signals | 67 |
| The procmon Program | 67 |
| Unix Run Levels | 71 |
| Program Listings | 74 |
| Listing 2.1—The dfmon Program | 74 |
| Listing 2.2—The dfmon Configuration File | 78 |
| Listing 2.3—The procmon Command | 82 |
| Listing 2.4—The procmon.cfg File | 94 |

| | | |
|----------|---|------------|
| 3 | Using UUCP | 95 |
| | The History of UUCP | 96 |
| | The UUCP Network..... | 98 |
| | How UUCP Works | 99 |
| | Naming Your Host | 100 |
| | The Naming Process | 101 |
| | The System V Basic Networking Utilities UUCP..... | 101 |
| | UUCP File Layout | 102 |
| | Configuring UUCP | 103 |
| | Testing the Connection | 106 |
| | The Dialers File..... | 106 |
| | The Systems File | 108 |
| | The UUCP Chat Script | 111 |
| | Testing the Connection—Using uucico | 114 |
| | Permissions File..... | 118 |
| | Allowing Anonymous UUCP Access | 123 |
| | UUCP Log Files | 124 |
| | Maintenance..... | 126 |
| | Configuring Version 2 UUCP..... | 128 |
| | What Is Version 2 UUCP? | 128 |
| | File Layout | 128 |
| | Configuring UUCP | 129 |
| | The L-devices File | 129 |
| | Testing the Connection | 130 |
| | The L.sys File | 131 |
| | Testing the Connection with uucico..... | 133 |
| | Version 2 Permissions..... | 134 |
| | Log Files | 137 |
| | Maintenance..... | 138 |
| | Configuring UUCP over TCP/IP | 139 |
| | Code Listings | 140 |
| | Listing 3.1—gtimes.c | 140 |
| | Listing 3.2—genUSER..... | 142 |
| 4 | Audit Trails | 145 |
| | Audit Trails under Unix | 146 |
| | Common Unix Logs..... | 146 |
| | Process Accounting..... | 153 |
| | Useful Utilities in Auditing | 155 |
| | Other Reporting Tools Available Online | 158 |

| | |
|---|------------|
| Audit Trails under Windows NT | 160 |
| Using the Event Viewer | 161 |
| Logging the ftp Server Service | 162 |
| Logging httpd Transactions | 163 |
| Logging by Other TCP/IP Applications under NT | 163 |
| Audit Trails under DOS | 164 |
| PC/DACS | 164 |
| Watchdog | 165 |
| LOCK | 165 |
| Using System Logs to Discover Intruders | 165 |
| Common Break-In Indications | 165 |
| Potential Problems | 166 |
| 5 RFC 1244—The Site Security Handbook | 169 |
| Contributing Authors | 170 |
| 1. Introduction | 170 |
| 1.1 Purpose of this Work | 170 |
| 1.2 Audience | 171 |
| 1.3 Definitions | 171 |
| 1.4 Related Work | 171 |
| 1.5 Scope | 172 |
| 1.6 Why Do We Need Security Policies and Procedures? | 172 |
| 1.7 Basic Approach | 174 |
| 1.8 Organization of this Document | 174 |
| 2. Establishing Official Site Policy on Computer Security | 175 |
| 2.1 Brief Overview | 175 |
| 2.2 Risk Assessment | 177 |
| 2.3 Policy Issues | 179 |
| 2.4 What Happens When the Policy is Violated | 184 |
| 2.5 Locking In or Out | 186 |
| 2.6 Interpreting the Policy | 187 |
| 2.7 Publicizing the Policy | 188 |
| 3. Establishing Procedures to Prevent Security Problems | 188 |
| 3.1 Security Policy Defines What Needs to be Protected | 188 |
| 3.2 Identifying Possible Problems | 189 |
| 3.3 Choose Controls to Protect Assets in a Cost-Effective Way | 190 |
| 3.4 Use Multiple Strategies to Protect Assets | 191 |
| 3.5 Physical Security | 191 |
| 3.6 Procedures to Recognize Unauthorized Activity | 191 |
| 3.7 Define Actions to Take When Unauthorized Activity is Suspected | 193 |

| | |
|--|-----|
| 3.8 Communicating Security Policy | 193 |
| 3.9 Resources to Prevent Security Breaches | 197 |
| 4. Types of Security Procedures | 214 |
| 4.1 System Security Audits | 214 |
| 4.2 Account Management Procedures | 215 |
| 4.3 Password Management Procedures | 215 |
| 4.4 Configuration Management Procedures | 217 |
| 5. Incident Handling | 218 |
| 5.1 Overview | 218 |
| 5.2 Evaluation | 222 |
| 5.3 Possible Types of Notification | 224 |
| 5.4 Response | 226 |
| 5.5 Legal/Investigative | 229 |
| 5.6 Documentation Logs | 232 |
| 6. Establishing Post-Incident Procedures | 232 |
| 6.1 Overview | 232 |
| 6.2 Removing Vulnerabilities | 233 |
| 6.3 Capturing Lessons Learned | 234 |
| 6.4 Upgrading Policies and Procedures | 235 |
| 7. References | 236 |
| 8. Annotated Bibliography | 237 |
| 8.1 Computer Law | 238 |
| 8.2 Computer Security | 239 |
| 8.3 Ethics | 244 |
| 8.4 The Internet Worm | 246 |
| 8.5 National Computer Security Center (NCSC) | 248 |
| 8.6 Security Checklists | 251 |
| 8.7 Additional Publications | 251 |
| 9. Acknowledgments | 253 |
| 10. Security Considerations | 253 |
| 11. Authors' Addresses | 253 |

Part II: Gaining Access and Securing the Gateway

| | |
|---|------------|
| 6 IP Spoofing and Sniffing | 257 |
| Sniffing | 258 |
| Sniffing: How It Is Done | 258 |
| Sniffing: How It Threatens Security | 260 |
| Protocol Sniffing: A Case Study | 262 |
| Sniffing: How to Prevent It | 265 |
| Hardware Barriers | 266 |
| Avoiding Transmission of Passwords | 274 |

| | |
|---|------------|
| Spoofing | 279 |
| Hardware Address Spoofing | 279 |
| ARP Spoofing | 281 |
| Preventing an ARP Spoof | 284 |
| Sniffing Case Study Revisited | 287 |
| Detecting an ARP Spoof | 288 |
| Spoofing the IP Routing System | 293 |
| ICMP-Based Route Spoofing | 293 |
| Misdirecting IP Datagrams from Hosts | 297 |
| Preventing Route Spoofing | 298 |
| A Case Study Involving External Routing | 300 |
| Spoofing Domain Name System Names | 301 |
| Spoofing TCP Connections | 309 |
| 7 How to Build a Firewall | 317 |
| The TIS Firewall Toolkit | 318 |
| Understanding TIS | 318 |
| Where to Get TIS Toolkit | 319 |
| Compiling under SunOS 4.1.3 and 4.1.4 | 320 |
| Compiling under BSDI | 320 |
| Installing the Toolkit | 321 |
| Preparing for Configuration | 322 |
| Configuring TCP/IP | 326 |
| IP Forwarding | 326 |
| The netperm Table | 328 |
| Configuring netacl | 329 |
| Connecting with netacl | 331 |
| Restarting inetd | 333 |
| Configuring the Telnet Proxy | 333 |
| Connecting through the Telnet Proxy | 336 |
| Host Access Rules | 337 |
| Verifying the Telnet Proxy | 338 |
| Configuring the rlogin Gateway | 339 |
| Connecting through the rlogin Proxy | 342 |
| Host Access Rules | 342 |
| Verifying the rlogin Proxy | 343 |
| Configuring the FTP Gateway | 343 |
| Host Access Rules | 345 |
| Verifying the FTP Proxy | 346 |
| Connecting through the FTP Proxy | 347 |
| Allowing FTP with netacl | 348 |

| | |
|---|-----|
| Configuring the Sendmail Proxy: smap and smapd | 348 |
| Installing the smap Client | 349 |
| Configuring the smap Client | 349 |
| Installing the smapd Application | 351 |
| Configuring the smapd Application | 351 |
| Configuring DNS for smap | 353 |
| Configuring the HTTP Proxy | 354 |
| Non-Proxy Aware HTTP Clients | 355 |
| Using a Proxy Aware HTTP Client | 356 |
| Host Access Rules | 357 |
| Configuring the X Windows Proxy | 359 |
| Understanding the Authentication Server | 360 |
| The Authentication Database | 362 |
| Adding Users | 364 |
| The Authentication Shell—authmgr | 368 |
| Database Management | 368 |
| Authentication at Work | 370 |
| Using plug-gw for Other Services | 372 |
| Configuring plug-gw | 372 |
| plug-gw and NNTP | 373 |
| plug-gw and POP | 376 |
| The Companion Administrative Tools | 378 |
| portscan | 378 |
| netscan | 379 |
| Reporting Tools | 380 |
| Where to Go for Help | 389 |
| Sample netperm-table File | 390 |
| Manual Reference Pages | 394 |
| Authmgr—Network Authentication Client Program | 394 |
| authsrv—Network Authentication Third-Party Daemon | 395 |
| ftp-gw—FTP Proxy Server | 402 |
| http-gw—Gopher/HTTP Proxy | 406 |
| login-sh—Authenticating Login Shell | 412 |
| netacl—TCP Network Access Control | 414 |
| plug-gw—Generic TCP Plugboard Proxy | 416 |
| rlogin-gw—rlogin Proxy Server | 418 |
| smap—Sendmail Wrapper Client | 420 |
| smapd—Sendmail Wrapper Daemon | 421 |
| tn-gw—telnet Proxy Server | 423 |
| x-gw—X Gateway Service | 426 |

| | | |
|----------|--|------------|
| 8 | SATAN and the Internet Inferno | 429 |
| | The Nature of Network Attacks | 431 |
| | Internet Threat Levels (ITL) | 432 |
| | Common Attack Approaches | 435 |
| | An Overview of Holes | 438 |
| | Learning about New Security Holes | 443 |
| | Thinking Like an Intruder | 445 |
| | Gathering Information on Systems | 445 |
| | Know the Code | 465 |
| | Try All Known Problems | 466 |
| | Match Vulnerabilities with Opportunities | 466 |
| | Look for Weak Links | 467 |
| | Summarize the Remote Network Attack | 467 |
| | Automate the Search | 467 |
| | The First Meeting with SATAN | 468 |
| | History | 468 |
| | The Creators | 469 |
| | Comparison to Other Tools | 470 |
| | Vendor Reactions | 470 |
| | Long-Term Impact | 470 |
| | Detecting SATAN | 471 |
| | Courtney | 471 |
| | Gabriel | 471 |
| | TCP Wrappers | 471 |
| | netlog/TAMU | 472 |
| | Argus | 472 |
| | Using Secure Network Programs | 472 |
| | Kerberos | 472 |
| | Secure Shell (ssh) | 474 |
| | SSL | 474 |
| | Firewalls | 475 |
| | Investigating What SATAN Does | 477 |
| | SATAN's Information Gathering | 477 |
| | Vulnerabilities that SATAN Investigates | 478 |
| | Other Network Vulnerabilities | 488 |
| | Investigating IP Spoofing | 492 |
| | Examining Structural Internet Problems | 495 |
| | Rendezvous with SATAN | 499 |
| | Getting SATAN | 499 |
| | Examining the SATAN Files | 500 |

| | |
|--|------------|
| Building SATAN | 513 |
| Using SATAN's HTML Interface | 514 |
| Running a Scan | 524 |
| Understanding the SATAN Database Record Format | 525 |
| Understanding the SATAN Rulesets | 529 |
| Extending SATAN | 532 |
| Long-Term Benefits of Using SATAN | 534 |
| Works Cited..... | 534 |
| | |
| 9 Kerberos | 535 |
| How Kerberos Works | 536 |
| The Kerberos Network | 537 |
| RFCs | 538 |
| Goals of Kerberos | 538 |
| How Authentication Works | 539 |
| What Kerberos Doesn't Do | 542 |
| Encryption | 543 |
| Private, Public, Secret, or Shared Key Encryption..... | 544 |
| Private or Secret Key Encryption | 545 |
| DES and Its Variations | 545 |
| Encryption Export Issues | 547 |
| Encryption and Checksum Specifications | 548 |
| Versions of Kerberos | 555 |
| Versions of Kerberos V4 | 555 |
| Versions of Kerberos V5 | 556 |
| Bones | 556 |
| Selecting a Vendor | 557 |
| Vendor Interoperability Issues | 558 |
| DEC ULTRIX Kerberos | 558 |
| Transarc's Kerberos | 558 |
| DCE | 559 |
| Interoperability Requirements | 559 |
| Naming Constraints | 561 |
| Realm Names | 562 |
| Principal Names | 563 |
| Cross-Realm Operation | 564 |
| Ticket Flags | 566 |
| Initial and Preauthenticated Tickets | 567 |
| Invalid Tickets | 567 |
| Renewable Tickets | 567 |
| Postdated Tickets | 568 |

| | |
|---|-----|
| Proxiable and Proxy Tickets | 569 |
| Forwardable Tickets | 569 |
| Authentication Flags | 570 |
| Other Key Distribution Center Options | 570 |
| Message Exchanges | 571 |
| Tickets and Authenticators | 571 |
| The Authentication Service Exchange | 575 |
| The Ticket-Granting Service (TGS) Exchange | 578 |
| Specifications for the Authentication Server and Ticket Granting Service Exchanges | 584 |
| The Client/Server Authentication Exchange | 591 |
| Client/Server (CS) Message Specifications | 595 |
| The KRB_SAFE Exchange | 597 |
| KRB_SAFE Message Specification | 598 |
| The KRB_PRIV Exchange | 600 |
| KRB_PRIV Message Specification | 601 |
| The KRB_CRED Exchange | 602 |
| KRB_CRED Message Specification | 603 |
| Names | 605 |
| Time | 605 |
| Host Addresses | 605 |
| Authorization Data | 606 |
| Last Request Data | 606 |
| Error Message Specification | 607 |
| Kerberos Workstation Authentication Problem | 609 |
| Kerberos Port Numbers | 609 |
| Kerberos Telnet | 610 |
| Kerberos ftpd | 610 |
| Other Sources of Information | 611 |

Part III: Messaging: Creating a Secure Channel

| | |
|-------------------------------------|------------|
| 10 Encryption Overview | 615 |
| What Is Encryption? | 616 |
| Transposition | 617 |
| Deciphering | 619 |
| Substitution | 621 |
| Caesar Cipher | 621 |
| Monoalphabetic Substitutions | 624 |
| Vigenere Encryption | 628 |

| | |
|--|------------|
| 11 PGP | 633 |
| PGP Overview | 634 |
| History of PGP | 634 |
| Why Use PGP? | 635 |
| Short Encryption Review | 636 |
| PGP How-To | 637 |
| Before You Use PGP | 637 |
| Generate a PGP Key | 639 |
| Distributing the Public Key | 640 |
| Signing a Message | 641 |
| Adding Someone Else's Key | 642 |
| Encrypting a Message | 643 |
| Decrypting and Verifying a Message | 644 |
| PGP Keys | 645 |
| What's in a Name? | 646 |
| PGP Key Rings | 647 |
| The Web of Trust | 648 |
| Degrees of Trust | 649 |
| Key Management | 650 |
| Key Generation | 651 |
| Adding Keys to the Public Key Ring | 654 |
| Extracting Keys from the Public Key Ring | 656 |
| Signing Keys | 657 |
| Viewing the Contents of a Key Ring | 660 |
| Removing Keys and Signatures | 661 |
| Key Fingerprints and Verifying Keys | 663 |
| Revoking Your Key | 664 |
| Basic Message Operations | 665 |
| PGP: Program or Filter? | 665 |
| Compressing the Message | 666 |
| Processing Text and Binary Files | 666 |
| Sending PGP Messages via E-Mail | 667 |
| Conventional Encryption | 668 |
| Signing a Message | 668 |
| Encrypting a Message Using Public Key | 669 |
| Signing and Encrypting Messages | 670 |
| Decrypting and Verifying Messages | 671 |
| Advanced Message Operations | 673 |
| Clearsigning | 674 |
| Detached Signatures | 675 |
| For Her Eyes Only | 676 |
| Wiping Files | 676 |

| | |
|---|-----|
| The PGP Configuration File | 677 |
| Security of PGP | 682 |
| The Brute Force Attack | 682 |
| Secret Keys and Pass Phrases | 683 |
| Public Key Ring Attacks | 684 |
| Program Security | 685 |
| Other Attacks Against PGP | 685 |
| PGP Add-Ons | 686 |
| PGP Public Keyservers | 686 |
| PGPMenu: A Menu Interface to PGP for Unix | 687 |
| MITSign: A Kerberized PGP Key Signer | 687 |
| Windows Front-Ends | 688 |
| Unix Mailers | 688 |
| Mac PGP | 689 |

Part IV: Modern Concerns

| | |
|---|------------|
| 12 Java Security | 693 |
| Java's Functionality | 695 |
| Java Is Portable | 696 |
| Java Is Robust | 697 |
| Java Is Secure | 697 |
| Java Is Object-Oriented | 698 |
| Java Is High Performance | 698 |
| Java Is Easy | 699 |
| History of the Java Language | 699 |
| Main Features of the Java Environment | 701 |
| Features of the Java Language | 703 |
| The Java Architecture | 707 |
| From Class File to Execution | 712 |
| The Compilation of Code | 712 |
| Running Code | 715 |
| The Java Virtual Machine | 718 |
| Why a New Machine Code Specification? | 719 |
| The Java Virtual Machine Description | 719 |
| Setting Up Java Security Features | 724 |
| Using the Appletviewer | 724 |
| Netscape 2.0 | 727 |
| Other Issues in Using Java Programs | 729 |

| | |
|--|------------|
| 13 CGI Security | 731 |
| Introducing the CGI Interface | 732 |
| Why CGI Is Dangerous | 733 |
| How CGI Works | 733 |
| CGI Data: Encoding and Decoding | 734 |
| CGI Libraries | 735 |
| Understanding Vulnerabilities | 736 |
| The HTTP Server | 736 |
| The HTTP Protocol | 736 |
| The Environment Variables | 737 |
| GET and POST Input Data | 737 |
| Minimizing Vulnerability | 738 |
| Restrict Access to CGI | 739 |
| Run CGIs with Minimum Privileges | 739 |
| Execute in a chrooted Environment | 740 |
| Secure the HTTP Server Machine | 740 |
| CGIWrap: An Alternative Model | 740 |
| Advantages and Disadvantages | 741 |
| Bypassing CGI | 741 |
| Server Side Includes (SSI) | 742 |
| Restrict Access to SSI | 742 |
| Alternatives to SSI | 742 |
| Language Issues | 743 |
| PERL | 743 |
| C and C++ | 746 |
| Safe Languages | 746 |
| Protecting Sensitive Data | 747 |
| Logging | 749 |
| 14 Viruses | 751 |
| What Is a Computer Virus? | 752 |
| Most Likely Targets | 753 |
| Key Hardware | 754 |
| Key Software | 755 |
| Floppy Boot Records (FBRs) | 756 |
| Hard Drive Master Boot Record | 757 |
| Partition Boot Records | 758 |
| System Services | 760 |
| Program Files | 762 |
| Data Files with Macro Capabilities | 765 |

| | |
|---|-----|
| IBM PC Computer Virus Types | 767 |
| Boot Record Viruses | 767 |
| Floppy Boot Record Viruses | 768 |
| Partition Boot Record Viruses | 776 |
| Master Boot Record Viruses | 780 |
| Program File Viruses | 784 |
| SYS File Infections | 788 |
| Companion Viruses | 797 |
| Potential Damage by File Infecting Viruses | 798 |
| Macro Viruses | 800 |
| Worms | 802 |
| Network and Internet Virus Susceptibility | 803 |
| Network Susceptibility to File Viruses | 803 |
| Boot Viruses | 805 |
| Macro Viruses | 806 |
| Virus Classes | 806 |
| Polymorphic Viruses | 807 |
| Stealth Viruses | 808 |
| Slow Viruses | 812 |
| Retro Viruses | 813 |
| Multipartite Viruses | 814 |
| How Antivirus Programs Work | 814 |
| Virus Scanners | 815 |
| Memory Scanners | 820 |
| Integrity Checkers | 822 |
| Behavior Blockers | 825 |
| Heuristics | 826 |
| Preventative Measures and Cures | 827 |
| Preventing and Repairing Boot Record Viruses | 827 |
| Preventing and Repairing Executable File Viruses | 830 |
| Repairing Files Infected with a Read-Stealth Virus | 830 |
| Preventing and Repairing Macro Viruses | 832 |
| Profile: Virus Behavior under Windows NT | 832 |
| Master Boot Record Viruses under Windows NT | 832 |
| The NT Bootup Process with MBR Infection | 833 |
| Boot Record Viruses under Windows NT | 834 |
| Possible Damage Due to Boot Record Virus Infection | 835 |
| Windows NT Installation with Existing Boot Record Infection | 836 |
| MBR and Boot Record Viruses—The Bottom Line | 837 |

| | |
|--|-----|
| DOS File Viruses under a Windows NT DOS Box | 837 |
| Damage by File Viruses under a Windows NT DOS Box | 838 |
| File Virus Infections under Windows NT—Outside a DOS Box | 839 |
| DOS File Viruses under Windows NT—System Susceptibility during Bootup | 839 |
| DOS File Viruses—The Bottom Line | 839 |
| Windows 3.1 Viruses under Windows NT | 840 |
| Macro Viruses under Windows NT | 841 |
| Native Windows NT Viruses | 841 |

Part V: Appendixes

| | |
|---------------------------------------|------------|
| A Security Information Sources | 845 |
| CIAC | 846 |
| COAST | 846 |
| CERT | 846 |
| FIRST | 847 |
| 8lgm: Eight Little Green Men | 848 |
| bugtraq | 848 |
| Vendors | 848 |
| Others | 848 |
| B Internet Security References | 849 |
| Index | 855 |

INTRODUCTION INTRODUCTION INTRODUCTION
INTRODUCTION INTRODUCTION INTRODUCTION
INTRODUCTION INTRODUCTION INTRODUCTION

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!*