Computer Security

2nd Edition
Expanded & Updated

PRACTICAL UNIX & INTERNET SECURITY

Simson Garfinkel and Gene Spafford

O'Reilly & Associates, Inc.

Practical UNIX and Internet Security

Second Edition

Simson Garfinkel and Gene Spafford

O'Reilly & Associates, Inc.
Bonn · Cambridge · Paris · Sebastopol · Tokyo

Table of Contents

Preface ..... *xiii*

I: Computer Security Basics *1*

1: Introduction *3*

What Is Computer Security? 6

What Is an Operating System? 7

History of UNIX 8

Security and UNIX 15

Role of This Book 20

2: Policies and Guidelines *23*

Planning Your Security Needs 24

Risk Assessment 27

Cost-Benefit Analysis 30

Policy 35

The Problem with Security Through Obscurity 40

II: User Responsibilities *47*

3: Users and Passwords *49*

Usernames 49

Passwords 51

Entering Your Password 57

Changing Your Password 58
Verifying Your New Password 59
The Care and Feeding of Passwords 61
One-Time Passwords 67
Summary 68

4: Users, Groups, and the Superuser 71
Users and Groups 71
Special Usernames 78
su: Changing Who You Claim to Be 84
Summary 90

5: The UNIX Filesystem 91
Files 91
Using File Permissions 100
The umask 113
Using Directory Permissions 115
SUID 118
Device Files 128
chown: Changing a File's Owner 132
chgrp: Changing a File's Group 134
Oddities and Dubious Ideas 134
Summary 137

6: Cryptography 139
A Brief History of Cryptography 139
What Is Encryption? 142
The Enigma Encryption System 147
Common Cryptographic Algorithms 149
Message Digests and Digital Signatures 167
Encryption Programs Available for UNIX 175
des: The Data Encryption Standard 178
Encryption and U.S. Law 190

III: System Security *195*

7: Backups *197*
Make Backups! 198
Sample Backup Strategies 210
Backing Up System Files 215
Software for Backups 218

8: Defending Your Accounts *225*
Dangerous Accounts 225
Monitoring File Format 235
Restricting Logins 236
Managing Dormant Accounts 237
Protecting the root Account 243
The UNIX Encrypted Password System 246
One-Time Passwords 250
Administrative Techniques for Conventional Passwords 255

9: Integrity Management *271*
Prevention 273
Detecting Change 277
A Final Note 286

10: Auditing and Logging *289*
The Basic Log Files 290
The acct/pacct Process Accounting File 299
Program-Specific Log Files 302
Per-User Trails in the Filesystem 307
The UNIX System Log (syslog) Facility 309
Swatch: A Log File Tool 318
Handwritten Logs 321
Managing Log Files 324

11: Protecting Against Programmed Threats *327*
Programmed Threats: Definitions 327
Damage 337
Authors 338

Entry 339
Protecting Yourself 341
Protecting Your System 353

12: Physical Security 357
One Forgotten Threat 357
Protecting Computer Hardware 359
Protecting Data 375
Story: A Failed Site Inspection 386

13: Personnel Security 389
Background Checks 390
On the Job 391
Outsiders 395

IV: Network and Internet Security 397

14: Telephone Security 399
Modems: Theory of Operation 399
Serial Interfaces 401
The RS-232 Serial Protocol 401
Modems and Security 405
Modems and UNIX 411
Additional Security for Modems 419

15: UUCP 421
About UUCP 422
Versions of UUCP 426
UUCP and Security 427
Security in Version 2 UUCP 430
Security in BNU UUCP 437
Additional Security Concerns 444
Early Security Problems with UUCP 445
UUCP Over Networks 447
Summary 448

16: TCP/IP Networks *449*
Networking 449
IPv4: The Internet Protocol Version 4 453
IP Security 470
Other Network Protocols 477
Summary 478

17: TCP/IP Services *479*
Understanding UNIX Internet Servers 480
Controlling Access to Servers 484
Primary UNIX Network Services 485
Security Implications of Network Services 530
Monitoring Your Network with netstat 531
Network Scanning 534
Summary 535

18: WWW Security *537*
Security and the World Wide Web 537
Running a Secure Server 539
Controlling Access to Files on Your Server 549
Avoiding the Risks of Eavesdropping 555
Risks of Web Browsers 560
Dependence on Third Parties 563
Summary 564

19: RPC, NIS, NIS+, and Kerberos *565*
Securing Network Services 566
Sun's Remote Procedure Call (RPC) 567
Secure RPC (AUTH_DES) 570
Sun's Network Information Service (NIS) 579
Sun's NIS+ 587
Kerberos 594
Other Network Authentication Systems 603

20: NFS *605*
Understanding NFS 605
Server-Side NFS Security 616

Client-Side NFS Security 621
Improving NFS Security 622
Some Last Comments 631

V: Advanced Topics *635*

21: Firewalls *637*
What's a Firewall? 638
Building Your Own Firewall 648
Example: Cisco Systems Routers as Chokes 652
Setting Up the Gate 658
Special Considerations 664
Final Comments 666

22: Wrappers and Proxies *669*
Why Wrappers? 669
sendmail (smap/smapd) Wrapper 670
tcpwrapper 675
SOCKS 687
UDP Relayer 697
Writing Your Own Wrappers 698

23: Writing Secure SUID and Network Programs *701*
One Bug Can Ruin Your Whole Day 701
Tips on Writing Network Programs 713
Tips on Writing SUID/SGID Programs 716
Tips on Using Passwords 719
Tips on Generating Random Numbers 721

VI: Handling Security Incidents *729*

24: Discovering a Break-in *731*
Prelude 731
Discovering an Intruder 734
The Log Files: Discovering an Intruder's Tracks 746
Cleaning Up After the Intruder 747
An Example 752

Resuming Operation 755
Damage Control 756

25: Denial of Service Attacks and Solutions *759*
Destructive Attacks 760
Overload Attacks 760
Network Denial of Service Attacks 775

26: Computer Security and U.S. Law *779*
Legal Options After a Break-in 779
Criminal Prosecution 780
Civil Actions 789
Other Liability 791

27: Who Do You Trust? *799*
Can You Trust Your Computer? 799
Can You Trust Your Suppliers? 803
Can You Trust People? 810
What All This Means 814

VII: Appendixes *817*

A: UNIX Security Checklist *819*

B: Important Files *841*
Security-Related Devices and Files 841
Important Files in Your Home Directory 848
SUID and SGID Files 848

C: UNIX Processes *859*
About Processes 859
Creating Processes 868
Signals 869
The kill Command 871
Starting Up UNIX and Logging In 873

D: Paper Sources *877*
UNIX Security References 877

Other Computer References 878
Security Periodicals 889

E: Electronic Resources *893*
Mailing Lists 894
Usenet Groups 897
WWW Pages 898
Software Resources 899

F: Organizations *909*
Professional Organizations 909
U. S. Government Organizations 913
Emergency Response Organizations 914

G: Table of IP Services *925*

Index *937*

O'Reilly & Associates, Inc.

PRACTICAL UNIX & INTERNET SECURITY

When *Practical UNIX Security* was first published in 1991, it became an instant classic. Crammed with information about host security, it saved many a UNIX system administrator and user from disaster.

This second edition is a complete rewrite of the original book. It's packed with twice the pages and offers even more practical information for UNIX users and administrators. You'll find coverage of features of many types of UNIX systems, including SunOS, Solaris, BSDI, AIX, HP-UX, Digital UNIX, and Linux. The first edition was practical, entertaining, and full of useful scripts, tips, and warnings. This edition is all those things—and more.

Practical UNIX and Internet Security includes detailed coverage of Internet security and networking issues, including World Wide Web security, wrapper and proxy programs, integrity management tools, secure programming, and how to secure TCP/IP services (e.g., FTP, SMTP, DNS). Chapters on host security contain up-to-date details on passwords, the UNIX filesystem, cryptography, backups, logging, physical security, telephone security, UUCP, firewalls, and dealing with breakins. You'll also find extensive summary appendixes on freely available security tools, references, and security-related organizations.

Practical UNIX and Internet Security is the authoritative book covering every aspect of computer security on UNIX machines and the Internet. Don't even *think* of running a system without it!

"Buy this book and save on aspirin."

—*Cliff Stoll, Author of* The Cuckoo's Egg *and* Silicon Snake Oil

"This is exactly the type of practical, easy to follow book that system administrators need to stay one step ahead of the system crackers—if you have time to read only one security book, this should be it."

—*Kevin J. Ziese, Captain, United States Air Force;*
Chief, Countermeasures Development, AF Information Warfare Center

"The previous edition...was one of the first to seriously address the issues of security in a networked UNIX environment; with the explosive growth of the Internet since that time, plus the book's expanded coverage of cryptography, tools, new services, and protocols, the second edition will be an important part of any system administrator's bookshelf."

—*Alec Muffett, Network Security Consultant and Author of the* Crack *Program*

"This revised edition...ably chronicles the changing security world of the Internet, with a greatly increased emphasis on network security and firewalls. If you could only purchase one book on Internet security, this is the one you'd want."

—*Dan Farmer, Author of the* SATAN *and* COPS *Programs*

Printed on Recycled Paper

ISBN 1-56592-148-8