
THIRD EDITION

Practical Unix and Internet Security

*Simson Garfinkel, Gene Spajjard,
and Schwartz*

O'REILLY

Beijing • Cambridge • Farnham • Koln • Paris • Sebastopol • Taipei • Tokyo

Table of Contents

Preface.....	xiii
--------------	------

Part I. Computer Security Basics

1. Introduction: Some Fundamental Questions.....	3
What Is Computer Security?	5
What Is an Operating System?	6
What Is a Deployment Environment?	8
2. Unix History and Lineage.....	11
History of Unix	12
Security and Unix	23
Role of This Book	30
3. Policies and Guidelines.....	32
Planning Your Security Needs	33
Risk Assessment	35
Cost-Benefit Analysis and Best Practices	38
Policy	45
Compliance Audits	53
Outsourcing Options	54
The Problem with Security Through Obscurity	61

Part II. Security Building Blocks

4. Users, Passwords, and Authentication.	67
Logging in with Usernames and Passwords	68
The Care and Feeding of Passwords	76
How Unix Implements Passwords	82
Network Account and Authorization Systems	91
Pluggable Authentication Modules (PAM)	94
5. Users, Groups, and the Superuser.	98
Users and Groups	98
The Superuser (root)	105
The su Command: Changing Who You Claim to Be	109
Restrictions on the Superuser	117
6. Filesystems and Security.	122
Understanding Filesystems	122
File Attributes and Permissions	127
chmod: Changing a File's Permissions	136
The umask	142
SUID and SGID	145
Device Files	155
Changing a File's Owner or Group	157
7. Cryptography Basics.	161
Understanding Cryptography	161
Symmetric Key Algorithms	169
Public Key Algorithms	180
Message Digest Functions	187
8. Physical Security for Servers.	194
Planning for the Forgotten Threats	194
Protecting Computer Hardware	197
Preventing Theft	211
Protecting Your Data	216
Story: A Failed Site Inspection	226

9. Personnel Security.....	230
Background Checks	231
On the Job	233
Departure	236
Other People	237

Part III. Network and Internet Security

10. Modems and Dialup Security.....	241
Modems: Theory of Operation	242
Modems and Security	246
Modems and Unix	257
Additional Security for Modems	265
11. TCP/IP Networks.....	267
Networking	267
IP: The Internet Protocol	271
IP Security	290
12. Securing TCP and UDP Services.	305
Understanding Unix Internet Servers and Services	306
Controlling Access to Servers	314
Primary Unix Network Services	329
Managing Services Securely	389
Putting It All Together: An Example	399
13. Sun RPC.....	407
Remote Procedure Call (RPC)	408
Secure RPC (AUTH DES)	411
14. Network-Based Authentication Systems.....	421
Sun's Network Information Service (NIS)	422
Sun's NIS+	431
Kerberos	438
LDAP	447
Other Network Authentication Systems	453

15. Network Filesystems.....	456
Understanding NFS	457
Server-Side NFS Security	468
Client-Side NFS Security	473
Improving NFS Security	474
Some Last Comments on NFS	483
Understanding SMB	485
16. Secure Programming Techniques.....	498
One Bug Can Ruin Your Whole Day...	498
Tips on Avoiding Security-Related Bugs	505
Tips on Writing Network Programs	514
Tips on Writing SUID/SGID Programs	516
Using chroot()	519
Tips on Using Passwords	520
Tips on Generating Random Numbers	522

Part IV. Secure Operations

17. Keeping Up to Date ...	533
Software Management Systems	533
Updating System Software	538
18. Backups.....	544
Why Make Backups?	545
Backing Up System Files	561
Software for Backups	565
19. Defending Accounts.....	571
Dangerous Accounts	571
Monitoring File Format	583
Restricting Logins	584
Managing Dormant Accounts	586
Protecting the root Account	591
One-Time Passwords	595
Administrative Techniques for Conventional Passwords	600
Intrusion Detection Systems	613

20. Integrity Management	616
The Need for Integrity	616
Protecting Integrity	618
Detecting Changes After the Fact	622
Integrity-Checking Tools	630
21. Auditing, Logging, and Forensics	641
Unix Log File Utilities	642
Process Accounting: The acct/pacct File	664
Program-Specific Log Files	666
Designing a Site-Wide Log Policy	670
Handwritten Logs	673
Managing Log Files	67.6
Unix Forensics	677

Part V. Handling Security Incidents

22. Discovering a Break-in	683
Prelude	683
Discovering an Intruder	686
Cleaning Up After the Intruder	700
Case Studies	713
23. Protecting Against Programmed Threats	734
Programmed Threats: Definitions	735
Damage	746
Authors	747
Entry	749
Protecting Yourself	750
Preventing Attacks	762
24. Denial of Service Attacks and Solutions	767
Types of Attacks	767
Destructive Attacks	769
Overload Attacks	769
Network Denial of Service Attacks	787

25. Computer Crime	795
Your Legal Options After a Break-in	795
Criminal Hazards	801
Criminal Subject Matter	805
26. Who Do You Trust?	811
Can You Trust Your Computer?	811
Can You Trust Your Suppliers?	815
Can You Trust People?	823

Part VI. Appendixes

A. Unix Security Checklist	831
B. Unix Processes	850
C. Paper Sources	873
D. Electronic Resources	883
E. Organizations	896
Index	907