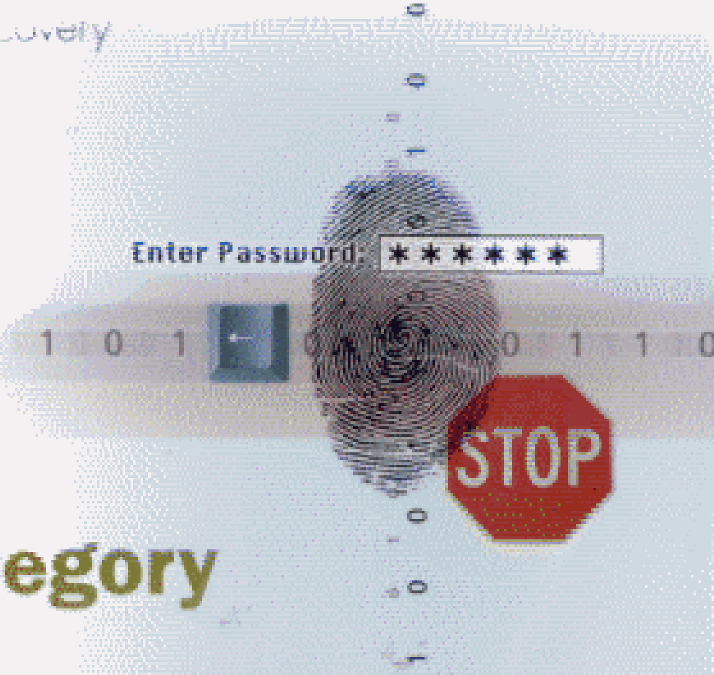
Foreword by Steven M. Bellovin

SOLARIS Security

- A concise guide to maintaining secure systems in the Solaris environment
- Covers standalone and networked systems running Solaris
- A special section on disaster preparations and recovery operations

SOLARIS

Sun microsystems



Peter H. Gregory

CONTENTS

List of Figures xxvii

List of Tables xxix

Foreword xxxi

Preface xxxv

Part One: Introduction 1

1 The Security Problem 3

Causes of Security Weaknesses 6

Growth of Network Connectivity 6

Software Vulnerabilities 7

Employees and Contractors 8

Motivated and Resourceful Hackers 9

Site Policies 9

2 The Security Paradigm 11

Principle 1: The Hacker Who Breaks into Your System Will Probably Be Someone You Know 11

Principle 2: Trust No One, *or* Be Careful About Whom You Are Required to Trust 12

Principle 2a: Don't Trust Yourself, *or* Verify Everything You Do 13

Principle 3: Make Would-Be Intruders Believe They Will Be Caught 14

Principle 4: Protect in Layers 14

Principle 5: While Planning Your Security Strategy, Presume the Complete Failure of Any Single Security Layer 15

Principle 6: Make Security a Part of the Initial Design 16

Principle 7: Disable Unneeded Services, Packages, and Features 17

Principle 8: Before Connecting, Understand and Secure 18

Principle 9: Prepare for the Worst 19

The Nine Principles: A Way of Life 19

Part Two: The Standalone System 21

3 The PROM, OpenBoot, and Physical Security 23

What Is the PROM? 23

What Is OpenBoot? 24

Why Users Must Be Kept Out of OpenBoot 24

Protecting OpenBoot by Setting Security Parameters 24

Procedures for Changing OpenBoot Security Levels 25

All Passwords Lost—Partial Recovery Procedure 26

Boot Device Recommendations 27

Change the OpenBoot Banner 27

Recover a Lost Root Password 28

Physical Security Considerations 30

Theft and Access Prevention 30

Audit PROMs 31

OpenBoot Passwords *31*

CD-ROM Drives *31*

Backup Media *31*

OS Release Media *32*

Where to Go for Additional Information 32

4 The Filesystem 33

What Is the Filesystem? 33

Some Applications Require Open Permissions *34*

Understanding File and Directory Permissions 35

Who: User, Group, and Other *35*

Permission Summary: Read, Write, Execute, SetUID, SetGID, Sticky Bit *35*

Putting It All Together: The Who and the What 39

How to View File and Directory Permissions 39

Permissions: Numeric Form *40*

Setting File and Directory Permissions—Numeric *42*

Setting File and Directory Permissions—Symbolic *43*

umask and How It Works 44

Default File Permissions and umask *45*

Root User umask *45*

Default Directory Permissions and umask *45*

How to Find Files with Specific Permission Settings *46*

System Device Access Permissions 46

Filesystem Auditing Tools 47

ASET *47*

COPS *49*

Tiger *49*

Tripwire *50*

lsof (list open files) *50*

Other Security Tools and Techniques 51

Check /etc *Permissions 51*

Ensure Proper utmp *and* utmpx *Permissions 51*

Use Fix-modes *Tool to Enhance Security 51*

Use the fuser *Command 52*

Use the ls *Command to Show Hidden Files and Hidden Characters in Filenames 52*

Alias the rm *Command 53*

Randomize Filesystem Inode Numbers with fsirand *54*

Filesystem Quotas 54

Filesystem Access Control Lists 55

Where to Go for Additional Information 57

5 User Accounts and Environments 59

Introduction 59

User Account Security 60

The Root Account 60

Other Administrative Accounts and Groups 61

User Accounts 62

When Users Need Root Privileges 62

PATH and LD_LIBRARY_PATH 62

The Password, Shadow, and Group Files 63

Password File 63

Shadow File 63

Password Security 64

UNIX Groups 65

The /etc/default/passwd *File 67*

Root Access 67

Direct Root Login 67

The su *Command 68*

Shell and Application Security 70

Forced Application Startup 70

Include System Name in Root Shell Prompt 70

Restricted Shell 71

Default Login Environment 72

Writing Directly to the Console 72

Program Buffer Overflow 73

Additional Process Information 73

X-Windows Security 73

X-Windows Screen Lock, Manual 74

X-Windows Screen Lock, Auto 75

X-Windows Display Permissions 75

Auditing Tools 77

COPS 77

Crack 77

Where to Go for Additional Information 78

6 System Startup and Shutdown 79

System Run Levels 79

Determining Current Run Level 80

System Startup 82

PROM 82

init *82*

Multiuser Mode 82

The rc Mechanism 82

System Shutdown 83

init 84

uadmin 84

More Information on rc Files 84

An Example rc *File Examined 85*

Auditing Startup and Shutdown Mechanisms 86

COPS 86

Tripwire 87

Modifying Startup and Shutdown Mechanisms 87

Adding Startup and Shutdown Scripts 87

Changing Startup and Shutdown Scripts 87

Disabling Startup and Shutdown Scripts 88

More on Linked Startup Files 88

Where to Go for Additional Information 89

7 *cron* and *at* 91

cron 91

What is cron*? 91*

How cron *Works 93*

How cron *Is Configured 93*

cron *User Configuration 93*

User Access to cron *System 94*

at 95

What Is at*? 95*

How at *Works 95*

User Access to at *System 95*

Common Mistakes to Avoid 96

Failure to Adequately Conceal Programs Launched by cron *96*

Leaving crontab *Files Lying Around for All to See 96*

Unsecure PATH *Elements in Scripts Launched by* cron *96*

Indeterminate PATH Elements in Scripts Launched by cron *96*

Use of stdin *and* stdout *in* cron *and* at *Jobs 97*

Auditing Tools 97

Tripwire *97*

COPS *97*

Where to Go for Additional Information 98

8 System Logs 99

What Is a System Log 99

syslog 100

syslog *Facilities and Severity Levels* *100*

syslog *Message Classification Notation* *101*

syslog *Configuration* *101*

Debugging syslog *103*

loginlog 105

sulog 106

Last Log 106

Volume Manager Log 107

Install Log 107

sysidtool Log 107

Tools to Help with Logging 107

Logcheck *107*

Where to Go for Additional Information 109

Part Three: The Network-Connected System ***111***

9 Network Interfaces and Services 113

Networks 113

Network Interfaces 114

Network Interface Characteristics *114*

Network Interface Configuration 115

ifconfig *115*

ndd *116*

Turn Off IP Forwarding with /etc/notrouter *118*

netstat *119*

/etc/inet/hosts *121*

/etc/inet/netmasks *121*

/etc/defaultrouter *122*

/etc/nodename *122*

/etc/hostname.interface *122*

How Adaptors Are Configured *122*

Promiscuous Mode *123*

Network Services 124

Unnecessary Services *124*

Network Service Numbers *124*

Network Service Configuration *124*

How Network Services Are Started *126*

Daemon Network Services Not Started with inetd *127*

Routing 128

Adding Static Routes *129*

Adding Dynamic Routes *129*

Using *snoop* 130

Where to Go for Additional Information 132

10 Network/System Architecture 133

What Is an Architecture? 133

Simple vs. Complex Architectures 134

Architecture Principles 134

Principle 1: Minimize the Number of Failure Points (or *Shorten the Critical Path)* 135

Principle 2: Keep Services Close to Those Being Served 136

Principle 3: Vertically Align Services with Their Applications 136

Principle 4: Prepare for Increasing Network Partitioning 137

11 Electronic Mail 139

Overview of E-Mail 139

Transport Agent 140

Delivery Agent 140

User Agent 140

Types of E-Mail Security Weaknesses 141

Auth *(or* Identd*) Protocol* 141

Message Brokering 142

Message Source Routing 143

Privacy 143

Authenticity 144

Mitigating E-Mail Security Weaknesses 144

Run Sendmail *Only on Mail Servers* 144

Disconnect Inside Mail Server(s) from the Internet 146

Prevent Message Source Routing 148

Implement Mail Encryption and Digital Signatures 148

Replace Sendmail 149

Remove Unnecessary E-Mail Aliases 150

Implement Smrsh 151

Implement ForwardPath 151

Where to Go for Additional Information 152

12 Printing 153

Printing Architectures 153

Print Subsystem Directories 154

Auditing Print Subsystem Directories 154

Local Printing 154

Local Print Devices 155

How to Determine Which Device a Specific Printer Uses 155

Print Device Permissions 155

Auditing Print Device Permissions 156

Restricting Access to Printers and Print Servers 156

Direct Access to Network Printers 157

Where to Go for Additional Information 157

13 Network Access Control 159

Network Access Control Principles 159

Unnecessary Network Access Points Are Security Risks 160

Unguarded Network Access Points Are Security Risks 160

Necessary and Unnecessary Services 160

How to Disable Unnecessary Services 166

Strengthening Network Access Control 166

inetd *Connection Tracing 167*

TCP Wrappers 168

Public-Domain rpcbind *169*

.rhosts *File—Gateway to the r-Commands 169*

/etc/hosts.equiv *File 170*

Auditing .rhosts *and* hosts.equiv *Files 170*

Secure Replacement for telnet, rsh, *and* rlogin *171*

ftp *171*

tftp *172*

X-Windows Is Unsecure 172

Firewalls 173

Testing System Accessibility 173

Satan 174

ISS 174

Intrusion Detection 174

Syn 175

Klaxon 175

Courtney 175

Tocsin 175

Gabriel 175

Intrusion Detection: Staying Current 176

Authentication 176

System Authentication 176

DH Authentication 176

Kerberos Authentication 177

Virtual Private Networks 178

SKIP 178

IPsec 178

Where to Go for Additional Information 179

14 Name Services 181

Domain Name Service (DNS) 181

/etc/nsswitch.conf 183

/etc/resolv.conf 184

DNS Security Weaknesses and Solutions 184

Too Much Information Visible to the Internet 184

Illicit Zone Transfers from DNS Servers 187

Differences Between nslookup and Actual DNS Queries 187

Public-Domain DNS (BIND) 188

DIG Public-Domain Tool *188*

Disable nscd *Caching* *188*

Know Your BIND Version *188*

NIS 189

Obtaining and Installing NISKIT *190*

NIS Security Weaknesses and Solutions 191

Move NIS Maps out of /etc *Directory* *191*

Protect NIS Maps Directory *191*

Use a Hard-to-Guess NIS Domain Name *191*

Implement /var/yp/securenets *191*

Hide Shadow Fields *192*

Avoid Illicit NIS Servers *192*

Keep Root and Other Administrative Accounts out of NIS *193*

Disable nscd *Caching* *193*

Other NIS Weaknesses *193*

NIS+ 194

NIS+ Default Access Rights *194*

Access Rights for Principal ***nobody*** *195*

NIS+ Security Level *195*

Administering NIS+ *196*

Back Up NIS+ Tables *196*

Flush NIS+ Transactions *197*

Keep Root and Other Administrative Accounts Out of NIS+ *197*

Disable nscd *Caching* *197*

Name Service Switch 197

nscd 198

Where to Go for Additional Information 200

15 NFS and the Automounter 203

NFS 204

NFS Operations 204

Improving Security with NFS Share 204

Improving Security with NFS Mount 206

Improving Security by Setting NFS Portmon 207

NFS Authentication 207

Servers as NFS Clients 208

NFS and Access Control Lists 208

NFS on the Network 209

Disabling NFS 209

Automounter 209

Indirect Automounter Maps 210

Direct Automounter Maps 210

Automounter Browsing 211

Automounter and the Name Service Switch 213

Disabling Automounter 213

Where to Go for Additional Information 213

Part Four: Disaster and Recovery 215

16 System Recovery Preparation 217

What Can and Will Go Wrong 217

Natural Disaster 217

Man-Made Disaster 218

Inside Utility Failure 218

Hardware Failure 218

UNIX Administrator Error 218

Documentation Error 218

Programmer Error 219
User Error 219
Sabotage 219
Preparing for Recovery 219
Create an Incident Reponse Team 220
System Filesystem Design 220
Filesystem Geometry 221
Tape Backups 221
System Recovery Testing 222
Release Media 222
System Event Logbooks 223
Solaris and Tool Patches 223
CD-ROM Drives 223
Hardware and Software Service Agreements 223
Keep Hardware Spares 224
Copies of Critical Server PROMs 224
Disk Space to Spare 225
Recovery Documentation 225
Contacts and Cross-Training 225
Partner with Inside Suppliers 226
Partner with Outside Suppliers 226
Where to Go for Additional Information 226

Part Five: Appendices 227

A Online Sources for Security Information 229
Security Web Sites 229
Hacker Web Sites 230

Security Mailing Lists 231

Patches 231

B Online Sources for Public-Domain Security Tools 233

TCP/IP Security Tools 233

ISS (Internet security scan) 233

Satan (Security Administrator's Tool for Analyzing Networks) 233

cpm (check promiscuous mode) 234

tcpdump (network monitoring and data acquisition) 234

Access Control Security Tools 234

TCP Wrappers 234

rpcbind 234

Ssh (secure shell) 234

Kerberos 234

crack (password cracker) 234

fwtk (firewall toolkit) 235

S/Key 235

Intrusion Detection Tools 235

Klaxon 235

Courtney 235

Tocsin 235

Gabriel 235

syn 235

Filesystem Security Tools 236

Tiger 236

Tripwire 236

COPS 236

Encryption Tools 236

PGP 236

MD5 236

E-Mail Security Tools 236

SMAP (sendmail *wrapper) 236*

sendmail *V8 (public-domain* sendmail*) 236*

Postfix (formerly Vmailer) 237

smrsh 237

DNS Tools 237

Public-Domain BIND 237

Dig 237

Other DNS Tools 237

Other Tools and Sources 237

logcheck 237

lsof (list open files) 237

Patchdiag 238

fix-modes 238

perl 238

Washington University ftpd 238

Security Tools Sites 238

CERT Tools 238

CIAC Tools 238

COAST Tools 238

Doug's Tools 239

LIST (Laboratory for Information Security Technology) Security Tools 239

Sun Freeware Site 239

Wietse Venema's UNIX Security Tools Collection 239

Hacker Tools Sites 239

C Obtaining and Applying Solaris Patches 241

Sources for Patch Information 241

Understanding Solaris Patches 242

Understanding Solaris Patch Clusters 242

Sources for Patches 243

Patch Installation Strategies 243

Before Installing Patches 243

Which Patches to Install 244

Testing Patches 244

For Patches Requiring System Reboot 245

The patchdiag *Program 245*

Patch Installation Procedure, Solaris 2.x—2.5.1 245

Patch Installation Procedures for Solaris 2.6 and Solaris 7 246

Solaris OS Upgrades 247

Where to Go for Additional Information 248

D Suggested Reading 249

Books 249

Publications and Articles Available Online 250

SunSolve Publications 251

Periodicals Online 252

Internet RFCs 253

E Solaris Security Products 255

SunScreen EFS 255

SunScreen SPF 255

SunScreen SKIP 256

Sun Security Manager 256

SunScreen SecureNet 256

Trusted Solaris 256

Where to Go for Additional Information 257

F Implementing C2 Security 259

What Is C2 Security? 259

Implications of C2 Security 259

Enabling C2 Security 260

Disabling C2 Security 260

Managing C2 Security 261

Configuration of C2 Audit Capture 261

Management of C2 Logs 261

Management of Performance 262

Audit Events 262

Audit Trail Analysis 262

Removable Media Management 262

Device Allocation 263

Recommendations 263

Where to Go for Additional Information 263

G Verifying the Integrity of Public-Domain Software 265

Verification Using PGP 265

Verification Using MD5 268

Where to Go for Additional Information 269

H Glossary of Attacks 271

I Secure System Checklist 279

Index 283