Table of Content

Table of Content ii
Preface vii
Protect Your Network with SSH vii
Intended Audience vii
Reading This Book viii
Our Approach ix
Which Chapters Are for You? ix
Supported Platforms x
Disclaimers x
Conventions Used in This Book x
Comments and Questions xi
Acknowledgments xi
Chapter 1. Introduction to SSH 1
1.1 What Is SSH? 1
1.2 What SSH Is Not 2
1.3 The SSH Protocol 3
1.4 Overview of SSH Features 5
1.5 History of SSH 8
1.6 Related Technologies 10
1.7 Summary 14
Chapter 2. Basic Client Use 15
2.1 A Running Example 15
2.2 Remote Terminal Sessions with ssh 15
2.3 Adding Complexity to the Example 17
2.4 Authentication by Cryptographic Key 20
2.5 The SSH Agent 25
2.6 Connecting Without a Password or Passphrase 29
2.7 Miscellaneous Clients 30
2.8 Summary 32
Chapter 3. Inside SSH 33
3.1 Overview of Features 33
3.2 A Cryptography Primer 35
3.3 The Architecture of an SSH System 38
3.4 Inside SSH-1 40
3.5 Inside SSH-2 56
3.6 As-User Access (userfile) 67
3.7 Randomness 67
3.8 SSH and File Transfers (scp and sftp) 69
3.9 Algorithms Used by SSH 72
3.10 Threats SSH Can Counter 78
3.11 Threats SSH Doesn't Prevent 80
3.12 Summary 83
Chapter 4. Installation and Compile-Time Configuration 84
4.1 SSH1 and SSH2 84
4.2 F-Secure SSH Server 102
4.3 OpenSSH 103

4.4 Software Inventory 106
4.5 Replacing R-Commands with SSH 107
4.6 Summary 110
Chapter 5. Serverwide Configuration 111
5.1 The Name of the Server 111
5.2 Running the Server 112
5.3 Server Configuration: An Overview 114
5.4 Getting Ready: Initial Setup 118
5.5 Letting People in: Authentication and Access Control 132
5.6 User Logins and Accounts 151
5.7 Subsystems 153
5.8 History, Logging, and Debugging 154
5.9 Compatibility Between SSH-1 and SSH-2 Servers 163
5.10 Summary 164
Chapter 6. Key Management and Agents 165
6.1 What Is an Identity? 166
6.2 Creating an Identity 168
6.3 SSH Agents 175
6.4 Multiple Identities 192
6.5 Summary 194
Chapter 7. Advanced Client Use 196
7.1 How to Configure Clients 196
7.2 Precedence 205
7.3 Introduction to Verbose Mode 205
7.4 Client Configuration in Depth 206
7.5 Secure Copy with scp 233
7.6 Summary 241
Chapter 8. Per-Account Server Configuration 242
8.1 Limits of This Technique 242
8.2 Public Key-Based Configuration 243
8.3 Trusted-Host Access Control 259
8.4 The User rc File 260
8.5 Summary 260
Chapter 9. Port Forwarding and X Forwarding 261
9.1 What Is Forwarding? 262
9.2 Port Forwarding 262
9.3 X Forwarding 280
9.4 Forwarding Security: TCP-wrappers and libwrap 290
9.5 Summary 295
Chapter 10. A Recommended Setup 296
10.1 The Basics 296
10.2 Compile-Time Configuration 296
10.3 Serverwide Configuration 297
10.4 Per-Account Configuration 301
10.5 Key Management 301
10.6 Client Configuration 302
10.7 Remote Home Directories (NFS, AFS) 302
10.8 Summary 304
Chapter 11. Case Studies 305
11.1 Unattended SSH: Batch or cron Jobs 305

11.2 FTP Forwarding 310
11.3 Pine, IMAP, and SSH 327
11.4 Kerberos and SSH 333
11.5 Connecting Through a GatewayHost 349
Chapter 12. Troubleshooting and FAQ 356
12.1 Debug Messages: Your First Line of Defense 356
12.2 Problems and Solutions 358
12.3 Other SSH Resources 373
12.4 Reporting Bugs 375
Chapter 13. Overview of Other Implementations 376
13.1 Common Features 376
13.2 Covered Products 376
13.3 Table of Products 377
13.4 Other SSH-Related Products 383
Chapter 14. SSH1 Port by Sergey Okhapkin (Windows) 384
14.1 Obtaining and Installing Clients 384
14.2 Client Use 388
14.3 Obtaining and Installing the Server 388
14.4 Troubleshooting 390
14.5 Summary 391
Chapter 15. SecureCRT (Windows) 392
15.1 Obtaining and Installing 392
15.2 Basic Client Use 392
15.3 Key Management 393
15.4 Advanced Client Use 394
15.5 Forwarding 395
15.6 Troubleshooting 397
15.7 Summary 398
Chapter 16. F-Secure SSH Client (Windows, Macintosh) 399
16.1 Obtaining and Installing 399
16.2 Basic Client Use 399
16.3 Key Management 400
16.4 Advanced Client Use 401
16.5 Forwarding 403
16.6 Troubleshooting 405
16.7 Summary 406
Chapter 17. NiftyTelnet SSH (Macintosh) 407
17.1 Obtaining and Installing 407
17.2 Basic Client Use 408
17.3 Troubleshooting 409
17.4 Summary 410
Appendix A. SSH2 Manpage for sshregex 411
Appendix B. SSH Quick Reference 414
2.1 Legend 414
2.2 sshd Options 414
2.3 sshd Keywords 415
2.4 ssh and scp Keywords 419
2.5 ssh Options 421
2.6 scp Options 422
2.7 ssh-keygen Options 423

2.8 ssh-agent Options 424
2.9 ssh-add Options 424
2.10 Identity and Authorization Files 424
2.11 Environment Variables 425
Colophon 426