

SECOND EDITION

SSH, the Secure Shell

The Definitive Guide

*Daniel J. Barrett, Richard E. Silverman,
and Robert G. Byrnes*

O'REILLY®

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

Table of Contents

Preface	xi
1. Introduction to SSH	1
1.1 What Is SSH?	1
1.2 What SSH Is Not	3
1.3 The SSH Protocol	3
1.4 Overview of SSH Features	5
1.5 History of SSH	9
1.6 Related Technologies	10
1.7 Summary	15
2. Basic Client Use	16
2.1 A Running Example	16
2.2 Remote Terminal Sessions with ssh	16
2.3 Adding Complexity to the Example	18
2.4 Authentication by Cryptographic Key	21
2.5 The SSH Agent	28
2.6 Connecting Without a Password or Passphrase	32
2.7 Miscellaneous Clients	33
2.8 Summary	34
3. Inside SSH	36
3.1 Overview of Features	36
3.2 A Cryptography Primer	39
3.3 The Architecture of an SSH System	43
3.4 Inside SSH-2	45
3.5 Inside SSH-1	68

3.6	Implementation Issues	69
3.7	SSH and File Transfers (scp and sftp)	81
3.8	Algorithms Used by SSH	84
3.9	Threats SSH Can Counter	91
3.10	Threats SSH Doesn't Prevent	93
3.11	Threats Caused by SSH	97
3.12	Summary	98
4.	Installation and Compile-Time Configuration	99
4.1.	Overview	99
4.2	Installing OpenSSH	106
4.3	Installing Tectia	111
4.4	Software Inventory	124
4.5	Replacing r-Commands with SSH	125
4.6	Summary	127
5.	Serverwide Configuration	128
5.1	Running the Server	129
5.2	Server Configuration: An Overview	132
5.3	Getting Ready: Initial Setup	141
5.4	Authentication: Verifying Identities	171
5.5	Access Control: Letting People In	184
5.6	User Logins and Accounts	198
5.7	Forwarding	201
5.8	Subsystems	206
5.9	Logging and Debugging	209
5.10	Compatibility Between SSH-1 and SSH-2 Servers	223
5.11	Summary	226
6.	Key Management and Agents	227
6.1	What Is an Identity?	227
6.2	Creating an Identity	233
6.3	SSH Agents	242
6.4	Multiple Identities	260
6.5	PGP Authentication in Tectia	262
6.6	Tectia External Keys	264
6.7	Summary	265

7. Advanced Client Use	266
7.1 How to Configure Clients	266
7.2 Precedence	276
7.3 Introduction to Verbose Mode	277
7.4 Client Configuration in Depth	278
7.5 Secure Copy with scp	313
7.6 Secure, Interactive Copy with sftp	323
7.7 Summary	325
8. Per-Account Server Configuration	326
8.1 Limits of This Technique	326
8.2 Public-Key-Based Configuration	328
8.3 Hostbased Access Control	346
8.4 The User rc File	348
8.5 Summary	348
9. Port Forwarding and X Forwarding	349
9.1 What Is Forwarding?	350
9.2 Port Forwarding	351
9.3 Dynamic Port Forwarding	373
9.4 X Forwarding	377
9.5 Forwarding Security: TCP-wrappers and libwrap	389
9.6 Summary	395
10. A Recommended Setup	396
10.1 The Basics	396
10.2 Compile-Time Configuration	397
10.3 Serverwide Configuration	397
10.4 Per-Account Configuration	403
10.5 Key Management	404
10.6 Client Configuration	404
10.7 Remote Home Directories (NFS, AFS)	404
10.8 Summary	407
11. Case Studies	408
11.1 Unattended SSH: Batch or cron Jobs	408
11.2 FTP and SSH	415
11.3 Pine, IMAP, and SSH	436
11.4 Connecting Through a Gateway Host	444

11.5 Scalable Authentication for SSH	452
11.6 Tectia Extensions to Server Configuration Files	468
11.7 Tectia Plugins	479
12. Troubleshooting and FAQ	495
12.1 Debug Messages: Your First Line of Defense	495
12.2 Problems and Solutions	497
12.3 Other SSH Resources	513
13. Overview of Other Implementations	515
13.1 Common Features	515
13.2 Covered Products	516
13.3 Other SSH Products	516
14. OpenSSH for Windows	521
14.1 Installation	521
14.2 Using the SSH Clients	522
14.3 Setting Up the SSH Server	522
14.4 Public-Key Authentication	524
14.5 Troubleshooting	525
14.6 Summary	525
15. OpenSSH for Macintosh	526
15.1 Using the SSH Clients	526
15.2 Using the OpenSSH Server	526
16. Tectia for Windows	531
16.1 Obtaining and Installing	532
16.2 Basic Client Use	533
16.3 Key Management	534
16.4 Accession Lite	536
16.5 Advanced Client Use	539
16.6 Port Forwarding	542
16.7 Connector	543
16.8 File Transfers	551
16.9 Command-Line Programs	552
16.10 Troubleshooting	554
16.11 Server	555

17. SecureCRT and SecureFX for Windows	563
17.1 Obtaining and Installing	563
17.2 Basic Client Use	564
17.3 Key Management	564
17.4 Advanced Client Use	568
17.5 Forwarding	570
17.6 Command-Line Client Programs	572
17.7 File Transfer	572
17.8 Troubleshooting	574
17.9 VShell	574
17.10 Summary	575
18. PuTTY for Windows	576
18.1 Obtaining and Installing	576
18.2 Basic Client Use	576
18.3 File Transfer	578
18.4 Key Management	580
18.5 Advanced Client Use	583
18.6 Forwarding	587
18.7 Summary	589
A. OpenSSH 4.0 New Features	591
B. Tectia Manpage for sshregex	595
C. Tectia Module Names for Debugging	604
D. SSH-1 Features of OpenSSH and Tectia	609
E. SSH Quick Reference	612
Index	629