

Inhaltsverzeichnis

I Grundlagen	3
1 Ziel dieses Buches	5
2 Einführung	11
2.1 Meine Daten sind sicher – oder?	11
2.1.1 Authentifizierung	12
2.1.2 Vertraulichkeit	13
2.1.3 Integrität	14
2.1.4 Nichtabstreitbarkeit	15
2.1.5 Autorisierung	15
2.2 Die Secure Shell stellt sich vor	15
2.2.1 Leistungsumfang	17
2.2.2 Grenzen und Nachteile	21
2.2.3 Lizenzierung	23
2.2.4 Secure Shell Produkte und Plattformen	23
2.2.4.1 Dropbear	25
2.2.4.2 freeSSHd	25
2.2.4.3 GNU SSH: lsh	25
2.2.4.4 MacSSH	25
2.2.4.5 MindTerm	26
2.2.4.6 OpenSSH	26
2.2.4.7 PuTTY	30

2.2.4.8	SecureCRT	31
2.2.4.9	Tectia Secure Shell	31
2.2.4.10	WinSCP	32
2.2.5	Die Zukunft der Secure Shell	32
2.2.6	Zusammenfassung: Secure Shell	32
2.3	Geschichte	33
2.4	Verwandte Technologien	34
2.4.1	Internet Protocol Security	34
2.4.2	r-Kommandos	36
2.4.3	Kerberos	38
2.4.4	Firewalls	38
2.4.5	Secure Socket Layer/Transport Layer Security	39
2.4.6	OpenPGP	41
2.5	Zusammenfassung	41
3	Allgemeine Grundlagen	43
3.1	Kryptographische Grundlagen	43
3.1.1	Kryptographische Algorithmen und Schlüssel	44
3.1.2	Symmetrische Verfahren	48
3.1.3	Asymmetrische Verfahren	51
3.1.4	Hybridverfahren	53
3.1.5	Hash-Funktionen und Message Authentication Codes	55
3.1.5.1	Hash-Funktionen	56
3.1.5.2	Message Authentication Codes	57
3.1.6	Digitale Signatur	58
3.1.7	Schlüsselaustausch	62
3.1.8	Kryptoanalytische Verfahren	64
3.1.9	Anforderungen an Kryptosysteme	67
3.1.10	Kompromittierung kryptographischer Schlüssel	69
3.1.11	Verschlüsselung durch SSH	70
3.1.12	Zusammenfassung: Kryptographie im Schnelldurchlauf	74
3.2	Referenzmodelle und Protokolle	76
3.2.1	Protokollarchitekturen und Schichtenmodelle	77

3.2.2	Das ISO/OSI-Referenzmodell	80
3.2.3	TCP/IP-Referenzmodell	84
3.2.3.1	Protokollarchitektur	84
3.2.3.2	Netzzugangsschicht	85
3.2.3.3	Internet-Schicht	85
3.2.3.4	Transportschicht	87
3.2.3.5	Anwendungsschicht	90
3.2.4	ISO/OSI und TCP/IP im Vergleich	90
3.2.5	Zusammenfassung	92
3.3	Angriffsmethoden im Netz	93
3.3.1	Sitzungsübernahme/Sitzungsabbruch	94
3.3.1.1	Man-in-the-middle	95
3.3.1.2	IP Adreßfälschung	96
3.3.2	Replay	100
3.3.3	DNS-Fälschung	100
3.3.4	IP source routing	102
3.3.5	Zusammenfassung	103
3.4	Die Secure Shell in der Netzwerkwelt	104
3.4.1	Sicherheit auf unterschiedlichen Schichten	104
3.4.2	Secure Shell	106
3.4.3	Zusammenfassung	107
4	Die Secure Shell im Überblick		109
4.1	Protokolldefinition	110
4.1.1	Der Internet-Standardisierungsprozeß	111
4.1.2	Secure Shell Protokolle	111
4.2	Grundsätze	112
4.3	Komponenten und ihr Zusammenspiel	114
5	SSHv1: Die Grundlagen		117
5.1	Protokollstruktur	117
5.1.1	Verschlüsselung	120
5.1.2	Prüfsummenbildung	120

5.2	Protokollablauf	121
5.2.1	Verbindungsaufbau und -abbau	122
5.2.2	Authentifizierungsmethoden	126
5.2.2.1	Server-Host-Authentifizierung	126
5.2.2.2	Client-Authentifizierung	127
5.2.3	Authentifizierungsagenten	134
5.2.4	Datenaustausch und interaktive Sitzungen	136
5.3	Überlegungen zur Sicherheit	137
5.4	Schwächen in SSHv1	139
5.4.1	Zugangskontrolle und Authentifizierung	140
5.4.2	Integrität von Daten	140
5.4.3	Umleitung von Verbindungen	141
5.5	Zusammenfassung: SSHv1	143
6	SSHv2: Die Grundlagen	145
6.1	Protokollstruktur	145
6.1.1	Teilprotokolle	148
6.1.1.1	SSH Protocol Architecture	150
6.1.1.2	SSH Transport Layer Protocol	150
6.1.1.3	SSH Authentication Protocol	151
6.1.1.4	SSH Connection Protocol	151
6.1.1.5	SSH File Transfer Protocol	152
6.1.1.6	URI Scheme for SFTP and Secure Shell (SSH)	152
6.1.1.7	Generic Message Exchange Authentication	153
6.1.1.8	Secure Shell Authentication Agent Protocol	153
6.1.1.9	Secure Shell Public-Key Subsystem	154
6.1.1.10	SSH Public Key File Format	154
6.1.1.11	SSH Transport Layer Encryption Modes	155
6.1.1.12	GSSAPI Authentication and Key Exchange for the Secure Shell Protocol	155
6.1.1.13	Using DNS to Securely Publish SSH Key Fingerprints	156
6.1.1.14	Diffie-Hellman Group Exchange for the SSH Transport Layer Protocol	156

6.1.1.15	Session Channel Break Extension	. . .	156
6.1.1.16	SSH Protocol Assigned Numbers	. . .	157
6.1.1.17	X.509 authentication in SSHv2	. . .	157
6.1.2	Paketaufbau	157
6.1.3	Host-Schlüssel	159
6.1.3.1	Überprüfung der Schlüssel	160
6.1.3.2	Kommunikation ohne Host-Schlüssel	160
6.1.4	Verbindungsaufbau	161
6.1.5	Verbindungseigenschaften	163
6.1.6	Auffinden von Ressourcen	163
6.1.6.1	SSH-URLs	164
6.1.6.2	SFTP-URLs	165
6.1.6.3	Hinweise zur Sicherheit	166
6.1.7	Abwärtskompatibilität	167
6.1.8	Erweiterbarkeit	167
6.1.9	Subsysteme	169
6.1.10	Zusammenfassung: SSHv2-Protokollstruktur	169
6.2	Das Transportprotokoll	170
6.2.1	Aushandlung von Verfahren	171
6.2.2	Vertraulichkeit	172
6.2.3	Integrität	174
6.2.4	Kompression	175
6.2.5	Schlüsselaustausch	175
6.2.5.1	Erneuter Schlüsselaustausch	176
6.2.5.2	Schlüsselbestimmung	177
6.2.5.3	Ablauf des Schlüsselaustauschs	178
6.2.6	Public-Key-Verfahren	181
6.2.7	Dienstanfrage	182
6.2.8	Meldungen	183
6.2.9	Sicherheit des Transportprotokolls	183
6.2.10	Zusammenfassung: Transportprotokoll	185
6.3	Das Authentifizierungsprotokoll	186

6.3.1	Ablauf der Authentifizierung	186
6.3.1.1	Authentifizierungsanfrage	186
6.3.1.2	Authentifizierungsantwort	188
6.3.2	Authentifizierungsmethoden	189
6.3.2.1	Authentifizierungsmethode publickey	190
6.3.2.2	Authentifizierungsmethode password	192
6.3.2.3	Authentifizierungsmethode hostbased	193
6.3.2.4	Authentifizierungsmethode keyboard-interactive	195
6.3.2.5	Authentifizierungsmethoden in GSSAPI	197
6.3.3	Sicherheit des Authentifizierungsprotokolls	201
6.3.4	Zusammenfassung: Authentifizierungsprotokoll	204
6.4	Das Verbindungsprotokoll	204
6.4.1	Kanäle	205
6.4.2	Interaktive Sitzungen	207
6.4.2.1	Aufbau einer Sitzung	207
6.4.2.2	Umgebungsvariablen	207
6.4.2.3	Starten einer Shell oder Anwendung	207
6.4.3	TCP/IP-Port-Weiterleitung	208
6.4.3.1	Lokale Weiterleitung	210
6.4.3.2	Entfernte Weiterleitung	211
6.4.3.3	Off-Host-Weiterleitung	211
6.4.3.4	Einschränkungen bei der Weiterleitung	213
6.4.4	X11-Weiterleitung	213
6.4.5	Sicherheit des Verbindungsprotokolls	215
6.4.6	Zusammenfassung: Verbindungsprotokoll	217
6.5	SSH File Transfer Protocol	218
6.5.1	Eigenschaften	220
6.5.2	Protokollstruktur	222
6.5.3	Paketverarbeitung	223
6.5.3.1	Anfrage-Antwort-Verhältnis	225
6.5.3.2	Mehrfachanfragen	226
6.5.3.3	Bedingte Reihenfolgetreue	226

6.5.3.4	Zuverlässigkeit	227
6.5.3.5	Toleranz zu fehlerhaften Paketen	228
6.5.3.6	Flexible Zugriffssteuerung	228
6.5.3.7	Client-Anfragen	231
6.5.3.8	Server-Antworten	233
6.5.4	Protokollerweiterungen	236
6.5.4.1	Einfluß auf die Protokollversion durch den Client: version-select	237
6.5.4.2	Auslesen von Server Produktinformationen: vendor-id	237
6.5.4.3	Einfluß auf die Protokollversion durch den Client: supported2	238
6.5.4.4	Plattformneutrale Behandlung: newline	240
6.5.4.5	Zeichensatz-Codierung: filename-charset	240
6.5.4.6	Zeichensatzkonvertierung auf dem Server: filename-translation-control	240
6.5.4.7	Überprüfung von Dateiinhalten: check-file	241
6.5.4.8	Verfügbarer Speicherplatz: space-available	241
6.5.4.9	Home-Verzeichnis: home-directory	241
6.5.5	Überlegungen zur Sicherheit	241
6.5.6	Zusammenfassung: SFTP	243
6.6	Das Public-Key-Subsystem	243
6.6.1	Protokollablauf	244
6.6.2	Überlegungen zur Sicherheit	249
6.6.3	Zusammenfassung: Public-Key Subsystem	250
6.7	Agenten in SSHv2	251
6.7.1	Protokollablauf: Agenten und Clients	254
6.7.1.1	Client-Anfragen zur Schlüsselverwaltung	257
6.7.1.2	Client-Anfragen zur Administration	259
6.7.1.3	Client-Anfragen zu Schlüsseloperationen	259
6.7.2	Protokollablauf: Agenten und Weiterleitung	261
6.7.2.1	Agentenweiterleitung aus Verwaltungsgründen	266
6.7.3	Überlegungen zur Sicherheit	266

6.7.4	Zusammenfassung: Agenten	268
6.8	SSHv1 und SSHv2 – Die Unterschiede auf einem Blick	269
6.9	Zusammenfassung	273

II Praktischer Einsatz 275

7	Konfiguration und Setup	277
7.1	Hallo, Welt!	278
7.1.1	Der einfachste Fall	278
7.1.2	Nur ein Befehl	279
7.1.3	Echte Shell mit Pipes	279
7.1.4	xterm im Hintergrund starten	280
7.1.5	Die laufende Sitzung kontrollieren	281
7.2	Installation von OpenSSH	282
7.2.1	Secure Shell Installation mit RPM	282
7.2.2	Secure Shell Installation aus den Quellen	283
7.3	OpenSSH: Konfiguration im Überblick	290
7.3.1	Konfigurationsdateien von OpenSSH-Client und OpenSSH-Server	292
7.3.2	Dateien zur Zugriffskontrolle	296
7.3.3	Formales: Regeln für Konfigurationsdateien	298
7.3.3.1	OpenSSH-Variablen	298
7.3.3.2	Angaben mit Mustern	299
7.3.3.3	Vorrangregelungen	300
7.4	Grundlegende Server-Konfiguration	302
7.4.1	Einstellen der Basiskonfiguration	303
7.4.2	Starten des Servers	306
7.4.2.1	Starten des OpenSSH-Servers über rcsshd	306
7.4.2.2	Direktes Starten des OpenSSH-Servers	308
7.4.2.3	Starten des OpenSSH-Servers beim Systemstart	313
7.5	Grundlegende Client-Konfiguration	314
7.6	Authentifizierungsmethoden	321
7.6.1	Authentifizierung in SSHv1	321

7.6.2	Server-Host-Authentifizierung	322
7.6.3	Client-Authentifizierung im Überblick	324
7.6.4	hostbased	324
7.6.5	Challenge/Response	328
7.6.6	publickey	332
7.6.7	password	339
7.6.7.1	Zusatzfunktionen mit PAM	341
7.6.7.2	Paßwortverifikation mit Kerberos	341
7.6.8	PAM und OpenSSH	342
7.6.8.1	PAM im Überblick	343
7.6.8.2	PAM und OpenSSH-Authentifizierungsmethoden	344
7.6.9	GSSAPI	347
7.7	Erweiterte Server-Konfiguration	350
7.7.1	Einstellungen beim Übersetzen des Programms	350
7.7.2	Serverweite Konfiguration	350
7.7.2.1	TCP/IP-Einstellungen	351
7.7.2.2	Zugriffskontrolle	355
7.7.2.3	Nachricht des Tages und Umgebungseinstellungen	359
7.7.2.4	Subsysteme	364
7.7.2.5	Logging und Debugging	365
7.7.2.6	sshd_config – Die Konfigurationsdatei des Servers	366
7.7.3	Account-bezogene Konfiguration	387
7.7.3.1	Authentifizierung	388
7.7.3.2	Schlüsselattribute der <i>publickey</i> -Authentifizierung	388
7.7.3.3	Benutzerspezifische Umgebungsvariablen und Skripte	392
7.8	Erweiterte Client-Konfiguration	394
7.8.1	Der OpenSSH-Client	395
7.8.1.1	Umgebungsvariablen	395
7.8.1.2	Befehlsoptionen	396
7.8.1.3	Prüfung von Host-Schlüsseln mit SSHFP	413

7.8.2	Globale Konfiguration	415
7.8.3	Benutzerspezifische Konfiguration	415
7.8.4	~/ssh/config und /etc/ssh/ssh_config – Die Konfigurationsdatei des Clients	416
7.9	Einrichten einer OpenSSH-Infrastruktur	443
7.9.1	Schrittweise Konfiguration	443
7.9.2	Empfohlenes Setup	445
7.9.2.1	Der OpenSSH-Server	446
7.9.2.2	Der OpenSSH-Client	448
8	OpenSSH im Einsatz	451
8.1	Schlüsselverwaltung und Agenten	451
8.1.1	Schlüssel-Management	452
8.1.1.1	Identitäten	452
8.1.1.2	Passphrases und Fingerprints	454
8.1.1.3	Komponenten im Zusammenspiel	454
8.1.2	Schlüsselerzeugung: ssh-keygen	455
8.1.2.1	Befehlsoptionen	456
8.1.2.2	Schlüssel generieren	463
8.1.2.3	Schlüsseltransfer zum Server	465
8.1.2.4	Schlüssel konvertieren	466
8.1.2.5	Kommentare, Fingerprints und SSHFP Resource Records	467
8.1.2.6	Ändern von Passphrases	468
8.1.2.7	Hashing der Known-Hosts-Datei	469
8.1.3	SSH-Agenten	470
8.1.3.1	Befehlsoptionen: ssh-agent	472
8.1.3.2	Befehlsoptionen: ssh-add	474
8.1.3.3	Starten und Beenden	476
8.1.3.4	Schlüssel hinzufügen und entfernen	477
8.1.3.5	Verwendung genehmigen	478
8.1.3.6	Sperren und Entsperren	479
8.1.4	Schlüssel sammeln: ssh-keyscan	479

8.1.4.1	Befehlsoptionen	480
8.1.4.2	Durchführung eines Scan-Vorgangs	482
8.2	Port und X Forwarding	482
8.2.1	Lokales Forwarding	485
8.2.1.1	Lokales Forwarding über die Kommandozeile	486
8.2.1.2	Port Forwarding über die Konfigurationsdatei	487
8.2.2	Remote Forwarding	488
8.2.3	Dynamic Forwarding	491
8.2.4	Off-Host Forwarding	494
8.2.5	Port Forwarding ohne Login	495
8.2.6	X Forwarding	495
8.2.6.1	Exkurs: Das X Window System	496
8.2.6.2	X Forwarding im Überblick	498
8.2.6.3	X-Forwarding aktivieren	500
8.2.6.4	Die X-Authentifizierung	502
8.2.6.5	OpenSSH und xauth	503
8.3	Sicherer Dateitransfer: scp	504
8.3.1	Befehlsoptionen	504
8.3.2	Dateitransfer zum Server	507
8.3.3	Dateitransfer vom Server	508
8.4	Das Subsystem SFTP	509
8.4.1	SFTP-Kommandos	510
8.4.2	SFTP-Optionen	513
8.5	OpenSSH in Unternehmensnetzen	517
8.5.1	SSH-Tunnel	517
8.5.2	NX/FreeNX und OpenSSH	519
8.5.3	CVS mit OpenSSH	521
8.5.4	OpenSSH in einer chroot-Umgebung	522
8.5.4.1	OpenSSH patchen	522
8.5.4.2	chroot-Benutzer anlegen	523
8.5.4.3	chroot-Umgebung des Benutzers anpassen	524
8.5.4.4	chroot-Umgebung testen	526

9 Migration bestehender Systeme	529
9.1 Ersetzen der r-Kommandos	529
9.1.1 Ersetzen von rcp und rsh	530
9.1.2 Absichern von rsync	531
9.1.2.1 anonymes rsync	531
9.1.2.2 rsync mit Benutzer-Shell	532
9.2 Versionswechsel von SSHv1- zu SSHv2-Produkten	533
9.2.1 Diagnose: Was ist im Einsatz?	535
9.2.2 Sichern der Konfiguration	536
9.2.2.1 Feststellen der aktuellen Server-Konfiguration	536
9.2.2.2 Feststellen der aktuellen Account-bezogenen Einstellungen	537
9.2.2.3 Feststellen der aktuellen Client-Konfiguration	537
9.2.3 Festlegen des Ziel-Szenarios	538
9.2.3.1 SSHv1- und SSHv2-Konfiguration	539
9.2.3.2 Bewertung der nötigen Maßnahmen	540
9.2.3.3 Welche Tools müssen neu installiert werden?	540
9.2.3.4 Besonderheiten in den neuen Versionen	540
9.2.3.5 Wie sind erweiterte Fähigkeiten der neuen Version einzubinden?	541
9.2.3.6 Ist ein Mischbetrieb ratsam?	541
9.2.3.7 Migration von Schlüsseln	542
9.2.4 Deinstallation und erneute Installation	542
9.2.5 Server-Konfiguration	543
9.2.6 Client-Konfiguration	544
9.2.7 Funktionstests des neuen Setups	545
10 Virtuelle Private Netze mit OpenSSH	547
10.1 Hallo, Welt!	547
10.2 Motivation	547
10.2.1 Billige private Netze für alle	547
10.2.2 Opportunistic Encryption	549
10.3 Alternativen	550

10.3.1	IPsec	550
10.3.2	OpenVPN	551
10.3.3	PPTP	552
10.3.4	Cisco PIX und andere Appliances	552
10.3.5	NCP und andere Software	553
10.4	Einsatzgebiet des OpenSSH VPNs	553
10.4.1	Vorteile	553
10.4.2	Nachteile	553
10.5	Begrifflichkeiten	554
10.5.1	VPN-Topologien	554
10.5.1.1	Netz-zu-Netz	554
10.5.1.2	Netz-zu-Client	554
10.5.1.3	Client-zu-Client	555
10.5.2	Schicht 2 oder 3	555
10.5.2.1	Schicht 3: IP	555
10.5.2.2	Schicht 2: Ethernet	555
10.5.3	tun-Interfaces	555
10.5.4	Subnetze und CIDR	558
10.5.4.1	Historisch: <i>classful routing</i>	559
10.5.4.2	Private Adreßräume	559
10.5.5	Gateways und Routen	559
10.6	Einrichten eines VPNs mit OpenSSH	560
10.6.1	Bestandsaufnahme	561
10.6.2	Rechner bereitmachen	561
10.6.2.1	Sicherstellen, daß SSH aktuell ist	561
10.6.2.2	tun-Unterstützung sicherstellen	562
10.6.2.3	IP-Forwarding sicherstellen	563
10.6.3	Konfigurationen erstellen	564
10.6.3.1	Auf vpngw-b Tunnels akzeptieren	564
10.6.3.2	Auf vpngw-b root-Zugang für Tunnel spezifizieren	564
10.6.4	VPN hochfahren	565
10.6.5	VPN debuggen	566