

SSH: Secure Shell

Ein umfassendes Handbuch

Daniel J. Barrett & Richard Silverman

Deutsche Übersetzung von Peter Klicman

O'REILLY®

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

Inhalt

<i>Vorwort</i>	<i>xi</i>
<i>1: Einführung in SSH</i>	<i>1</i>
1.1 Was ist SSH?	2
1.2 Was SSH nicht ist	3
1.3 Das SSH-Protokoll	4
1.4 Übersicht der SSH-Features	5
1.5 Die Geschichte von SSH	11
1.6 Verwandte Technologien	13
1.7 Zusammenfassung	19
<i>2: Grundlegende Verwendung der Clients</i>	<i>21</i>
2.1 Ein Fallbeispiel	21
2.2 Entfernte Terminal-Sessions mit ssh	22
2.3 Ein etwas komplexeres Beispiel	24
2.4 Authentifizierung über kryptographische Schlüssel	29
2.5 Der SSH-Agent	36
2.6 Verbindung ohne Paßwort und Paßphrase	41
2.7 Weitere Clients	42
2.8 Zusammenfassung	44
<i>3: Aufbau von SSH</i>	<i>45</i>
3.1 Features im Überblick	45
3.2 Grundlagen der Kryptographie	49
3-3 Die Architektur eines SSH-Systems	53

Inhalt

3.4	Das Innere von SSH-1.	57
3-5	Das Innere von SSH-2.	78
3.6	Benutzer-Zugriff (userfile).	93
3.7	Zufälligkeit	94
3.8	SSH und Dateitransfers (scp und sftp).	96
3.9	Von SSH verwendete Algorithmen.	100
3.10	Von SSH erkannte Gefahren	108
3.11	Was SSH nicht verhindern kann	112
3.12	Zusammenfassung.	115
4:	<i>Installation und Kompilierungs-Konfiguration.</i>	<i>117</i>
4.1	SSH1 und SSH2.	117
4.2	F-Secure SSH Server.	139
4.3	OpenSSH.	140
4.4	Software-Inventar.	143
4.5	R-Befehle durch SSH ersetzen.	145
4.6	Zusammenfassung.	148
5:	<i>Serverweite Konfiguration.</i>	<i>149</i>
5.1	Der Name des Servers.	150
5.2	Ausführen des Servers.	150
5-3	Server-Konfiguration: Ein Überblick	153
5.4	Das Setup vorbereiten	159
5.5	7M%2LV% gewähren: Authentifizierung und Zugriffskontrolle.	177
5.6	Benutzer-Logins und -Accounts.	200
5.7	Subsysteme.	202
5.8	History, Logging und Debugging	204
5.9	Kompatibilität zwischen SSH-1- und SSH-2-Servern.	214
5.10	Zusammenfassung	215
6:	<i>Key-Management und Agenten.....</i>	<i>217</i>
6.1	Was ist eine Identität?.	218
6.2	Eine Identität erzeugen.	222
6.3	SSH-Agenten	230
6.4	Mehrere Identitäten.	251
6.5	Zusammenfassung	254

7: Fortgeschrittene Verwendung von Clients	255
7.1 Wie man Clients konfiguriert	255
7.2 Vorrang	266
7.3 Einführung in den Verbose-Modus	266
7.4 Client-Konfiguration im Detail	268
7.5 Sicheres Kopieren mit scp	301
7.6 Zusammenfassung	309
8: Account-orientierte Serverkonfiguration	311
8.1 Grenzen dieser Technik	312
8.2 Public-Key-basierte Konfiguration	314
8.3 Trusted-Host-Zugriffskontrolle	332
8.4 Die benutzereigene rc-Datei	334
8.5 Zusammenfassung	334
9: Port- und X-Forwarding	337
9.1 Was ist Forwarding?	338
9.2 Port-Forwarding	339
9.3 X-Forwarding	363
9.4 Forwarding-Sicherheit: TCP-wrappers und libwrap	377
9.5 Zusammenfassung	383
10: Ein empfohlenes Setup	385
10.1 Grundlegendes	386
10.2 Kompilierungs-Konfiguration	386
10.3 Serverweite Konfiguration	387
10.4 Account-bezogene Konfiguration	392
10.5 Key-Management	392
10.6 Client-Konfiguration	392
10.7 Entfernte Home-Verzeichnisse (NFS, AFS)	393
10.8 Zusammenfassung	396
11: Fallstudien	397
11.1 Automatisches SSH: Batch- oder cron-Jobs	397
11.2 FTP-Forwarding	404
11.3 Pine, IMAP und SSH	427
11.4 Kerberos und SSH	435

11.5	Verbindungen über einen Gateway-Host	456
12: Fehlersuche und FAQ		465
12.1	Debugging-Meldungen: Ihre erste Verteidigungslinie	465
12.2	Probleme und Lösungen	467
12.3	Andere SSH-Ressourcen	488
12.4	Reporting von Bugs.	490
13- Übersicht anderer Implementierungen.		491
13.1	Gängige Features.	491
13.2	Behandelte Produkte.	492
13.3	Produktübersicht	492
13.4	Weitere SSH-nahe Produkte.	500
14: SSH 1-Portierung von Sergey Okhapkin (Windows).		501
14.1	Clients beschaffen und installieren.	501
14.2	Verwendung des Clients.	506
14.3	Beschaffen und Installieren des Servers.	506
14.4	Fehlersuche	509
14.5	Zusammenfassung	510
15: SecureCRT (Windows).		511
15.1	Beschaffung und Installation	511
15.2	Grundlegende Einrichtung des Clients.	512
15.3	Key-Management	512
15.4	Fortgeschrittene Einrichtung von Clients.	514
15.5	Forwarding.	516
15.6	Fehlersuche.	517
15.7	Zusammenfassung.	519
16: F-Secure SSH Client (Windows, Macintosh).		521
16.1	Beschaffung und Installation.	521
16.2	Grundlegende Einrichtung des Clients.	522
16.3	Key-Management	523
16.4	Fortgeschrittene Einrichtung des Clients.	524
16.5	Forwarding.	527
16.6	Fehlersuche.	529
16.7	Zusammenfassung.	530

<i>17: NiftyTelnet SSH (Macintosh)</i>	<i>531</i>
17.1 Beschaffung und Installation	531
17.2 Grundlegende Einrichtung des Clients	532
17.3 Fehlersuche	534
17.4 Zusammenfassung	535
<i>A: SSH2-Manpage für sshregex</i>	<i>537</i>
<i>B: SSH-Schnellübersicht</i>	<i>541</i>
<i>Index</i>	<i>557</i>