

Inhaltsverzeichnis

Einleitung	1
1.1 Internet und Sicherheit	1
1.2 Internet	9
1.3 Protokolle und Dienste des Internets	12
1.4 Internet Engineering Task Force (IETF)	37
1.5 Grundlagen der Kommunikationssicherheit	41
1.6 Zusammenfassung	61
Kryptographie für das Internet	63
2.1 Verschlüsselung	63
2.2 Schlüsselmanagement	69
2.3 Zertifikate und Zertifizierungsinfrastrukturen	71
2.4 Digitale Signaturen	85
2.5 Rechtliche Grundlagen	90
2.6 Zertifizierungsarchitekturen im Internet	97
2.7 Zertifizierungsstellen	113
2.8 Zusammenfassung	117
Data Link Layer Security	119
3.1 Methoden zur Security-Integration in den Data Link Layer	120
3.2 Point to Point Tunneling Protocol (PPTP)	124
3.3 Layer 2 Tunneling Protocol (L2TP)	134
3.4 Probleme der Data Link Layer Security	139
3.5 Zusammenfassung	141

Inhaltsverzeichnis	▪	XI
	▪	
	▪	

Network Layer Security **143**

4.1 Methoden zur Security-Integration in den Internet Layer 143
4.2 IP Security Protocol (IPsec)..... 150
4.3 Schlüsselverwaltung 168
4.4 IPsec und IPv6 208
4.5 Probleme und offene Punkte..... 209
4.6 Zusammenfassung 214

Transport Layer Security **215**

5.1 Secure Socket Layer Protocol..... 215
5.2 Secure Shell (ssh)..... 234
5.3 Private Communication Technology (PCT)..... 236
5.4 Transport Layer Security 241
5.5 Server Gated Cryptography 244
5.6 Zusammenfassung 248

Application Layer Security **249**

6.1 Sichere Dienste der Anwendungsschicht..... 250
6.2 Sicherheit im World Wide Web..... 253
6.3 Electronic Mail 255
6.4 File Transfer 262
6.5 Telnet 263
6.6 Sichere Dateisysteme 265
6.7 Zusammenfassung 276

Ausgewählte Kommunikationsanwendungen im Internet **277**

7.1 Internet-Telefonie 277
7.2 Internet-Banking 287
7.3 Zusammenfassung 335

Literaturverzeichnis **337**

Index **347**

Abkürzungsverzeichnis **361**

XII ■ Inhaltsverzeichnis
■
■



<http://www.springer.com/978-3-540-66814-5>

Open Internet Security

Von den Grundlagen zu den Anwendungen

Fischer, S.; Rensing, C.; Rödiger, U.

2000, XII, 368 S. 14 Abb., Softcover

ISBN: 978-3-540-66814-5