

Inhaltsverzeichnis

1	Einleitung	1
1.1	Rahmenbedingungen	1
1.2	Aufbau des Buches	3
2	Internet-Protokolle im kommerziellen Einsatz	5
2.1	Datenübertragung im Internet.....	5
2.2	Datenübertragung und das OSI-Referenzmodell	7
2.2.1	Grundlagen von Netzwerkprotokollen	8
2.2.2	OSI-Referenzarchitektur	9
2.3	Protokollfamilie TCP/IP	11
2.3.1	Aufbau der Internet-Protokolle.....	14
2.3.2	Internet-Protokoll (IP).....	15
2.3.3	Die Netzwerkzugangsebene	25
2.3.4	Die Protokolle der Transportschicht.....	30
2.4	Dienste der Anwendungsebene	34
2.4.1	Charakteristika von Internet-Diensten.....	35
2.4.2	DNS – Rechnernamen und IP-Adressen.....	36
2.4.3	Elektronische Post.....	38
2.4.4	World Wide Web	42
2.4.5	Internet-Dienste im kommerziellen Einsatz	49
2.5	Schwachstellen von TCP/IP im kommerziellen Einsatz....	51
3	Relevante kryptographische Verfahren	53
3.1	Grundbegriffe.....	53
3.2	Symmetrische Verschlüsselung	54
3.3	Hash-Verfahren.....	56
3.4	Asymmetrische Verschlüsselung.....	56
3.5	Anwendung kryptographischer Verfahren	59

4 Sicherheitsarchitektur für WWW-Informationssysteme	63
4.1 Ziele der Sicherheitsarchitektur	63
4.1.1 Transaktionssicherheit.....	64
4.1.2 Sicherheitsaspekte im Intranet	66
4.2 Sicherheitsarchitektur.....	68
5 Zertifikate und Vertrauensmanagement	71
5.1 Authentifizierung mit Zertifikaten	71
5.1.1 Zertifikate nach ITU-T X.509	73
5.1.2 Lebenszyklus eines Zertifikates	77
5.2 Vertrauensmodelle	79
5.3 Globale Vertrauenshierarchien	82
5.3.1 Sichere E-Mail: PEM und PGP	83
5.3.2 Kommerzielle X.509-Infrastrukturen	88
5.3.3 Modell der PKIX-Arbeitsgruppe	94
5.3.4 Europäisches Pilotprojekt: ICE-TEL	97
5.3.5 Sicherer elektronischer Zahlungsverkehr: SET	100
5.3.6 Distribution von Zertifikaten mittels DNS	102
5.4 Problembereiche und Entwicklungstendenzen.....	104
6 Verzeichnisdienst	107
6.1 X.500 – Das globale Directory	107
6.1.1 Architektur des globalen Verzeichnisdienstes.....	108
6.1.2 Informationsmodell und Namensraum	109
6.2 Verzeichnisse im Internet: LDAP	113
7 Absicherung der Internet-Protokolle	117
7.1 Übersicht	118
7.2 Absicherung auf Vermittlungsschicht	119
7.3 Absicherung auf Transportschicht.....	123
7.3.1 Abgesicherte Internet-Dienste.....	123
7.3.2 SSL-Protokoll.....	124
7.4 Absicherung auf Anwendungsebene	128
8 Zugriffskontrolle	131
8.1 Zugriffskontrollmodelle	132
8.1.1 Repräsentation der Zugriffskontrollinformation.....	134
8.1.2 Steuerungsmodelle	136
8.1.3 Generalisierungsmechanismen	138
8.1.4 Gängige Zugriffskontrollmodelle	139

8.1.5	Rollenbasierte Zugriffskontrollmodelle	142
8.1.6	Zwei kommerzielle Zugriffskontrollmodelle	146
8.2	Zugriffskontrolle in WWW-Informationssystemen	148
8.2.1	Elementare Zugriffskontrollmechanismen	149
8.2.2	Zugriffskontrollmechanismen mit zentralem Repository	150
8.3	Forschungsprojekte und Entwicklungstendenzen	157
8.3.1	Rollenbasierte Zugriffskontrollmodelle für WWW-Informationssysteme	157
8.3.2	Eigenständige Sicherheitsarchitekturen.....	163
8.3.3	Zugriffskontrolle mit Zertifikaten: SDSI und SPKI.....	168
8.4	Zusammenfassung.....	172

Glossar	173
----------------	------------

Bibliographie	191
----------------------	------------

Index	201
--------------	------------