

Inhaltsverzeichnis

1	Einleitung	1
1.1	Gegenstand des Buches	1
1.2	Aufbau des Buches	2
1.3	Zielgruppe	3
1.4	Anforderungen an den Leser	3
1.5	Konventionen in diesem Buch	3
1.6	Feedback	4
1.7	Danksagung	4
I	Grundlagen	5
2	Kommunikation in Netzen	7
2.1	Lernziele	7
2.2	Einleitung	7
2.2.1	Was ist das Internet?	7
2.2.2	Geschichte des Internets	8
2.3	Schichtenmodell der Kommunikation	10
2.3.1	Motivation für Schichtenmodelle	10
2.3.2	ISO/OSI-Referenzmodell	12
2.3.3	Das Internetmodell	15
3	Informations- und Kommunikationssicherheit	19
3.1	Lernziele	19
3.2	Einleitung	19
3.3	Gefahren und Angriffe	20
3.3.1	Passive Angriffe	21
3.3.2	Aktive Angriffe	21
3.4	Sicherheitsanalyse	23
3.5	Sicherheitsdienste	24
3.5.1	Vertraulichkeit	25

3.5.2	Integrität	25
3.5.3	Authentifizierung	25
3.5.4	Nicht-Abstreitbarkeit	29
3.5.5	Zugangs- und Zugriffskontrolle	29
4	Kryptographie	31
4.1	Lernziele	31
4.2	Einleitung	31
4.3	Symmetrische Kryptosysteme	32
4.3.1	Block- und Stromchiffren	32
4.3.2	Betriebsarten von Blockchiffren	35
4.3.3	Padding	39
4.4	Message Authentication Code	41
4.5	Kryptographische Hashfunktion	43
4.5.1	Resistenz-Eigenschaften	45
4.5.2	Realisierung von Hashfunktionen	47
4.5.3	HMAC: Hashfunktion-basierender MAC	49
4.6	Asymmetrische Kryptosysteme	51
4.7	Hybride Kryptosysteme	55
4.8	Digitale Signatur	56
4.8.1	Signaturverfahren mit Nachrichtenrückgewinnung	57
4.8.2	Signaturverfahren mit Anhang	58
4.9	Übungsaufgaben	59
5	Public-Key-Infrastrukturen	63
5.1	Lernziele	63
5.2	Einleitung	63
5.3	Akteure und Komponenten in einer PKI	64
5.4	Registrierungsinstanz	66
5.5	Zertifizierungsinstanz	66
5.6	Vertrauensmodelle	67
5.7	X.509-Zertifikate	69
5.8	Sperrliste	72
5.9	Verzeichnisdienst	74
5.10	Gültigkeitsmodell	75
5.10.1	Schalenmodell	75
5.10.2	Modifiziertes Schalenmodell	76

5.10.3	Kettenmodell	76
5.10.4	X.509-konforme Gültigkeitsprüfung	77
5.11	Übungsaufgaben	78
II	Absicherung lokaler Netze	81
6	Netzwerkinfrastrukturen	83
6.1	Lernziele	83
6.2	Einleitung	83
6.3	Angriffe in lokalen Netzen	84
6.3.1	CAM Table Flooding	84
6.3.2	ARP Spoofing	85
6.4	Abwehrmaßnahmen in der Netzwerkinfrastruktur	85
6.5	Firewalls	86
6.5.1	Erstellung von Firewall-Policies	87
6.5.2	Paket-Filter	89
6.5.3	Anwendungs-Firewall	91
6.5.4	Sichtbarkeit	92
6.5.5	Intrusion-Detection-Systeme	93
6.5.6	Probleme und Grenzen von Firewalls	94
6.6	Firewall-Architekturen	95
6.6.1	Einfacher Paketfilter	95
6.6.2	Dual-Homed-Host-Architektur	96
6.6.3	Screened-Host-Architektur	96
6.6.4	Screened-Subnet-Architektur	97
6.7	Virtuelle LANs	99
6.8	802.1X	101
6.9	Übungsaufgaben	103
7	Authentifizierung im Netzwerk	105
7.1	Lernziele	105
7.2	Einleitung	105
7.3	Einfache Authentifizierungsprotokolle	106
7.3.1	PAP	106
7.3.2	S/Key	108
7.3.3	CHAP	110
7.4	Extensible Authentication Protocol (EAP)	113
7.4.1	Einführung	113
7.4.2	EAP-Protokoll	114

7.4.3	EAP-TLS	116
7.4.4	EAP-TTLS	117
7.5	Weitere Authentifizierungs-Protokolle	118
7.6	Authentifizierungs-Methoden in Netzwerkprotokollen	119
7.7	Übungsaufgaben	120
8	WLAN-Sicherheit	121
8.1	Lernziele	121
8.2	Einleitung	121
8.3	Wired Equivalent Privacy	122
8.3.1	Verschlüsselung	122
8.3.2	Authentifizierung	124
8.3.3	Integritätsschutz	125
8.4	802.11i, WPA und WPA2	126
8.4.1	Authentifizierung und Schlüsselmanagement	126
8.4.2	TKIP	128
8.4.3	AES-CCMP	129
8.5	WPS	129
8.6	MAC-Adress-Filter und versteckte SSID	130
8.7	Übungsaufgaben	130
9	Kerberos	133
9.1	Lernziele	133
9.2	Einleitung	133
9.3	Die Kerberos-Architektur im Überblick	134
9.3.1	Authentifizierung	136
9.3.2	Autorisierung	138
9.3.3	Dienstnutzung	138
9.3.4	Entwurfsentscheidungen	138
9.4	Spezielle Eigenschaften von Kerberos	140
9.4.1	Passwort-Änderungen	140
9.4.2	Bindung an IP-Adressen	140
9.4.3	Weitergabe von Tickets	141
9.4.4	Zukünftige Gültigkeit	141
9.4.5	Erneuerbare Tickets	141
9.4.6	Replizierte KDCs	142
9.4.7	Domänen	142
9.5	Übungsaufgaben	144

III	Internet-Sicherheit	145
10	IPsec	147
10.1	Lernziele	147
10.2	Einleitung	147
10.3	Angriffe	148
10.3.1	IP Address Spoofing	148
10.4	Internet Key Exchange	149
10.5	Allgemeines zur gesicherten Kommunikation mit IPsec	152
10.5.1	Integritätsschutz und Authentifizierung	153
10.5.2	Schutz vor Wiederholungsangriffen	153
10.5.3	Security Parameters Index (SPI)	154
10.6	Authentication Header (AH)	155
10.7	Encapsulating Security Payload (ESP)	155
10.8	Kritik	156
10.9	Übungsaufgaben	157
11	Sicherheit der Transportschicht	159
11.1	Lernziele	159
11.2	Einleitung	159
11.3	Sicherheitsprobleme der Transportschicht	159
11.3.1	UDP	160
11.3.2	TCP	160
11.4	TLS im Überblick	164
11.4.1	TLS-gesicherte Dienste ansprechen	164
11.4.2	TLS-gesicherte Dienste aufsetzen	166
11.4.3	TLS in eigene Programme integrieren	167
11.5	Die Protokolle von TLS	168
11.5.1	Das Handshake-Protokoll	168
11.5.2	Das Record-Protokoll	172
11.6	Sicherheit von TLS	173
11.6.1	Sicherheitsziele	173
11.6.2	Schwächen und Angriffe	174
11.7	Übungsaufgaben	177
11.7.1	Sicherheitsprobleme der Transportschicht	177
11.7.2	TLS: Grundlegendes	177
11.7.3	TLS für den Webserver konfigurieren	178
11.7.4	TLS in eigene Programme integrieren	178

12	DNS-Sicherheit	179
12.1	Lernziele	179
12.2	Einleitung	179
12.2.1	Funktionsweise des DNS	179
12.2.2	DNS Records	181
12.3	Ein Angriff mit DNS	182
12.4	Sicherheitsprobleme und Angriffe auf das DNS	183
12.4.1	Hosts-Datei	183
12.4.2	Server-Kompromittierung	183
12.4.3	DNS Cache Poisoning	184
12.5	DNSSEC	187
12.5.1	DNSKEY Resource Record	188
12.5.2	RRSIG Resource Record	189
12.5.3	NSEC Resource Record	190
12.5.4	DS Resource Record	192
12.5.5	Aufbau einer Vertrauenskette	192
12.5.6	Kritik	195
12.6	Übungsaufgaben	195
12.6.1	DNS	195
12.6.2	DNSSEC	195
 IV	 Mobilfunk- und Web-Sicherheit	 197
13	GSM und UMTS	199
13.1	Lernziele	199
13.2	Einleitung	199
13.3	SIM-Karte	199
13.4	GSM	200
13.4.1	Authentifizierung und Verschlüsselung	200
13.4.2	Schutz der Teilnehmeridentität	202
13.4.3	Schwachstellen von GSM	202
13.5	UMTS	203
13.5.1	Authentifizierung und Verschlüsselung	203
13.5.2	Schutz der Teilnehmeridentität	204
13.5.3	Interoperabilität mit GSM	204
13.6	Übungsaufgaben	205

14	Web-Sicherheit	207
14.1	Lernziele	207
14.2	Einleitung	207
14.3	Verwendung von TLS	208
14.4	Authentifizierung im Web	209
14.4.1	Cookies	209
14.4.2	Einfache Authentifizierungsmethoden	211
14.4.3	OpenID	214
14.5	Angriffe und Gegenmaßnahmen im Web	217
14.5.1	Cross-Site-Scripting	217
14.5.2	Cross-Site-Request-Forgery	220
14.5.3	Cookie-Angriffe	221
14.5.4	Phishing	224
14.6	Übungsaufgaben	227
V	Szenarien	229
15	Der Blickwinkel des Penetrationstesters	231
15.1	Werkzeuge	231
15.2	Netz eines Kleinunternehmers	231
15.3	Spionage in einem Unternehmensnetz	232
15.4	Bemerkung	234
16	Der Blickwinkel des Sicherheitsbeauftragten	237
16.1	Unterwegs	237
16.2	Viele Wünsche auf einmal	238
16.3	WLAN	240
Abkürzungsverzeichnis		243
Literaturverzeichnis		249
Index		259