

Inhaltsverzeichnis

1	Einführung	1
1.1	Haben wir etwas zu verbergen?	2
1.2	Säulen des Datenschutzes	4
1.3	Themen dieses Buchs und Lernziele	5
1.4	Danksagung	7
	Literatur	7
2	Einführung in den Technischen Datenschutz	9
2.1	Schutzziele	9
2.1.1	„Klassische“ IT-Sicherheits-Schutzziele	10
2.1.2	„Neue“ Datenschutz-Schutzziele	10
2.2	Begriffsbestimmungen	11
2.2.1	Begriff des Datenschutzes	11
2.2.2	Begriffe zum technischen Datenschutz	12
2.3	Grundlegende kryptographische Verfahren	14
2.3.1	Verschlüsselung	14
2.3.2	Digitale Signatur	17
2.3.3	Blinde Signatur	18
2.3.4	Kryptographische Hashfunktion	19
2.3.5	Diffie-Hellman-Verfahren	20
2.4	Grundlegende Verfahren aus der IT-Sicherheit	22
2.4.1	Transport Layer Security	22
2.4.2	Virtual Private Networks	24
2.5	Fazit	26
2.6	Übungsaufgaben	26
	Literatur	26
3	Anonymitätsmaße	27
3.1	Überblick	27
3.1.1	Anonymitäts-Modelle	28
3.1.2	Quasi-Identifikatoren	30

3.2	k-Anonymität	32
3.2.1	Generalisierung von Daten	33
3.2.2	Angriffe auf k-Anonymität	34
3.2.3	l-Diversität	37
3.3	Differential Privacy	38
3.4	Anonymisierung in der Praxis	40
3.5	Fazit	40
3.6	Übungsaufgaben	41
	Literatur	43
4	Anonymität im Internet	45
4.1	Verkehrsflussanalyse	46
4.1.1	Angreiferklassifikation	46
4.1.2	Beispiel: Ablauf der Ticketbestellung	47
4.1.3	Beispiel: Mögliche Gegenmaßnahme	48
4.2	Mixes	49
4.2.1	Verfahren	50
4.2.2	Analyse	50
4.3	Mix-Kaskaden	51
4.3.1	Verfahren	51
4.3.2	Analyse	53
4.3.3	Antwort-Nachrichten	53
4.4	Onion Routing / Tor	55
4.4.1	Grundkonzept von Tor	55
4.4.2	Tor-Zellen	56
4.4.3	Aufbau eines Circuits	56
4.4.4	Leaky Pipe	59
4.4.5	Missbrauch von Tor	59
4.4.6	Hidden Services	60
4.4.7	Angriffe auf Tor	61
4.4.8	Zensurresistenz mit Tor	63
4.5	Fazit	63
4.6	Übungsaufgaben	64
	Literatur	64
5	Identitätsmanagement	67
5.1	Überblick	68
5.1.1	Schwerpunkte und Sichtweisen im Identitätsmanagement	68
5.2	OpenID	69
5.2.1	Ablauf der Authentifizierung	70
5.2.2	Analyse	70

5.3	OAuth	71
5.3.1	Verfahren	72
5.3.2	Analyse.....	73
5.4	OpenID Connect.....	74
5.5	Fazit	74
5.6	Übungsaufgaben.....	75
	Literatur	75
6	Anonymes Bezahlen	77
6.1	Anforderungen an ein anonymes Bezahlverfahren	77
6.2	Anonymes Bezahlen nach Chaum	78
6.2.1	Verfahren im Überblick	79
6.2.2	Bewertung.....	81
6.3	Bitcoin	82
6.3.1	Anonymität von Bitcoin	84
6.4	Anonymes Bezahlen in der Praxis	85
6.4.1	Geldkarte	85
6.4.2	Prepaid-Karten.....	86
6.5	Fazit	86
6.6	Übungsaufgaben.....	87
	Literatur	87
7	Datenschutz im World Wide Web	89
7.1	Tracking im Web	89
7.1.1	Cookies.....	90
7.1.2	Tracking-Pixel	93
7.1.3	Device Fingerprinting	94
7.1.4	History Hijacking.....	94
7.1.5	P3P	95
7.2	Social Plugins	95
7.3	Fazit	96
7.4	Übungsaufgaben.....	96
8	Instant Messaging	97
8.1	Abgrenzung des Instant Messagings von E-Mail	97
8.1.1	Schutzziele bei der E-Mail-Sicherheit	98
8.1.2	Schutzziele beim Instant Messaging	98
8.2	Off-the-record Messaging.....	98
8.2.1	Protokoll	99
8.2.2	Implementierung.....	101
8.2.3	Angriffe auf OTR Messaging	101
8.2.4	SIGMA-Protokoll.....	102

8.3	WhatsApp.....	103
8.3.1	Signal-Protokoll	104
8.3.2	Medien-Verschlüsselung	105
8.3.3	Sichere Telefonie	106
8.3.4	Schlüssel-Verifikation	106
8.3.5	Datenschutzrechtliche Probleme.....	106
8.4	Fazit.....	106
8.5	Übungsaufgaben.....	107
	Literatur	108
9	Elektronische Ausweisdokumente	109
9.1	Elektronischer Reisepass.....	110
9.1.1	Passive Authentication	110
9.1.2	Basic Access Control	111
9.1.3	Extended Access Control.....	113
9.2	Elektronischer Personalausweis	116
9.2.1	PACE	117
9.2.2	Extended Access Control Version 2	118
9.2.3	Restricted Identification	120
9.2.4	Weitere Anwendungen	122
9.2.5	Exkurs: Elektronische Signaturen	124
9.2.6	Administrative Aspekte	125
9.3	Fazit.....	126
9.4	Übungsaufgaben.....	127
	Literatur	128
10	Weitere kryptographische Verfahren für PETs	129
10.1	Weitere Signaturverfahren	129
10.1.1	Gruppensignatur	130
10.1.2	Ringsignatur	131
10.2	Secure Multiparty Computation	131
10.2.1	Klassische MPC-Protokolle	132
10.2.2	Anwendungen der Secure Multiparty Computation	133
10.3	Zero-Knowledge Proof.....	134
10.4	Anonyme Berechtigungsnachweise	135
10.4.1	Probleme	135
10.4.2	Verfahren.....	136
10.5	Fazit.....	137
10.6	Übungsaufgaben.....	137
	Literatur	137

11	Datenschutzrecht	139
11.1	Geschichte des Datenschutzes	140
11.2	Datenschutz im Grundgesetz	142
11.3	Bundesdatenschutzgesetz	144
11.3.1	Personenbezogene Daten	145
11.3.2	Zweck und Anwendungsbereich	146
11.3.3	Weitere Begriffsbestimmungen	148
11.3.4	Grundkonzept des deutschen Datenschutzrechts	149
11.3.5	Auskunftsanspruch	151
11.4	Bereichsspezifischer Datenschutz	152
11.4.1	Anwendungsbereich	152
11.4.2	Telemediengesetz	153
11.4.3	Telekommunikationsgesetz	158
11.5	Datenschutz-Grundverordnung	161
11.6	Datenschutzrechtliche Einzelfragen	163
11.6.1	Personenbezug bei IP-Adressen?	163
11.6.2	Einwilligung	164
11.6.3	Anwendungsbereich des TMG	165
11.6.4	Anwendung TMG bei E-Mail	166
11.6.5	Herausgabe personenbezogener Daten	167
11.6.6	Auskunft über Datei-Downloads	167
11.6.7	Ausweitung der Protokollierung	168
11.6.8	Rufnummernunterdrückung	168
11.7	Datenschutzrechtliche Betrachtung von Tracking im Web	169
11.7.1	Cookies	169
11.7.2	Google Analytics	169
11.7.3	Device Fingerprinting	170
11.7.4	Social Plugins	170
11.8	Fazit	171
11.9	Übungsaufgaben	171
	Literatur	172
12	Zusammenfassung und Ausblick	173
	Sachverzeichnis	175