

Roland Hellmann

IT-Sicherheit

Methoden und Schutzmaßnahmen für Sichere
Cybersysteme

2., aktualisierte und erweiterte Auflage

DE GRUYTER
OLDENBOURG

Inhalt

- 1 Grundlagen und Motivation — 1**
 - 1.1 Einleitung — 1
 - 1.2 Motivation — 1
 - 1.3 Grundbegriffe — 3
 - 1.3.1 Datensicherheit, Datensicherung und Datenschutz — 3
 - 1.3.2 Identifizierung, Authentifizierung, Autorisierung — 4
 - 1.4 Aufgaben — 6

- 2 Symmetrische Verschlüsselung — 7**
 - 2.1 Definitionen und Anwendung — 7
 - 2.2 Substitutions-Chiffren — 8
 - 2.2.1 Cäsar-Chiffre — 8
 - 2.2.2 Symmetrische und asymmetrische Verfahren — 11
 - 2.2.3 Kryptoanalyse — 11
 - 2.3 Affine Chiffrierverfahren — 13
 - 2.4 Polyalphabetische Substitutions-Chiffren — 13
 - 2.5 Perfekte Vertraulichkeit — 14
 - 2.6 Pseudo-Zufallsgeneratoren — 15
 - 2.7 Stromchiffren — 16
 - 2.7.1 XOR-Stromchiffre — 16
 - 2.7.2 Kerckhoffs' Prinzip — 22
 - 2.7.3 Synchrone Stromchiffren — 23
 - 2.7.4 Selbstsynchronisierende Stromchiffren — 24
 - 2.7.5 Weitere Stromchiffren — 25
 - 2.8 Blockchiffren — 25
 - 2.8.1 Allgemeines — 25
 - 2.8.2 Betriebsmodi — 25
 - 2.8.3 DES — 26
 - 2.8.4 AES — 28
 - 2.8.5 Weitere Blockchiffren — 29
 - 2.9 Hinreichende Sicherheit — 30
 - 2.10 Aufgaben — 31

- 3 Public Key-Verschlüsselungsverfahren — 33**
 - 3.1 Der Diffie-Hellman-Exponential-Schlüsseltausch — 33
 - 3.2 Rein asymmetrische Verschlüsselung — 34
 - 3.3 Einsatz eines Keyserver — 36
 - 3.4 MITM-Attack — 39
 - 3.5 Der RSA-Algorithmus — 43

3.5.1	Schlüsselgenerierung —	43
3.5.2	Ver- und Entschlüsselung —	45
3.5.3	Algorithmus —	45
3.5.4	Sicherheit —	46
3.6	Hybride Verschlüsselungsverfahren —	47
3.7	Weitere Public Key Verfahren —	51
3.7.1	Diskrete Logarithmen —	51
3.7.2	Elliptische Kurven —	51
3.7.3	Post-Quanten-Kryptographie —	52
3.8	Aufgaben —	52
4	Kryptographische Hash-Funktionen —	54
4.1	Arbeitsweise —	54
4.2	Anforderungen an Hash-Funktionen —	55
4.3	Hash-Funktion und Integrität —	55
4.4	Authentifizierung des Senders von Daten mittels Hash-Funktionen —	59
4.5	Authentifizierung von Benutzern durch das Betriebssystem mit Hash-Funktionen —	62
4.5.1	Arbeitsweise —	62
4.5.2	Hash-Funktion und Verschlüsselung —	64
4.5.3	Anmeldung an Anwendungsprogrammen —	64
4.5.4	Umgehung des Passwortschutzes —	65
4.5.5	Knacken von Passwörtern und Gegenmaßnahmen —	65
4.6	Probleme bei Hash-Funktionen —	67
4.6.1	Geburtsstagsangriff —	67
4.6.2	Gebrochene Hash-Funktionen —	69
4.7	Aufgaben —	69
5	Digitale Signaturen —	72
5.1	Anforderungen —	72
5.2	Digitale Signaturen mit asymmetrischen Verfahren —	72
5.3	Vergleich asymmetrische Verschlüsselung und digitale Signatur —	78
5.4	Algorithmen für digitale Signaturen —	81
5.5	Digitale Zertifikate —	81
5.5.1	Web of Trust (WOT) —	82
5.5.2	Public Key Infrastructure (PKI) —	83
5.6	Gesetzliche Regelungen —	84
5.7	Aufgaben —	86
6	Schutz vor Replay Attacks —	87
6.1	Nonce und Zeitstempel —	87
6.2	Bidirektionale Verwendung von Nonces —	91

- 6.3 Verwendung eines Pseudozufallsgenerators — 95
- 6.4 Aufgaben — 98

7 Weitere Anwendungen und abschließende Betrachtungen zur Kryptographie — 100

- 7.1 TLS — 100
 - 7.1.1 OSI-Modell — 100
 - 7.1.2 TLS im OSI-Modell — 101
 - 7.1.3 Verbindungsaufbau — 102
- 7.2 Wo sind die Grenzen der Kryptographie? — 103
- 7.3 Zusammenfassung der Angriffsmethoden — 104
 - 7.3.1 DoS Attack — 104
 - 7.3.2 Spoofing Attack — 104
 - 7.3.3 Hijacking Attack — 104
 - 7.3.4 Verkehrsflussanalyse — 105
 - 7.3.5 Replay Attack — 105
 - 7.3.6 Man-in-the-Middle-Attack — 105
 - 7.3.7 Verhandlungsfähige Protokolle — 105
 - 7.3.8 Illegaler Zustandswechsel — 105
 - 7.3.9 Known Plaintext Attack — 106
 - 7.3.10 Chosen Plaintext Attack — 106
- 7.4 Steganographie — 106
- 7.5 Aufgaben — 114

8 Verfügbarkeit — 115

- 8.1 Grundlagen — 115
 - 8.1.1 Definitionen — 115
 - 8.1.2 Die Badewannenkurve — 116
 - 8.1.3 Verbesserung der Verfügbarkeit — 118
- 8.2 RAID-Systeme — 118
 - 8.2.1 RAID Level 0 (Striping) — 119
 - 8.2.2 RAID Level 1 (Mirroring) — 120
 - 8.2.3 RAID Levels 2 bis 4 — 120
 - 8.2.4 RAID Level 5 — 124
 - 8.2.5 RAID Level 6 — 124
 - 8.2.6 RAID Level 10 — 127
 - 8.2.7 RAID Level 50 — 128
- 8.3 Grenzen der RAID-Systeme — 129
- 8.4 Verfügbarkeit von Software, Daten und Kommunikationsverbindungen — 129
- 8.5 Aufgaben — 130

9	Internetsicherheit — 132
9.1	Grundlagen — 132
9.2	Schadprogramme (Malware) — 132
9.2.1	Arten — 132
9.2.2	Malware-Erkennung — 138
9.2.3	Selbstschutz von Malware — 140
9.2.4	Malware-Baukästen (Malware Factory) — 141
9.2.5	Maßnahmen gegen Malware — 142
9.3	Botnetze — 143
9.3.1	Zweck der Botnetze — 143
9.3.2	Struktur — 144
9.3.3	Gegenmaßnahmen gegen Botnetze — 145
9.3.4	Abwehrmechanismen der Botnetz-Betreiber — 145
9.4	E-Mail, Spam und Phishing — 146
9.4.1	E-Mail-Prinzip — 146
9.4.2	Infizierte E-Mails — 147
9.4.3	Verbreitung von Spam — 148
9.4.4	E-Mail-Gefahren — 149
9.4.5	Schutzmaßnahmen — 151
9.5	Aktive Inhalte — 151
9.5.1	Gefahren — 151
9.5.2	Maßnahmen — 152
9.6	Schutzmaßnahmen: Alternativen zum üblichen PC am Internet — 153
9.6.1	Standalone-PC — 153
9.6.2	Autarkes Netzwerk — 153
9.6.3	Surf-PCs — 154
9.6.4	Live Medien — 155
9.6.5	Virtuelle Maschinen — 155
9.7	Aufgaben — 156
10	Firewalls — 157
10.1	Grundlagen — 157
10.1.1	Einsatzzweck — 157
10.1.2	Zu trennende Ressourcen — 157
10.1.3	Grenzen des Einsatzes — 159
10.1.4	IT-Sicherheitskonzept — 160
10.1.5	Filterebenen — 160
10.2	Paketfilter — 161
10.2.1	Beispiel: Ein IP-Spoofing-Angriff - die Kurzversion — 162
10.2.2	IP-Spoofing-Angriff - die ausführliche Version — 162
10.2.3	Abwehr des IP-Spoofing-Angriffs — 168
10.2.4	Nachteile von Paketfiltern — 168

- 10.3 Circuit Relays — 170
- 10.4 Application Gateways und Proxies — 170
- 10.5 Web Application Firewalls — 172
 - 10.5.1 Arbeitsweise — 172
 - 10.5.2 Notwendigkeit einer WAF — 172
 - 10.5.3 Beispiele für Angriffe auf Webanwendungen — 173
- 10.6 Firewall-Topologien — 177
 - 10.6.1 Zentrale Firewall — 178
 - 10.6.2 Zentrale Firewall mit DMZ — 180
 - 10.6.3 Kaskadierte Firewall mit DMZ — 180
 - 10.6.4 Sandwich-System — 181
 - 10.6.5 Hochverfügbare Firewall — 182
 - 10.6.6 Next-Generation Firewalls (NGFW) — 183
- 10.7 Aufgaben — 183

- 11 **IoT-Sicherheit — 185**
 - 11.1 Sicherheitsproblematik — 185
 - 11.2 Sicherheit im IoT-Gerät — 186
 - 11.2.1 Sicherheit von Webanwendungen für das IoT-Gerät — 186
 - 11.2.2 App-Sicherheit — 187
 - 11.2.3 Sicherheit der Datenübertragung — 187
 - 11.2.4 Cloud-Sicherheit — 188
 - 11.3 Auffinden verwundbarer Geräte — 188
 - 11.3.1 Problematik — 188
 - 11.3.2 Vorgehensweise — 189
 - 11.4 Sicherheitsmaßnahmen — 190
 - 11.4.1 Entwicklung sicherer Web-Anwendungen — 190
 - 11.4.2 Durchdachte Kaufentscheidungen — 191
 - 11.4.3 Erfassung aller IoT-Geräte und Strategie — 191
 - 11.4.4 Sichere Konfiguration — 192
 - 11.4.5 Eingeschränkte Zugriffsmöglichkeiten auf Daten — 192
 - 11.4.6 Sichtung von Log-Files — 192
 - 11.4.7 Pentesting — 193
 - 11.5 Aufgaben — 194

- 12 **Automotive Security — 195**
 - 12.1 Functional Safety und Cybersecurity — 195
 - 12.2 ISO/SAE 21434 — 196
 - 12.2.1 Cybersecurity-Management auf Unternehmensebene — 196
 - 12.2.2 Cybersecurity-Management auf Projektebene — 197
 - 12.2.3 Verteilte Cybersecurity-Aktivitäten — 197
 - 12.2.4 Kontinuierliche Cybersecurity-Aktivitäten — 197

12.2.5	Konzeptphase —	198
12.2.6	Produktentwicklung —	198
12.2.7	Cybersecurity-Validierung —	198
12.2.8	Produktion —	198
12.2.9	Betrieb und Wartung —	199
12.2.10	Ende des Cybersecurity-Supports und Außerbetriebnahme —	199
12.3	Security Threat Modeling —	199
12.3.1	Attack Surface und Trust Boundaries —	200
12.4	TARA —	202
12.4.1	Item Definition —	202
12.4.2	Assets und Schutzziele —	203
12.4.3	Schadensszenarien —	204
12.4.4	Schadenskategorien und Impact Rating —	205
12.4.5	Bedrohungsszenarien —	207
12.4.6	Angriffspfadanalyse (Attack Path Analysis) —	207
12.4.7	Attack Feasibility Rating —	207
12.4.8	Risiko-Ermittlung (Risk Value Determination) —	209
12.4.9	Entscheidung über den Umgang mit den Risiken —	211
12.5	Alternative Threat Modeling Methoden —	211
12.6	Aufgaben —	213

13 **Lösungen zu den Aufgaben — 214**

Stichwortverzeichnis — 237

Stichwortverzeichnis — 237

Literatur — 243