Inhaltsverzeichnis

1 Grundlagen der Datensicherheitstechnik 1

1 Einleitung ......................... 3
1.1 Inhalt und Aufbau dieses Buches ................................ 4
1.2 Bedrohungen und Sicherheitsziele ................................... 6
1.3 Sicherheitsanalyse für Netze ........................................... 10
1.4 Maßnahmen der Informationssicherheit ................................ 14
1.5 Zentrale Begriffe der Kommunikationssicherheit ................... 15

2 Grundbegriffe der Kryptologie 19

2.1 Kryptologie, Kryptografie und Kryptanalyse ....................... 19
2.2 Klassifizierung kryptografischer Algorithmen ....................... 20
2.3 Kryptanalyse ....................................................... 21
2.4 Einschätzung des Aufwandes kryptografischer Analysen ....... 24
2.5 Eigenschaften und Klassifizierung von Chiffrieralgorithmen .... 27
2.6 Schlüsselverwaltung ................................................. 29
2.7 Zusammenfassung .................................................... 31
2.8 Weiterführende Literatur ............................................. 33
2.9 Übungen .............................................................. 33

3 Symmetrische Chiffrierverfahren 35

3.1 Betriebsarten von Blockchiffren ...................................... 35
3.2 Der Data Encryption Standard ........................................ 42
3.3 Der Advanced Encryption Standard .................................. 49
3.4 Der RC4-Algorithmus .................................................. 54
3.5 Der KASUMI-Algorithmus .............................................. 57
3.6 Zusammenfassung ....................................................... 60
3.7 Weiterführende Literatur .............................................. 61
3.8 Übungen .............................................................. 62

4 Asymmetrische kryptografische Verfahren 63

4.1 Grundidee asymmetrischer kryptografischer Verfahren .......... 63
4.2 Mathematische Grundlagen ............................................ 67
4.3 Der RSA-Algorithmus .................................................. 76
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.4</td>
<td>Das Problem des diskreten Logarithmus</td>
<td>79</td>
</tr>
<tr>
<td>4.5</td>
<td>Das Diffie-Hellman-Schlüsselaustauschverfahren</td>
<td>83</td>
</tr>
<tr>
<td>4.6</td>
<td>Der ElGamal-Algorithmus</td>
<td>85</td>
</tr>
<tr>
<td>4.7</td>
<td>Sicherheit herkömmlicher asymmetrischer Kryptografie</td>
<td>88</td>
</tr>
<tr>
<td>4.8</td>
<td>Grundlagen der Kryptografie auf elliptischen Kurven</td>
<td>90</td>
</tr>
<tr>
<td>4.9</td>
<td>Zusammenfassung</td>
<td>102</td>
</tr>
<tr>
<td>4.10</td>
<td>Weiterführende Literatur</td>
<td>103</td>
</tr>
<tr>
<td>4.11</td>
<td>Übungen</td>
<td>105</td>
</tr>
<tr>
<td>5</td>
<td>Kryptografische Prüfwerte</td>
<td>107</td>
</tr>
<tr>
<td>5.1</td>
<td>Anforderungen und Klassifikation</td>
<td>107</td>
</tr>
<tr>
<td>5.2</td>
<td>Modifikationserkennungswerte</td>
<td>109</td>
</tr>
<tr>
<td>5.3</td>
<td>Nachrichtenauthentisierungswerte</td>
<td>125</td>
</tr>
<tr>
<td>5.4</td>
<td>Authentisierte Verschlüssel</td>
<td>130</td>
</tr>
<tr>
<td>5.5</td>
<td>Zusammenfassung</td>
<td>135</td>
</tr>
<tr>
<td>5.6</td>
<td>Weiterführende Literatur</td>
<td>136</td>
</tr>
<tr>
<td>5.7</td>
<td>Übungen</td>
<td>136</td>
</tr>
<tr>
<td>6</td>
<td>Erzeugung sicherer Zufallszahlen</td>
<td>139</td>
</tr>
<tr>
<td>6.1</td>
<td>Zufallszahlen und Pseudozufallszahlen</td>
<td>139</td>
</tr>
<tr>
<td>6.2</td>
<td>Kryptografisch sichere Zufallszahlen</td>
<td>140</td>
</tr>
<tr>
<td>6.3</td>
<td>Statistische Tests für Zufallszahlen</td>
<td>142</td>
</tr>
<tr>
<td>6.4</td>
<td>Erzeugung von Zufallszahlen</td>
<td>143</td>
</tr>
<tr>
<td>6.5</td>
<td>Erzeugung kryptografisch sicherer Pseudozufallszahlen</td>
<td>145</td>
</tr>
<tr>
<td>6.6</td>
<td>Implementierungssicherheit</td>
<td>148</td>
</tr>
<tr>
<td>6.7</td>
<td>Zusammenfassung</td>
<td>149</td>
</tr>
<tr>
<td>6.8</td>
<td>Weiterführende Literatur</td>
<td>150</td>
</tr>
<tr>
<td>6.9</td>
<td>Übungen</td>
<td>151</td>
</tr>
<tr>
<td>7</td>
<td>Kryptografische Protokolle</td>
<td>153</td>
</tr>
<tr>
<td>7.1</td>
<td>Eigenschaften und Notation kryptografischer Protokolle</td>
<td>153</td>
</tr>
<tr>
<td>7.2</td>
<td>Nachrichten- und Instanzenauthentisierung</td>
<td>156</td>
</tr>
<tr>
<td>7.3</td>
<td>Das Needham-Schroeder-Protokoll</td>
<td>161</td>
</tr>
<tr>
<td>7.4</td>
<td>Kerberos</td>
<td>165</td>
</tr>
<tr>
<td>7.5</td>
<td>Der internationale Standard X.509</td>
<td>175</td>
</tr>
<tr>
<td>7.6</td>
<td>Sicherheit ausgehandelter Sitzungsschlüssel</td>
<td>180</td>
</tr>
<tr>
<td>7.7</td>
<td>Fortgeschrittene Verfahren zur Passwortauthentisierung</td>
<td>182</td>
</tr>
<tr>
<td>7.8</td>
<td>Formale Betrachtung kryptografischer Protokolle</td>
<td>187</td>
</tr>
<tr>
<td>7.9</td>
<td>Zusammenfassung</td>
<td>198</td>
</tr>
<tr>
<td>7.10</td>
<td>Weiterführende Literatur</td>
<td>199</td>
</tr>
<tr>
<td>7.11</td>
<td>Übungen</td>
<td>200</td>
</tr>
</tbody>
</table>
## Inhaltsverzeichnis

### 8 Sichere Gruppenkommunikation

- 8.1 Spezifische Anforderungen sicherer Gruppenkommunikation   203
- 8.2 Aushandlung von Gruppenschlüsseln                     205
- 8.3 Quellenauthentisierung                                   214
- 8.4 Zusammenfassung                                          219
- 8.5 Weiterführende Literatur                                220
- 8.6 Übungen                                                 220

### 9 Zugriffskontrolle

- 9.1 Begriffsdefinitionen und Konzepte                       223
- 9.2 Security Labels                                         225
- 9.3 Spezifikation von Zugriffskontrollrichtlinien           227
- 9.4 Kategorien von Zugriffskontrollmechanismen              228
- 9.5 Zusammenfassung                                         231
- 9.6 Weiterführende Literatur                                231
- 9.7 Übungen                                                 232

### II Netzsicherheit

### 10 Integration von Sicherheitsdiensten

- 10.1 Motivation                                             235
- 10.2 Ein pragmatisches Modell                               237
- 10.3 Überlegungen zur Platzierung von Sicherheitsdiensten   239
- 10.4 Integration in untere Protokollschichten vs. Anwendungen 243
- 10.5 Integration in End- oder Zwischensysteme               245
- 10.6 Zusammenfassung                                        246
- 10.7 Weiterführende Literatur                               247
- 10.8 Übungen                                                247

### 11 Sicherheitsprotokolle der Datensicherungsschicht

- 11.1 Virtuelle Separation von Datenverkehr mit IEEE 802.1Q  250
- 11.2 Sicherung der lokalen Netzinfrastruktur mit IEEE 802.1X 252
- 11.3 Verschlüsselung des Datenverkehrs mit IEEE 802.1AE      255
- 11.4 Point-to-Point Protocol                                 256
- 11.5 Point-to-Point Tunneling Protocol                      266
- 11.6 Virtuelle private Netze                                272
- 11.7 Zusammenfassung                                        274
- 11.8 Weiterführende Literatur                               276
- 11.9 Übungen                                                278
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>Die IPsec-Sicherheitsarchitektur</td>
<td>279</td>
</tr>
<tr>
<td>12.1</td>
<td>Kurze Einführung in die Internetprotokollfamilie</td>
<td>279</td>
</tr>
<tr>
<td>12.2</td>
<td>Überblick über die IPsec-Architektur</td>
<td>284</td>
</tr>
<tr>
<td>12.3</td>
<td>Einsatz des Transport- und des Tunnelmodus</td>
<td>293</td>
</tr>
<tr>
<td>12.4</td>
<td>IPsec-Protokollverarbeitung</td>
<td>297</td>
</tr>
<tr>
<td>12.5</td>
<td>Das ESP-Protokoll</td>
<td>300</td>
</tr>
<tr>
<td>12.6</td>
<td>Das AH-Protokoll</td>
<td>307</td>
</tr>
<tr>
<td>12.7</td>
<td>Das ISAKMP-Protokoll</td>
<td>313</td>
</tr>
<tr>
<td>12.8</td>
<td>Der Internet Key Exchange Version 1</td>
<td>321</td>
</tr>
<tr>
<td>12.9</td>
<td>Der Internet Key Exchange Version 2</td>
<td>329</td>
</tr>
<tr>
<td>12.10</td>
<td>Weitere Aspekte von IPsec</td>
<td>333</td>
</tr>
<tr>
<td>12.11</td>
<td>Zusammenfassung</td>
<td>336</td>
</tr>
<tr>
<td>12.12</td>
<td>Weiterführende Literatur</td>
<td>337</td>
</tr>
<tr>
<td>12.13</td>
<td>Übungen</td>
<td>339</td>
</tr>
<tr>
<td>13</td>
<td>Sicherheitsprotokolle der Transportschicht</td>
<td>341</td>
</tr>
<tr>
<td>13.1</td>
<td>Secure Socket Layer (SSL)</td>
<td>342</td>
</tr>
<tr>
<td>13.2</td>
<td>Transport Layer Security (TLS)</td>
<td>355</td>
</tr>
<tr>
<td>13.3</td>
<td>Datagram Transport Layer Security (DTLS)</td>
<td>363</td>
</tr>
<tr>
<td>13.4</td>
<td>Secure Shell (SSH)</td>
<td>364</td>
</tr>
<tr>
<td>13.5</td>
<td>Zusammenfassung</td>
<td>374</td>
</tr>
<tr>
<td>13.6</td>
<td>Weiterführende Literatur</td>
<td>375</td>
</tr>
<tr>
<td>13.7</td>
<td>Übungen</td>
<td>375</td>
</tr>
<tr>
<td>III</td>
<td>Sichere drahtlose und mobile Kommunikation</td>
<td>377</td>
</tr>
<tr>
<td>14</td>
<td>Sicherheitsaspekte der Mobilkommunikation</td>
<td>379</td>
</tr>
<tr>
<td>14.1</td>
<td>Bedrohungen in Mobilkommunikationsnetzeln</td>
<td>379</td>
</tr>
<tr>
<td>14.2</td>
<td>Wahrung der Vertraulichkeit des Aufenthaltsortes</td>
<td>381</td>
</tr>
<tr>
<td>14.3</td>
<td>Zusammenfassung</td>
<td>386</td>
</tr>
<tr>
<td>14.4</td>
<td>Weiterführende Literatur</td>
<td>386</td>
</tr>
<tr>
<td>14.5</td>
<td>Übungen</td>
<td>387</td>
</tr>
<tr>
<td>15</td>
<td>Sicherheit in drahtlosen lokalen Netzen</td>
<td>389</td>
</tr>
<tr>
<td>15.1</td>
<td>Der Standard IEEE 802.11 für drahtlose lokale Netze</td>
<td>389</td>
</tr>
<tr>
<td>15.2</td>
<td>Instanzenauthentisierung</td>
<td>392</td>
</tr>
<tr>
<td>15.3</td>
<td>Wired Equivalent Privacy</td>
<td>397</td>
</tr>
<tr>
<td>15.4</td>
<td>Robust Secure Networks</td>
<td>404</td>
</tr>
<tr>
<td>15.5</td>
<td>Sicherheit in öffentlichen WLANs</td>
<td>411</td>
</tr>
<tr>
<td>15.6</td>
<td>Zusammenfassung</td>
<td>413</td>
</tr>
<tr>
<td>15.7</td>
<td>Weiterführende Literatur</td>
<td>415</td>
</tr>
<tr>
<td>15.8</td>
<td>Übungen</td>
<td>415</td>
</tr>
<tr>
<td>16</td>
<td>Sicherheit in funkbasierten Weitverkehrsnetzen</td>
<td>417</td>
</tr>
<tr>
<td>----</td>
<td>-----------------------------------------------</td>
<td>-----</td>
</tr>
<tr>
<td>16.1</td>
<td>Global System for Mobile Communication (GSM)</td>
<td>417</td>
</tr>
<tr>
<td>16.2</td>
<td>Universal Mobile Telecommunications System (UMTS)</td>
<td>425</td>
</tr>
<tr>
<td>16.3</td>
<td>Long Term Evolution (LTE)</td>
<td>433</td>
</tr>
<tr>
<td>16.4</td>
<td>Zusammenfassung</td>
<td>438</td>
</tr>
<tr>
<td>16.5</td>
<td>Weiterführende Literatur</td>
<td>439</td>
</tr>
<tr>
<td>16.6</td>
<td>Übungen</td>
<td>440</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IV</th>
<th>Schutz von Kommunikationsinfrastrukturen</th>
<th>441</th>
</tr>
</thead>
<tbody>
<tr>
<td>17</td>
<td>Schutz von Kommunikation und Infrastruktur in offenen Netzen</td>
<td>443</td>
</tr>
<tr>
<td>17.1</td>
<td>Systematische Bedrohungsanalyse</td>
<td>444</td>
</tr>
<tr>
<td>17.2</td>
<td>Sicherheit von Endsystemen</td>
<td>448</td>
</tr>
<tr>
<td>17.3</td>
<td>Zusammenfassung</td>
<td>460</td>
</tr>
<tr>
<td>17.4</td>
<td>Weiterführende Literatur</td>
<td>461</td>
</tr>
<tr>
<td>17.5</td>
<td>Übungen</td>
<td>462</td>
</tr>
<tr>
<td>18</td>
<td>Verfügbarkeit des Datentransports</td>
<td>463</td>
</tr>
<tr>
<td>18.1</td>
<td>Sabotageangriffe</td>
<td>463</td>
</tr>
<tr>
<td>18.2</td>
<td>Verteilte Sabotageangriffe</td>
<td>471</td>
</tr>
<tr>
<td>18.3</td>
<td>Gegenmaßnahmen</td>
<td>473</td>
</tr>
<tr>
<td>18.4</td>
<td>Zusammenfassung</td>
<td>485</td>
</tr>
<tr>
<td>18.5</td>
<td>Weiterführende Literatur</td>
<td>486</td>
</tr>
<tr>
<td>18.6</td>
<td>Übungen</td>
<td>487</td>
</tr>
<tr>
<td>19</td>
<td>Routing-Sicherheit</td>
<td>489</td>
</tr>
<tr>
<td>19.1</td>
<td>Kryptografische Sicherung von BGP</td>
<td>493</td>
</tr>
<tr>
<td>19.2</td>
<td>Erkennung von Routing-Anomalien*</td>
<td>503</td>
</tr>
<tr>
<td>19.3</td>
<td>Zusammenfassung</td>
<td>508</td>
</tr>
<tr>
<td>19.4</td>
<td>Weiterführende Literatur</td>
<td>510</td>
</tr>
<tr>
<td>19.5</td>
<td>Übungen</td>
<td>511</td>
</tr>
<tr>
<td>20</td>
<td>Sichere Namensauflösung</td>
<td>513</td>
</tr>
<tr>
<td>20.1</td>
<td>Funktionsweise von DNS</td>
<td>513</td>
</tr>
<tr>
<td>20.2</td>
<td>Sicherheitsziele und Bedrohungen</td>
<td>515</td>
</tr>
<tr>
<td>20.3</td>
<td>Sicherer Einsatz von traditionellem DNS</td>
<td>522</td>
</tr>
<tr>
<td>20.4</td>
<td>Kryptografische Sicherung von DNS</td>
<td>524</td>
</tr>
<tr>
<td>20.5</td>
<td>Zusammenfassung</td>
<td>537</td>
</tr>
<tr>
<td>20.6</td>
<td>Weiterführende Literatur</td>
<td>538</td>
</tr>
<tr>
<td>20.7</td>
<td>Übungen</td>
<td>539</td>
</tr>
</tbody>
</table>
21 Internet-Firewalls ........................................... 541
21.1 Aufgaben und Grundprinzipien einer Firewall .......... 541
21.2 Firewall-relevante Internetdienste und Protokolle ....... 544
21.3 Terminologie und Grundbausteine ....................... 546
21.4 Firewall-Architekturen ..................................... 548
21.5 Paketfilterung .............................................. 552
21.6 Bastion Hosts und Proxyserver ............................. 557
21.7 Weitere Aspekte moderner Firewall-Systeme ............. 560
21.8 Zusammenfassung ........................................... 561
21.9 Weiterführende Literatur .................................... 562
21.10 Übungen ..................................................... 563

22 Automatisierte Angriffserkennung und -reaktion ........ 565
22.1 Arbeitsweise und Ziele von Intrusion-Detection-Systemen 566
22.2 Aufbau und Funktionsweise netzwerkbasierter IDS .... 570
22.3 Reaktion auf Angriffe und automatische Unterbindung .. 581
22.4 Techniken zur Umgehung von NIDS .................... 583
22.5 Zusammenfassung ........................................... 586
22.6 Weiterführende Literatur .................................... 587
22.7 Übungen ..................................................... 588

23 Verwaltung komplexer Kommunikationsinfrastrukturen* 589
23.1 Automatisches Zertifikatsmanagement ..................... 589
23.2 Automatische VPN-Konfiguration ......................... 597
23.3 Zusammenfassung ........................................... 612
23.4 Weiterführende Literatur .................................... 614
23.5 Übungen ..................................................... 616

Literaturverzeichnis .............................................. 617

Abkürzungsverzeichnis ........................................... 647

Index .............................................................. 656