

# Inhaltsverzeichnis

|               |  |           |
|---------------|--|-----------|
|               | <b>Vorwort</b> .....   | <b>11</b> |
| <b>1</b>      | <b>Einführung</b> .....  | <b>15</b> |
| 1.1           | Angriffe, Dienste und Mechanismen .....                                    | 18        |
| 1.1.1         | Dienste .....  | 18        |
| 1.1.2         | Mechanismen .....  | 20        |
| 1.1.3         | Angriffe .....   | 21        |
| 1.2           | Sicherheitsangriffe .....  | 22        |
| 1.2.1         | Passive Angriffe .....   | 23        |
| 1.2.2         | Aktive Angriffe .....  | 24        |
| 1.3           | Sicherheitsdienste .....   | 25        |
| 1.3.1         | Vertraulichkeit .....  | 25        |
| 1.3.2         | Authentifizierung .....  | 26        |
| 1.3.3         | Integrität .....   | 26        |
| 1.3.4         | Nicht-Anfechtbarkeit .....   | 27        |
| 1.3.5         | Zugriffssteuerung .....  | 27        |
| 1.3.6         | Verfügbarkeit .....  | 27        |
| 1.4           | Ein Netzwerksicherheitsmodell .....  | 27        |
| 1.5           | Internet-Standards und RFCs .....  | 30        |
| 1.5.1         | Die Internet Society .....   | 30        |
| 1.5.2         | RFC-Veröffentlichung .....   | 31        |
| 1.5.3         | Der Standardisierungsprozess .....   | 31        |
| 1.5.4         | Erfassung von Nicht-Standards .....  | 33        |
| 1.6           | Empfohlene Lektüre .....   | 33        |
| 1.7           | Anhang 1A Quellen im Internet .....  | 33        |
| 1.7.1         | Web-Sites für dieses Buch .....  | 34        |
| 1.7.2         | Andere Web-Sites .....   | 34        |
| 1.7.3         | USENET Newsgroups .....  | 35        |
| <b>Teil 1</b> | <b>Kryptographie</b> .....   | <b>37</b> |
| <b>2</b>      | <b>Herkömmliche Verschlüsselungstechniken<br/>und Briefgeheimnis</b> ..... | <b>39</b> |
| 2.1           | Herkömmliche Verschlüsselungsprinzipien .....                              | 39        |
| 2.1.1         | Kryptographie .....  | 41        |

|          |  |           |
|----------|--|-----------|
| 2.1.2    | Kryptoanalyse  | 41        |
| 2.1.3    | Der Feistel-Verschlüsselungsalgorithmus                          | 44        |
| 2.2      | Herkömmliche Verschlüsselungsalgorithmen                         | 47        |
| 2.2.1    | Der Data Encryption Standard (DES)                               | 47        |
| 2.2.2    | Triple DEA   | 52        |
| 2.2.3    | Der Advanced Encryption Standard                                 | 54        |
| 2.2.4    | Andere symmetrische Blockverschlüsselungen                       | 55        |
| 2.3      | Betriebsmodi von Blockverschlüsselungen                          | 58        |
| 2.3.1    | CBC-Modus (Cipher Block Chaining)                                | 59        |
| 2.3.2    | CFB-Modus (Cipher Feedback)                                      | 61        |
| 2.4      | Verschlüsselungsort  | 63        |
| 2.5      | Schlüsselverteilung  | 64        |
| 2.6      | Empfohlene Lektüre   | 67        |
| 2.7      | Aufgaben   | 67        |
| <b>3</b> | <b>Public-Key-Kryptographie und Nachrichtenauthentifizierung</b> | <b>71</b> |
| 3.1      | Verfahren der Nachrichtenauthentifizierung                       | 71        |
| 3.1.1    | Authentifizierung mit herkömmlicher Verschlüsselung              | 71        |
| 3.1.2    | Nachrichtenauthentifizierung ohne Nachrichtenverschlüsselung     | 72        |
| 3.1.3    | Nachrichtenauthentifizierungscode                                | 73        |
| 3.1.4    | Einweg-Hash-Funktion   | 74        |
| 3.2      | Sichere Hash-Funktionen und HMAC                                 | 76        |
| 3.2.1    | Anforderungen an Hash-Funktionen                                 | 77        |
| 3.2.2    | Einfache Hash-Funktionen   | 78        |
| 3.2.3    | Die sichere Hash-Funktion SHA-1                                  | 80        |
| 3.2.4    | Andere sichere Hash-Funktionen                                   | 83        |
| 3.2.5    | HMAC   | 85        |
| 3.3      | Grundlagen der Public-Key-Kryptographie                          | 87        |
| 3.3.1    | Struktur der Public-Key-Verschlüsselung                          | 88        |
| 3.3.2    | Anwendungen von Public-Key-Verschlüsselung                       | 91        |
| 3.3.3    | Anforderungen an die Public-Key-Kryptographie                    | 92        |
| 3.4      | Algorithmen der Public-Key-Kryptographie                         | 93        |
| 3.4.1    | Der Public-Key-Verschlüsselungsalgorithmus RSA                   | 93        |
| 3.4.2    | Diffie-Hellman-Schlüsselaustausch                                | 96        |
| 3.4.3    | Andere Algorithmen der Public-Key-Kryptographie                  | 99        |
| 3.5      | Digitale Unterschriften  | 100       |
| 3.6      | Schlüsselverwaltung  | 101       |
| 3.6.1    | Digitale Zertifikate   | 102       |
| 3.6.2    | Verteilung geheimer Schlüssel mittels öffentlicher Schlüssel     | 102       |
| 3.7      | Empfohlene Lektüre   | 104       |

|               |   |            |
|---------------|---|------------|
| 3.8           | Aufgaben .....                                      | 105        |
| 3.9           | Anhang 3A: Primzahlen und modulare Arithmetik ..... | 108        |
| 3.9.1         | Primzahlen und relative Primzahlen .....            | 108        |
| <b>Teil 2</b> | <b>Anwendungen für die Netzwerksicherheit .....</b> | <b>113</b> |
| <b>4</b>      | <b>Authentifizierungsanwendungen .....</b>          | <b>115</b> |
| 4.1           | Kerberos .....                                      | 115        |
| 4.1.1         | Motivation .....                                    | 116        |
| 4.1.2         | Kerberos Version 4 .....                            | 118        |
| 4.1.3         | Kerberos Version 5 .....                            | 131        |
| 4.2           | X.509-Authentifizierungsdienst .....                | 138        |
| 4.2.1         | Zertifikate .....                                   | 139        |
| 4.2.2         | Authentifizierungsverfahren .....                   | 144        |
| 4.2.3         | X.509 Version 3 .....                               | 147        |
| 4.3           | Empfohlene Lektüre und Web-Sites .....              | 150        |
| 4.4           | Aufgaben .....                                      | 150        |
| 4.5           | ANHANG 4A: Kerberos-Verschlüsselungsverfahren ..... | 152        |
| 4.5.1         | Passwort-Schlüssel-Umwandlung .....                 | 152        |
| 4.5.2         | Propagating Cipher Block Chaining Mode (PCBC) ..... | 153        |
| <b>5</b>      | <b>E-Mail-Sicherheit .....</b>                      | <b>155</b> |
| 5.1           | Pretty Good Privacy (PGP) .....                     | 155        |
| 5.1.1         | Notation .....                                      | 156        |
| 5.1.2         | Verfahrensweise .....                               | 157        |
| 5.1.3         | Kryptographische Schlüssel und Schlüsselringe ..... | 164        |
| 5.1.4         | Verwaltung von öffentlichen Schlüsseln .....        | 173        |
| 5.2           | S/MIME .....  | 180        |
| 5.2.1         | RFC 822 .....                                       | 180        |
| 5.2.2         | Multipurpose Internet Mail Extensions .....         | 181        |
| 5.2.3         | S/MIME-Funktionalität .....                         | 187        |
| 5.2.4         | S/MIME-Nachrichten .....                            | 192        |
| 5.2.5         | S/MIME-Zertifizierungsverfahren .....               | 197        |
| 5.2.6         | Erweiterte Sicherheitsdienste .....                 | 200        |
| 5.3           | Empfohlene Web-Sites .....                          | 200        |
| 5.4           | Aufgaben .....                                      | 201        |
| 5.5           | Anhang 5A: Datenkomprimierung mit ZIP .....         | 202        |
| 5.5.1         | Komprimierungsalgorithmus .....                     | 203        |
| 5.5.2         | Dekomprimierungsalgorithmus .....                   | 204        |

|          |  |            |
|----------|--|------------|
| 5.6      | ANHANG 5B: Radix-64-Umwandlung .....                       | 205        |
| 5.7      | ANHANG 5C: PGP-Zufallszahlengenerierung .....              | 207        |
| 5.7.1    | Echte Zufallszahlen .....                                  | 207        |
| 5.7.2    | Pseudozufallszahlen .....                                  | 208        |
| <b>6</b> | <b>IP-Sicherheit .....</b>                                 | <b>211</b> |
| 6.1      | IP-Sicherheit – ein Überblick .....                        | 211        |
| 6.1.1    | Anwendungen von IPSec .....                                | 212        |
| 6.1.2    | Vorteile von IPSec .....                                   | 213        |
| 6.1.3    | Routing-Anwendungen .....                                  | 214        |
| 6.2      | IP-Sicherheitsaufbau .....                                 | 215        |
| 6.2.1    | IPSec-Dokumente .....                                      | 215        |
| 6.2.2    | IPSec-Dienste .....  | 216        |
| 6.2.3    | Sicherheitsverknüpfung (Security Association – SA) .....   | 217        |
| 6.2.4    | Transport- und Tunnelmodus .....                           | 221        |
| 6.3      | Authentifizierungs-Header .....                            | 223        |
| 6.3.1    | Wiederholungsvermeidung .....                              | 225        |
| 6.3.2    | Integritätsprüfwert .....                                  | 226        |
| 6.3.3    | Transport- und Tunnelmodus .....                           | 227        |
| 6.4      | Encapsulating Security Payload (ESP) .....                 | 229        |
| 6.4.1    | ESP-Format .....   | 229        |
| 6.4.2    | Verschlüsselungs- und Authentifizierungsalgorithmen .....  | 230        |
| 6.4.3    | Padding .....  | 231        |
| 6.4.4    | Transport- und Tunnelmodus .....                           | 232        |
| 6.5      | Kombinationen von Sicherheitsverknüpfungen .....           | 236        |
| 6.5.1    | Authentifizierung plus Vertraulichkeit .....               | 237        |
| 6.5.2    | Grundlegende Kombinationen von Sicherheitsverknüpfungen .. | 238        |
| 6.6      | Schlüsselverwaltung .....                                  | 240        |
| 6.6.1    | Oakley-Protokoll zur Schlüsselbestimmung .....             | 241        |
| 6.6.2    | ISAKMP .....   | 246        |
| 6.7      | Empfohlene Lektüre und Web-Sites .....                     | 254        |
| 6.8      | Aufgaben .....   | 255        |
| 6.9      | Anhang 6A: Netzwerkarbeit und Internet-Protokolle .....    | 256        |
| 6.9.1    | Die Aufgabe eines Internet-Protokolls .....                | 256        |
| 6.9.2    | IPv4 .....   | 258        |
| 6.9.3    | IPv6 .....   | 261        |
| <b>7</b> | <b>Netzsicherheit .....</b>                                | <b>267</b> |
| 7.1      | Überlegungen zur Netzsicherheit .....                      | 267        |
| 7.1.1    | Bedrohungen der Netzsicherheit .....                       | 268        |
| 7.1.2    | Vorgehensweisen zur Verkehrssicherheit im Netz .....       | 270        |

|               |   |            |
|---------------|---|------------|
| 7.2           | Secure-Socket-Layer-Sicherheit und Transportschichtsicherheit | 271        |
| 7.2.1         | SSL-Aufbau  | 271        |
| 7.2.2         | SSL-Record-Protokoll  | 273        |
| 7.2.3         | Change-Cipher-Spec-Protokoll                                  | 277        |
| 7.2.4         | Das Alert-Protokoll   | 277        |
| 7.2.5         | Das Handshake-Protokoll                                       | 279        |
| 7.2.6         | Kryptographische Berechnungen                                 | 286        |
| 7.2.7         | Sicherheit der Transportschicht                               | 287        |
| 7.3           | Secure Electronic Transactions (SET)                          | 293        |
| 7.3.1         | Überblick über SET  | 294        |
| 7.3.2         | Duale Signatur  | 299        |
| 7.3.3         | Zahlungsprozess   | 300        |
| 7.4           | Empfohlene Lektüre und Web-Sites                              | 307        |
| 7.5           | Aufgaben  | 308        |
| <b>8</b>      | <b>Sicherheit in der Netzwerkverwaltung</b>                   | <b>311</b> |
| 8.1           | Die Grundlagen von SNMP                                       | 312        |
| 8.1.1         | Aufbau der Netzwerkverwaltung                                 | 312        |
| 8.1.2         | Aufbau des Netzwerkverwaltungsprotokolls                      | 314        |
| 8.1.3         | Proxies   | 315        |
| 8.1.4         | SNMPv2  | 317        |
| 8.2           | SNMPv1-Verbundeinrichtungen                                   | 321        |
| 8.2.1         | Verbunde und Verbundnamen                                     | 321        |
| 8.2.2         | Authentifizierungsdienst                                      | 322        |
| 8.2.3         | Zugriffsrichtlinien   | 323        |
| 8.2.4         | Proxy-Dienst  | 324        |
| 8.3           | SNMPv3  | 324        |
| 8.3.1         | Der Aufbau von SNMP   | 326        |
| 8.3.2         | Nachrichtenverarbeitung und das Benutzer-Sicherheitsmodell    | 336        |
| 8.3.3         | Sichtbasierte Zugriffssteuerung                               | 350        |
| 8.4           | Empfohlene Lektüre und Web-Sites                              | 355        |
| 8.5           | Aufgaben  | 356        |
| <b>Teil 3</b> | <b>Systemsisicherheit</b>                                     | <b>361</b> |
| <b>9</b>      | <b>Eindringlinge und Viren</b>                                | <b>363</b> |
| 9.1           | Eindringlinge   | 363        |
| 9.1.1         | Techniken des Eindringens                                     | 366        |
| 9.1.2         | Passwortschutz  | 368        |
| 9.1.3         | Die Anfälligkeit von Passwörtern                              | 369        |

|           |  |            |
|-----------|--|------------|
| 9.1.4     | Strategien zur Passwortwahl .....                | 373        |
| 9.1.5     | Erkennung von Eindringlingen .....               | 379        |
| 9.2       | Viren und ähnliche Bedrohungen .....             | 392        |
| 9.2.1     | Bösartige Programme .....                        | 393        |
| 9.2.2     | Die Natur der Viren .....                        | 397        |
| 9.2.3     | Virenarten .....                                 | 401        |
| 9.2.4     | Makroviren .....                                 | 402        |
| 9.2.5     | Antivirenmethoden .....                          | 404        |
| 9.2.6     | Erweiterte Antiviren-Techniken .....             | 405        |
| 9.3       | Empfohlene Lektüre und Web-Sites .....           | 408        |
| 9.4       | Aufgaben .....                                   | 409        |
| <b>10</b> | <b>Firewalls .....</b>                           | <b>413</b> |
| 10.1      | Entwurfsprinzipien von Firewalls .....           | 413        |
| 10.1.1    | Merkmale von Firewalls .....                     | 414        |
| 10.1.2    | Arten von Firewalls .....                        | 416        |
| 10.1.3    | Firewall-Konfigurationen .....                   | 423        |
| 10.2      | Gesicherte Systeme .....                         | 426        |
| 10.2.1    | Zugriffssteuerung .....                          | 426        |
| 10.2.2    | Das Konzept gesicherter Systeme .....            | 428        |
| 10.2.3    | Abwehr Trojanischer Pferde .....                 | 431        |
| 10.3      | Empfohlene Lektüre .....                         | 432        |
| 10.4      | Aufgaben .....                                   | 433        |
| <b>A</b>  | <b>In diesem Buch zitierte RFCs .....</b>        | <b>435</b> |
| <b>B</b>  | <b>Lehrprojekte zur Netzwerksicherheit .....</b> | <b>439</b> |
| B.1       | Forschungsprojekte .....                         | 439        |
| B.2       | Programmierprojekte .....                        | 440        |
| B.3       | Lese-/Berichtsaufgaben .....                     | 441        |
| <b>C</b>  | <b>Glossar .....</b>                             | <b>443</b> |
| <b>D</b>  | <b>Literaturverzeichnis .....</b>                | <b>449</b> |
| <b>E</b>  | <b>Akronyme .....</b>                            | <b>457</b> |
|           | <b>Stichwortverzeichnis .....</b>                | <b>459</b> |