

# Inhaltsverzeichnis

|          |                                       |          |
|----------|---------------------------------------|----------|
| <b>1</b> | <b>Einführung</b>                     | <b>1</b> |
| 1.1      | Motivation                            | 1        |
| 1.2      | Kapitelüberblick                      | 2        |
| 1.3      | Für wen dieses Buch geschrieben wurde | 3        |
| 1.4      | Über den Autor                        | 3        |
|          | Literatur                             | 4        |

## Teil I Grundlagen

|          |                                                          |          |
|----------|----------------------------------------------------------|----------|
| <b>2</b> | <b>Grundlagen der Netzwerktechnik</b>                    | <b>7</b> |
| 2.1      | Einführung                                               | 7        |
| 2.1.1    | Reichweite von Netzwerken                                | 8        |
| 2.1.2    | Netzwerktopologien                                       | 9        |
| 2.1.3    | Netzwerkarchitekturen                                    | 9        |
| 2.2      | Datenpakete, Einkapselung und die Entwicklung von TCP/IP | 12       |
| 2.2.1    | Einige Worte zum OSI-Modell                              | 14       |
| 2.2.2    | OSI- vs. TCP/IP-Modell                                   | 15       |
| 2.2.3    | Das Hybridmodell von Tanenbaum                           | 15       |
| 2.3      | Grundzüge des TCP/IP-Modells                             | 16       |
| 2.3.1    | Link Layer                                               | 16       |
| 2.3.2    | Internet Layer                                           | 26       |
| 2.3.3    | Transport Layer                                          | 28       |
| 2.3.4    | Application Layer                                        | 29       |
| 2.3.5    | Zusammenfassung                                          | 30       |
| 2.4      | Die wichtigsten Protokolle                               | 30       |
| 2.5      | Link Layer: ARP                                          | 30       |
| 2.5.1    | Reverse-ARP                                              | 32       |
| 2.5.2    | Proxy-ARP                                                | 32       |

|        |                                                           |    |
|--------|-----------------------------------------------------------|----|
| 2.6    | Internet Layer: IPv4 . . . . .                            | 32 |
| 2.6.1  | IP-Adressen . . . . .                                     | 35 |
| 2.6.2  | Fragmentierung . . . . .                                  | 37 |
| 2.7    | Internet Layer: ICMPv4 . . . . .                          | 39 |
| 2.7.1  | ICMP-Types 0 und 8 . . . . .                              | 39 |
| 2.7.2  | ICMP-Type 3 . . . . .                                     | 40 |
| 2.7.3  | ICMP-Type 4 . . . . .                                     | 41 |
| 2.7.4  | ICMP-Type 5 . . . . .                                     | 41 |
| 2.7.5  | ICMP-Types 9 und 10 . . . . .                             | 41 |
| 2.7.6  | ICMP-Type 11 . . . . .                                    | 42 |
| 2.7.7  | ICMP-Type 12 . . . . .                                    | 42 |
| 2.7.8  | Weitere ICMP-Typen . . . . .                              | 43 |
| 2.8    | Internet Layer: IGMP . . . . .                            | 43 |
| 2.8.1  | Der IGMPv2-Header . . . . .                               | 43 |
| 2.9    | Internet Layer: IPv6 . . . . .                            | 44 |
| 2.9.1  | IPv6-Adressen . . . . .                                   | 46 |
| 2.9.2  | IPv6 Header Extensions . . . . .                          | 46 |
| 2.10   | Internet Layer: ICMPv6 . . . . .                          | 47 |
| 2.11   | Transport Layer: UDP . . . . .                            | 49 |
| 2.11.1 | Der UDP-Header . . . . .                                  | 49 |
| 2.12   | Transport Layer: TCP . . . . .                            | 50 |
| 2.12.1 | TCP-Reliability . . . . .                                 | 50 |
| 2.12.2 | Sende- und Empfangspuffer . . . . .                       | 52 |
| 2.12.3 | Flusskontrolle (Flow-Control) . . . . .                   | 52 |
| 2.12.4 | Header . . . . .                                          | 53 |
| 2.12.5 | Kommunikationsphasen . . . . .                            | 54 |
| 2.13   | Application Layer: DHCP . . . . .                         | 58 |
| 2.14   | Application Layer: HTTP . . . . .                         | 58 |
| 2.14.1 | Aufbau des HTTP-Headers . . . . .                         | 59 |
| 2.14.2 | HTTP/2 und HTTP/3 . . . . .                               | 62 |
| 2.15   | Application Layer: DNS . . . . .                          | 63 |
| 2.15.1 | Resource Records . . . . .                                | 65 |
| 2.15.2 | Resolving . . . . .                                       | 65 |
| 2.15.3 | Der DNS-Header . . . . .                                  | 66 |
| 2.15.4 | DNS-Tools . . . . .                                       | 68 |
| 2.16   | Application Layer: E-Mail- und Usenetprotokolle . . . . . | 70 |
| 2.16.1 | POP3 . . . . .                                            | 71 |
| 2.16.2 | IMAP . . . . .                                            | 72 |
| 2.16.3 | SMTP . . . . .                                            | 75 |
| 2.16.4 | NNTP (Usenet) . . . . .                                   | 76 |

|          |                                                         |           |
|----------|---------------------------------------------------------|-----------|
| 2.17     | Application Layer: sonstige Protokolle . . . . .        | 79        |
| 2.18     | Ausblick . . . . .                                      | 80        |
| 2.19     | Zusammenfassung . . . . .                               | 81        |
| 2.20     | Weiterführende Literatur . . . . .                      | 81        |
| 2.21     | Übungsaufgaben. . . . .                                 | 81        |
|          | Literatur. . . . .                                      | 83        |
| <b>3</b> | <b>Grundlagen der IT-Sicherheit . . . . .</b>           | <b>85</b> |
| 3.1      | Einführung . . . . .                                    | 85        |
| 3.2      | Schutzziele der IT-Sicherheit . . . . .                 | 89        |
| 3.3      | Schwachstellen, Verwundbarkeiten und Co. . . . .        | 90        |
| 3.4      | Zugriffskontrolle . . . . .                             | 91        |
|          | 3.4.1 Discretionary Access Control (DAC). . . . .       | 92        |
|          | 3.4.2 DAC-Erweiterungen. . . . .                        | 92        |
|          | 3.4.3 MAC und DAC: Das Bell-LaPadula-Modell . . . . .   | 93        |
| 3.5      | Authentifizierung . . . . .                             | 95        |
| 3.6      | Privatsphäre . . . . .                                  | 97        |
|          | 3.6.1 Anonymität und Pseudonymität. . . . .             | 97        |
|          | 3.6.2 Verkettbarkeit und Verfolgbarkeit . . . . .       | 98        |
|          | 3.6.3 Überwachung . . . . .                             | 99        |
| 3.7      | Schadsoftware . . . . .                                 | 101       |
|          | 3.7.1 Arten von Schadsoftware . . . . .                 | 101       |
|          | 3.7.2 Schadsoftware-Mechanismen . . . . .               | 104       |
| 3.8      | IT-Sicherheit: ein Trade-off samt Vorschriften. . . . . | 105       |
| 3.9      | Science of Security. . . . .                            | 106       |
| 3.10     | Zusammenfassung . . . . .                               | 107       |
| 3.11     | Weiterführende Literatur . . . . .                      | 108       |
| 3.12     | Übungsaufgaben. . . . .                                 | 108       |
|          | Literatur. . . . .                                      | 109       |

**Teil II Kryptografie**

|          |                                                                    |            |
|----------|--------------------------------------------------------------------|------------|
| <b>4</b> | <b>Einführung in die Kryptografie. . . . .</b>                     | <b>113</b> |
| 4.1      | Einführung und Grundbegriffe. . . . .                              | 113        |
| 4.2      | Grundlegende Begriffe. . . . .                                     | 116        |
|          | 4.2.1 Verschlüsselung und Entschlüsselung als Abbildungen. . . . . | 116        |
|          | 4.2.2 Kryptografische Schlüssel . . . . .                          | 116        |
|          | 4.2.3 Kryptosysteme . . . . .                                      | 117        |
|          | 4.2.4 Symmetrische und Asymmetrische Kryptografie. . . . .         | 118        |
|          | 4.2.5 Grundlegendes Angreifermodell . . . . .                      | 118        |
| 4.3      | Historische Verfahren . . . . .                                    | 119        |

|        |                                                        |     |
|--------|--------------------------------------------------------|-----|
| 4.3.1  | Transpositionschiffre .....                            | 119 |
| 4.3.2  | Die Caesar-Chiffre .....                               | 120 |
| 4.3.3  | Die Vigenère-Chiffre .....                             | 121 |
| 4.3.4  | Die Vernam-Chiffre (One-Time-Pad).....                 | 121 |
| 4.4    | Kryptoanalyse für historische Chiffren .....           | 123 |
| 4.4.1  | Skytale-Chiffre.....                                   | 123 |
| 4.4.2  | Caesar-Chiffre .....                                   | 123 |
| 4.4.3  | Kryptoanalyse der Vigenère-Chiffre .....               | 124 |
| 4.4.4  | Kryptoanalyse der Vernam-Chiffre .....                 | 126 |
| 4.4.5  | Weitere Anmerkungen zu historischen Chiffren .....     | 127 |
| 4.5    | Stromchiffren und Zufallszahlengeneratoren.....        | 127 |
| 4.5.1  | Zufallszahlengeneratoren (PRNG).....                   | 127 |
| 4.5.2  | Der RC4-Algorithmus .....                              | 129 |
| 4.5.3  | Die A5/1- und A5/2-Algorithmen .....                   | 130 |
| 4.6    | Blockchiffren .....                                    | 131 |
| 4.6.1  | Der Data Encryption Standard (DES) .....               | 131 |
| 4.6.2  | Der Advanced Encryption Standard (AES) .....           | 137 |
| 4.6.3  | Blockchiffren-Betriebsmodi.....                        | 138 |
| 4.7    | Informationstheorie und Kryptografie .....             | 140 |
| 4.7.1  | Grundzüge der Informationstheorie.....                 | 140 |
| 4.7.2  | Informationstheorie in der Kryptografie .....          | 143 |
| 4.7.3  | Redundanz .....                                        | 144 |
| 4.7.4  | Sicherheit eines Kryptosystems .....                   | 144 |
| 4.7.5  | Abschätzung der Spurious Keys .....                    | 145 |
| 4.7.6  | Unizitätsdistanz .....                                 | 146 |
| 4.8    | Kryptografische Hashfunktionen .....                   | 147 |
| 4.8.1  | Einweg-Hashfunktionen.....                             | 147 |
| 4.8.2  | Kollisionsresistenz .....                              | 147 |
| 4.8.3  | Geburtsangriff und Substitutionsattacke .....          | 149 |
| 4.8.4  | Hashwertlänge im Kontext von Angriffen .....           | 150 |
| 4.8.5  | Wörterbuchangriff (Brute-Force-Angriff) .....          | 151 |
| 4.8.6  | Hashwerttabellen und Regenbogentabellen .....          | 151 |
| 4.8.7  | Sicherheit von Hashfunktionen .....                    | 153 |
| 4.8.8  | Aufbau einer typischen Hashfunktion .....              | 154 |
| 4.8.9  | Message Authentication Codes (MAC) .....               | 154 |
| 4.8.10 | Hashfunktionen und Unix-Passwortdateien.....           | 156 |
| 4.8.11 | Hashfunktionen und Filesystem Intrusion Detection..... | 157 |
| 4.8.12 | Hashfunktionen und Software Ports.....                 | 157 |
| 4.8.13 | Hashfunktionen und Hashbäume .....                     | 158 |
| 4.9    | Asymmetrische Kryptografie .....                       | 159 |
| 4.9.1  | Schlüsselaustausch.....                                | 159 |
| 4.9.2  | Rivest-Shamir-Adleman-Algorithmus (RSA) .....          | 162 |

|          |                                                                            |            |
|----------|----------------------------------------------------------------------------|------------|
| 4.10     | Digitale Signaturen . . . . .                                              | 163        |
| 4.11     | Zusammenfassung . . . . .                                                  | 164        |
| 4.12     | Weiterführende Literatur . . . . .                                         | 165        |
| 4.13     | Übungsaufgaben. . . . .                                                    | 165        |
|          | Literatur. . . . .                                                         | 169        |
| <b>5</b> | <b>Weiterführende Themen der Kryptografie. . . . .</b>                     | <b>171</b> |
| 5.1      | Einführung . . . . .                                                       | 171        |
| 5.2      | Public Key Infrastructure . . . . .                                        | 172        |
| 5.2.1    | Digitale Zertifikate und PKI-Bestandteile . . . . .                        | 172        |
| 5.2.2    | Vertrauensmodelle . . . . .                                                | 174        |
| 5.3      | Virtuelle Private Netzwerke . . . . .                                      | 177        |
| 5.3.1    | IPSec . . . . .                                                            | 178        |
| 5.3.2    | Transport Layer Security (TLS). . . . .                                    | 183        |
| 5.4      | Anonymität und Onion-Routing . . . . .                                     | 185        |
| 5.4.1    | Grundzüge der Mixe . . . . .                                               | 185        |
| 5.4.2    | Angriffe gegen Anonymisierungssysteme . . . . .                            | 187        |
| 5.5      | Visuelle Kryptografie . . . . .                                            | 188        |
| 5.6      | Secure Multi-Party Computation und homomorphe<br>Verschlüsselung . . . . . | 188        |
| 5.6.1    | Dining Cryptographers. . . . .                                             | 189        |
| 5.7      | Geteilte Geheimnisse . . . . .                                             | 190        |
| 5.8      | Zusammenfassung . . . . .                                                  | 191        |
| 5.9      | Weiterführende Literatur . . . . .                                         | 191        |
| 5.10     | Übungsaufgaben. . . . .                                                    | 191        |
|          | Literatur. . . . .                                                         | 192        |

### Teil III Netzwerksicherheit

|          |                                                              |            |
|----------|--------------------------------------------------------------|------------|
| <b>6</b> | <b>Einführung in die Netzwerksicherheit . . . . .</b>        | <b>197</b> |
| 6.1      | Einführung . . . . .                                         | 197        |
| 6.2      | Angriff . . . . .                                            | 197        |
| 6.2.1    | Scanning. . . . .                                            | 198        |
| 6.2.2    | Wireless Wardriving. . . . .                                 | 198        |
| 6.2.3    | Protocol Fuzzing . . . . .                                   | 198        |
| 6.2.4    | Sniffer und Promiscuous Mode . . . . .                       | 199        |
| 6.2.5    | Man-in-the-Middle- und Spoofing-Angriffe . . . . .           | 199        |
| 6.2.6    | Redirects (Routing-Angriffe). . . . .                        | 200        |
| 6.2.7    | Denial-of-Service (DoS) . . . . .                            | 201        |
| 6.2.8    | Exploits . . . . .                                           | 203        |
| 6.2.9    | Social Engineering und Advanced Persistent Threats . . . . . | 203        |
| 6.3      | Verteidigung . . . . .                                       | 204        |
| 6.3.1    | Firewalls. . . . .                                           | 205        |

|          |                                                         |            |
|----------|---------------------------------------------------------|------------|
| 6.3.2    | Intrusion Detection und Prevention . . . . .            | 206        |
| 6.3.3    | Honeypots und Honeynets . . . . .                       | 209        |
| 6.3.4    | Sandboxing . . . . .                                    | 211        |
| 6.3.5    | Threat Intelligence . . . . .                           | 211        |
| 6.3.6    | Social Engineering verhindern . . . . .                 | 213        |
| 6.4      | Zusammenfassung . . . . .                               | 213        |
| 6.5      | Weiterführende Literatur . . . . .                      | 213        |
| 6.6      | Übungsaufgaben . . . . .                                | 214        |
|          | Literatur . . . . .                                     | 214        |
| <b>7</b> | <b>Angriffe auf TCP/IP-Netzwerkprotokolle . . . . .</b> | <b>217</b> |
| 7.1      | Einführung . . . . .                                    | 217        |
| 7.2      | Angriffe auf der Netzzugangsschicht . . . . .           | 218        |
| 7.2.1    | Angriffe mit physikalischer Grobeinwirkung . . . . .    | 218        |
| 7.2.2    | Jamming . . . . .                                       | 218        |
| 7.2.3    | Eavesdropping (Sniffing) . . . . .                      | 218        |
| 7.2.4    | Falsche Access Points . . . . .                         | 220        |
| 7.2.5    | Sicherheit von ARP . . . . .                            | 220        |
| 7.3      | Angriffe auf der Internetschicht . . . . .              | 222        |
| 7.3.1    | Reconnaissance (Aufklärung) . . . . .                   | 222        |
| 7.3.2    | IP-Spoofing . . . . .                                   | 226        |
| 7.3.3    | Denial-of-Service-Angriffe . . . . .                    | 226        |
| 7.3.4    | Angriffe auf Basis von IP-Fragmenten . . . . .          | 228        |
| 7.3.5    | Grundlegende Angriffe auf das IP-Routing . . . . .      | 229        |
| 7.3.6    | Weitere Anmerkungen zur Sicherheit von IPv6 . . . . .   | 233        |
| 7.3.7    | Sicherheit von ICMPv6 . . . . .                         | 233        |
| 7.4      | Angriffe auf der Transportschicht . . . . .             | 234        |
| 7.4.1    | Sicherheitsaspekte von UDP . . . . .                    | 234        |
| 7.4.2    | Sicherheit von TCP . . . . .                            | 235        |
| 7.4.3    | Portscans mit TCP und UDP . . . . .                     | 236        |
| 7.5      | Angriffe auf der Anwendungsschicht . . . . .            | 239        |
| 7.5.1    | Anmerkungen zur Reconnaissance . . . . .                | 239        |
| 7.5.2    | HTTP . . . . .                                          | 240        |
| 7.5.3    | DNS . . . . .                                           | 243        |
| 7.5.4    | E-Mail . . . . .                                        | 245        |
| 7.5.5    | Angriffe auf DHCP . . . . .                             | 247        |
| 7.5.6    | Telnet, R-Dienste und SSH . . . . .                     | 247        |
| 7.5.7    | NNTP . . . . .                                          | 248        |
| 7.5.8    | FTP . . . . .                                           | 248        |
| 7.5.9    | Sonstige historische Dienste . . . . .                  | 249        |
| 7.5.10   | Zusammenspiel mehrerer Protokolle . . . . .             | 250        |
| 7.6      | Zusammenfassung . . . . .                               | 250        |

|          |                                                            |            |
|----------|------------------------------------------------------------|------------|
| 7.7      | Weiterführende Literatur .....                             | 251        |
| 7.8      | Übungsaufgaben. ....                                       | 251        |
|          | Literatur. ....                                            | 254        |
| <b>8</b> | <b>Absicherung der Netzwerkschichten. ....</b>             | <b>255</b> |
| 8.1      | Einführung .....                                           | 255        |
| 8.2      | Absicherung auf der Netzzugangsschicht .....               | 255        |
| 8.2.1    | Zutrittskontrolle und physikalischer Netzwerkzugang .....  | 256        |
| 8.2.2    | Erwerb and Integration von Produkten/Dienstleistungen .... | 256        |
| 8.2.3    | Verfügbarkeit .....                                        | 257        |
| 8.2.4    | Komponentenverwaltung .....                                | 258        |
| 8.2.5    | MAC-Filter. ....                                           | 259        |
| 8.2.6    | Denial-of-Service-Eindämmung .....                         | 260        |
| 8.2.7    | Virtuelle LANs. ....                                       | 260        |
| 8.2.8    | Absicherung des ARP-Caches .....                           | 261        |
| 8.2.9    | IEEE 802.1X .....                                          | 262        |
| 8.2.10   | Kryptographische Sicherung von WLANs. ....                 | 263        |
| 8.3      | Absicherung auf der Internetschicht .....                  | 264        |
| 8.3.1    | Härtung des IPv4/IPv6-Stacks .....                         | 265        |
| 8.3.2    | Firewalls für die IP-Kommunikation .....                   | 265        |
| 8.3.3    | SEND: Secure Neighbor Discovery Protocol .....             | 266        |
| 8.3.4    | Anmerkungen zu Internet-DDoS-Angriffen .....               | 267        |
| 8.4      | Absicherung der Transportschicht .....                     | 267        |
| 8.4.1    | Firewalls und Angriffserkennung für TCP und UDP. ....      | 267        |
| 8.4.2    | Portscan-Detektion. ....                                   | 269        |
| 8.4.3    | TCP-Härtung .....                                          | 271        |
| 8.5      | Absicherung der Anwendungsschicht .....                    | 272        |
| 8.5.1    | Generelle Anmerkungen zur Anwendungsschicht .....          | 272        |
| 8.5.2    | Proxyserver und Co. ....                                   | 275        |
| 8.5.3    | HTTP .....                                                 | 278        |
| 8.5.4    | DNS .....                                                  | 279        |
| 8.5.5    | E-Mail-Protokolle: SMTP, IMAP und POP3. ....               | 281        |
| 8.5.6    | Absicherung von DHCP. ....                                 | 283        |
| 8.5.7    | NNTP .....                                                 | 283        |
| 8.6      | Zusammenfassung .....                                      | 284        |
| 8.7      | Weiterführende Literatur .....                             | 285        |
| 8.8      | Übungsaufgaben. ....                                       | 286        |
|          | Literatur. ....                                            | 286        |

**Teil IV Vertiefung**

- 9 Netzwerksteganografie . . . . . 291**
  - 9.1 Einführung . . . . . 291
  - 9.2 Methoden der Netzwerksteganografie . . . . . 294
    - 9.2.1 Grundlegende Taxonomie . . . . . 294
    - 9.2.2 Versteckmuster . . . . . 295
    - 9.2.3 Spezifische Versteckmethoden . . . . . 298
  - 9.3 Gegenmaßnahmen zur Netzwerksteganografie . . . . . 300
    - 9.3.1 Detektion . . . . . 302
    - 9.3.2 Limitierung . . . . . 304
    - 9.3.3 Unterbindung . . . . . 305
  - 9.4 Exkurs: Linguistische Steganografie . . . . . 306
  - 9.5 Zusammenfassung . . . . . 308
  - 9.6 Weiterführende Literatur . . . . . 308
  - 9.7 Übungsaufgaben. . . . . 308
  - Literatur. . . . . 309
- 10 Sicherheit im Internet der Dinge . . . . . 313**
  - 10.1 Einführung . . . . . 313
  - 10.2 Schuld sind die anderen – der Cycle of Blame . . . . . 320
  - 10.3 Standardisierung (und Zertifizierung) im IoT . . . . . 321
  - 10.4 Software-Updates (Patching) . . . . . 323
  - 10.5 Smart Homes und Smart Buildings . . . . . 325
    - 10.5.1 Kommunikationsprotokolle . . . . . 325
    - 10.5.2 Angriffe . . . . . 327
    - 10.5.3 Angriffsdetektion und Härtung . . . . . 329
  - 10.6 Industriesteueranlagen (Industrial Control Systems) . . . . . 331
    - 10.6.1 Angriffe . . . . . 332
    - 10.6.2 Angriffsdetektion und Härtung . . . . . 333
  - 10.7 Stand der Verwendung von Kryptografie in IoT-Protokollen. . . . . 336
  - 10.8 Generische IoT-Protokolle der Anwendungsschicht . . . . . 338
    - 10.8.1 CoAP . . . . . 339
    - 10.8.2 MQTT . . . . . 343
  - 10.9 IT-Sicherheit weiterer IoT-Domänen . . . . . 345
    - 10.9.1 Mobile IoT-Systeme (Smart Cars und Co.) . . . . . 345
    - 10.9.2 Electronic Healthcare (eHealth) . . . . . 346
    - 10.9.3 Landwirtschaft und Handwerk. . . . . 348
    - 10.9.4 Altequipment . . . . . 349
  - 10.10 Digitale Forensik für das IoT . . . . . 349
  - 10.11 Zusammenfassung . . . . . 352



---

|                                                                                  |                                    |            |
|----------------------------------------------------------------------------------|------------------------------------|------------|
| 10.12                                                                            | Weiterführende Literatur . . . . . | 353        |
| 10.13                                                                            | Übungsaufgaben. . . . .            | 353        |
|                                                                                  | Literatur . . . . .                | 354        |
| <b>Anhang A: Wichtige wissenschaftliche Zeitschriften und Tagungen . . . . .</b> |                                    | <b>359</b> |
| <b>Anhang B: Ausgewählte Lösungen zu Übungsaufgaben . . . . .</b>                |                                    | <b>363</b> |
| <b>Stichwortverzeichnis . . . . .</b>                                            |                                    | <b>381</b> |