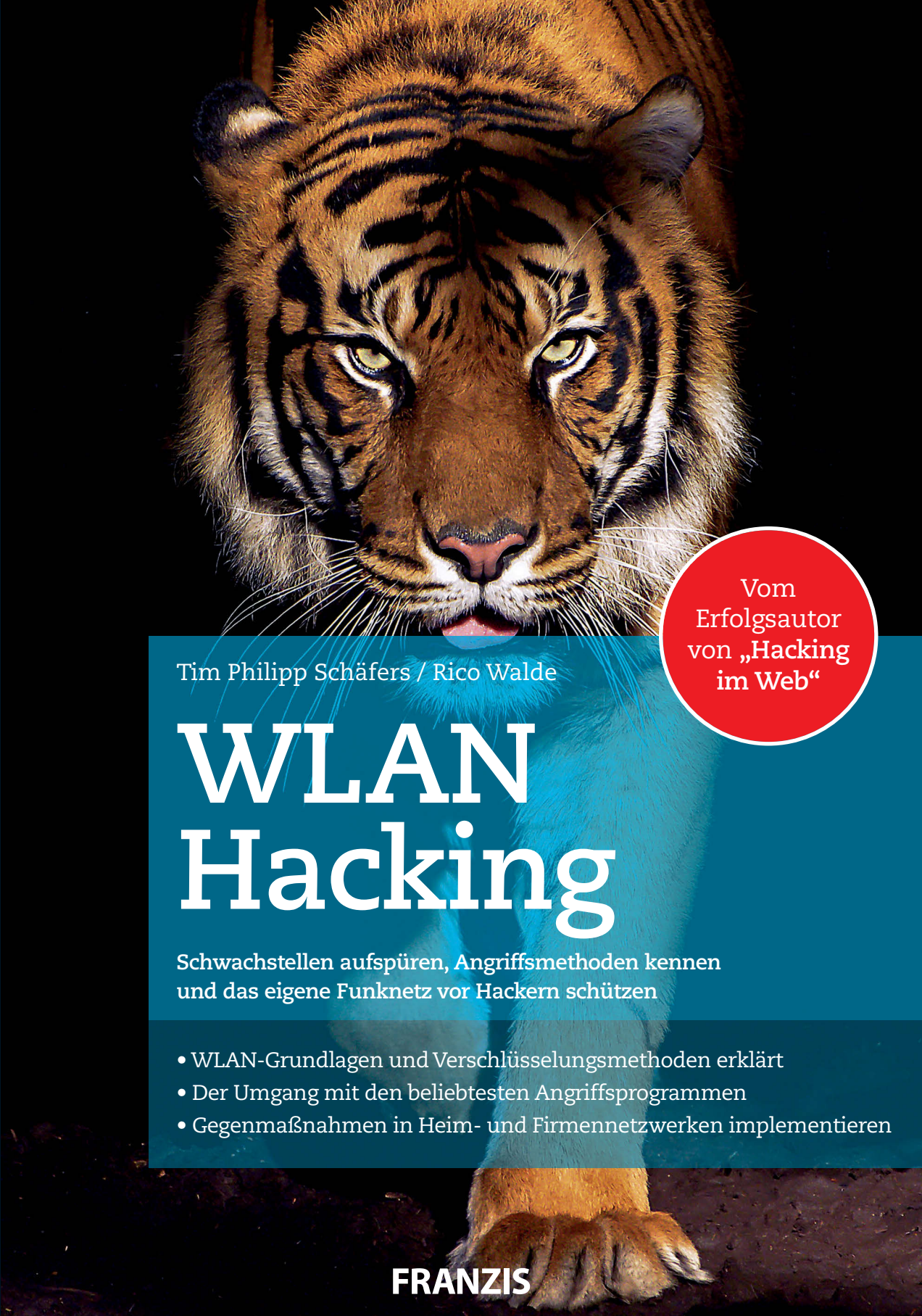


Vom Erfolgsautor von **„Hacking im Web“**

Tim Philipp Schäfers / Rico Walde

# WLAN Hacking

**Schwachstellen aufspüren, Angriffsmethoden kennen und das eigene Funknetz vor Hackern schützen**

- WLAN-Grundlagen und Verschlüsselungsmethoden erklärt
- Der Umgang mit den beliebtesten Angriffsprogrammen
- Gegenmaßnahmen in Heim- und Firmennetzwerken implementieren

FRANZIS

Tim Philipp Schäfers / Rico Walde

# WLAN Hacking

Tim Philipp Schäfers / Rico Walde

# WLAN Hacking

**Schwachstellen aufspüren, Angriffsmethoden kennen und das eigene Funknetz vor Hackern schützen**

- WLAN-Grundlagen und Verschlüsselungsmethoden erklärt
- Der Umgang mit den beliebtesten Angriffsprogrammen
- Gegenmaßnahmen in Heim- und Firmennetzwerken implementieren

Bibliografische Information der Deutschen Bibliothek

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie;
detaillierte Daten sind im Internet über http://dnb.ddb.de abrufbar.

Alle Angaben in diesem Buch wurden vom Autor mit größter Sorgfalt erarbeitet bzw. zusammengestellt und unter Einschaltung wirksamer Kontrollmaßnahmen reproduziert. Trotzdem sind Fehler nicht ganz auszuschließen. Der Verlag und der Autor sehen sich deshalb gezwungen, darauf hinzuweisen, dass sie weder eine Garantie noch die juristische Verantwortung oder irgendeine Haftung für Folgen, die auf fehlerhafte Angaben zurückgehen, übernehmen können. Für die Mitteilung etwaiger Fehler sind Verlag und Autor jederzeit dankbar. Internetadressen oder Versionsnummern stellen den bei Redaktionsschluss verfügbaren Informationsstand dar. Verlag und Autor übernehmen keinerlei Verantwortung oder Haftung für Veränderungen, die sich aus nicht von ihnen zu vertretenden Umständen ergeben. Evtl. beigefügte oder zum Download angebotene Dateien und Informationen dienen ausschließlich der nicht gewerblichen Nutzung. Eine gewerbliche Nutzung ist nur mit Zustimmung des Lizenzinhabers möglich.

**© 2018 Franzis Verlag GmbH, 85540 Haar bei München**

Alle Rechte vorbehalten, auch die der fotomechanischen Wiedergabe und der Speicherung in elektronischen Medien. Das Erstellen und Verbreiten von Kopien auf Papier, auf Datenträgern oder im Internet, insbesondere als PDF, ist nur mit ausdrücklicher Genehmigung des Verlags gestattet und wird widrigenfalls strafrechtlich verfolgt.

Die meisten Produktbezeichnungen von Hard- und Software sowie Firmennamen und Firmenlogos, die in diesem Werk genannt werden, sind in der Regel gleichzeitig auch eingetragene Warenzeichen und sollten als solche betrachtet werden. Der Verlag folgt bei den Produktbezeichnungen im Wesentlichen den Schreibweisen der Hersteller.

**Autor:** Tim Philipp Schäfers / Rico Walde
**Programmleitung:** Benjamin Hartlmaier
**Satz:** DTP-Satz A. Kugge, München
**art & design:** www.ideehoch2.de

ISBN 978-3-645-20523-8

# Vorwort

Die technische Vernetzung unserer Gesellschaft ist in den letzten zwei Dekaden so schnell vorangeschritten wie noch niemals zuvor in der Menschheitsgeschichte. Die meisten von uns nutzen täglich unzählige Apps auf ihrem Smartphone. So gilt der Griff zum Ausschalten des Wecktons morgens mittlerweile oft dem Smartphone oder der Smartwatch und nicht einem gewöhnlichen Wecker. Direkt danach oder spätestens beim Frühstück werden die sonstigen Funktionen all dieser Geräte genutzt – etwa um Informationen in sozialen Netzen zu verbreiten, Neuigkeiten zu erfahren, das Wetter des Tages oder die Aktienkurse zu prüfen, Überweisungen vorzunehmen und noch für viele weitere Dinge.

Kurzum: Die digitale Omnipräsenz ist integraler Bestandteil unserer Gesellschaft – zugleich aber auch die Abhängigkeit von diesen Technologien. Die Verfügbarkeit der Dienste ist für uns zu einer Selbstverständlichkeit geworden. Oft scheinen wir zu vergessen, dass bei der Nutzung all dieser Dienste ein großes Datenvolumen anfällt, das es zu managen gilt. Es bedarf immer einer Infrastruktur, die diese Daten übermittelt und an den richtigen Endpunkt weiterleitet, damit die Informationen dort genutzt oder verarbeitet werden können.

Da eine Anbindung über Kabel auf Dauer nicht bequem genug erschien und Computer immer kleiner und kompakter wurden, hat sich neben der kabelgebundenen Lösung spätestens mit der IEEE-Norm 802.11 auch eine standardisierte drahtlose Technologie etabliert. Diese soll mittels Funk die Übertragung von Daten sicherstellen und wurde im Laufe der Zeit immer weiter angepasst. Heute ist uns diese Technologie unter dem Begriff WLAN bzw. Wi-Fi bekannt.

WLAN wird beispielsweise von Routern verwendet, die ihre Funknetze zur Verfügung stellen (klassischer Infrastrukturbetrieb) – mittlerweile wird auch der Ad-hoc-Betrieb eingesetzt. Im Heimbereich ist WLAN sehr üblich geworden, oft verfügen Router über vorkonfigurierte WLANs. Aber auch in Unternehmen wird, in unterschiedlichen Einsatzgebieten, ein drahtloser Zugriff auf Daten benötigt, hier wird ebenfalls die WLAN-Technologie eingesetzt.

In der Zukunft wird die WLAN-Technologie weiterhin eine bedeutende Rolle spielen. Viele Gadgets und Geräte aus dem Bereich »Internet der Dinge« haben die WLAN-Technologie verbaut, und auch im Bereich des modernen Straßenverkehrs (Car-to-Car Communication) könnte sich WLAN zu einer der wichtigsten Technologien entwickeln.

Wie die meisten Technologien verfügt WLAN über Stärken und Schwächen – in diesem Buch möchten wir Ihnen primär nahebringen, wie Sie WLAN-Strukturen habhaft werden, also deren Schwächen erkunden können, damit Sie letztlich lernen, wie Sie Ihr eigenes Wireless LAN prüfen, durch Nutzen der Stärken dieser Technologie möglichst sicher betreiben und gegen Angriffe härten können.

Sollten Sie Hinweise zum Buch, zu Themen aus diesem Buch oder einfach nur Interesse an einem fachlichen Austausch haben, freuen wir uns über Ihre E-Mail: *autoren@wlan-hacking.de.*

Wir werden auch nach Veröffentlichung dieses Buchs immer mal wieder neue Tools vorstellen oder Artikel zum Thema WLAN-Hacking schreiben. Diese Beiträge lassen sich auf der Webseite zum Buch einsehen: *https://wlan-hacking.de*

Wir wünschen viel Spaß bei der Lektüre!

## Danksagung

Dieses Buch liegt nur in dieser Form vor Ihnen, da uns einige Personen in dem Vorhaben, etwas zum Thema WLAN-Sicherheit zu Papier zu bringen, unterstützt haben. Unser Dank gilt also vor allem den Personen, die uns bei der Erstellung dieses Buchs durch ihr Fachwissen geholfen haben, aber auch jenen Personen, die uns noch mehr für das Thema WLAN begeistert haben, uns täglich ermutigt haben weiterzumachen und die uns im Alltag entlastet haben.

Rico dankt seiner Familie, insbesondere seinen Eltern, Frau Nielebock und Laura K. Des Weiteren dankt er seinen Freunden und Kommilitonen für das Verständnis, das ihm entgegengebracht wurde, als er aufgrund des Buchs wenig Zeit für sie hatte.

Tim dankt besonders seiner Familie und seinen Freunden. Ein zusätzliches Dankeschön geht an Marco Brinkmann, da er durch ihn (noch) mehr mit dem Thema WLAN-Sicherheit in Berührung gekommen ist. Zudem hat er durch sein seit Jahren angehäuftes Wissen im Bereich Netzwerktechnik entscheidende Themenideen zum Inhalt des Buchs beigetragen.

Darüber hinaus danken wir Prof. Dr. Markus Stäuble und Benjamin Hartlmaier, die als Programmleiter bei Franzis immer ein offenes Ohr für uns hatten und sich von Anfang an auf das Buchprojekt eingelassen haben. Außerdem gilt unser Dank Ulrich Dorn für die Arbeit und Mühe mit dem Lektorat und dem Layout. Zudem danken wir dem gesamten Franzis-Team – auch wenn uns die meisten nicht namentlich bekannt sind – für die Hilfe.

Abschließend möchten wir noch drei Personen im Besonderen für ihre intensive Unterstützung bei diesem Buchprojekt danken.

Sebastian Neef ist als langjähriger Begleiter immer erreichbar für Nachfragen gewesen und hat seine Erfahrung rund um IT-Sicherheit in das Projekt eingebracht.

Merlin Blom hat uns sowohl inhaltlich als auch durch seine Hilfe bei Formalien sehr weitergeholfen. Insbesondere in der finalen Bearbeitungsphase stand er mit Rat und Tat, beispielsweise mit seinen Kenntnissen rund um Mac und Photoshop, zur Seite. Wir danken ihm sehr für sein Engagement!

Unser größter, abschließender Dank gilt Florian Eimer! Er hat uns durch sein Fachwissen und das Zurverfügungstellen von WLAN-Equipment während des Schreibens noch mehr für das Thema begeistert. Außerdem hat er durch vielfaches Lesen während des Erstellungsprozesses und Anregungen zum Buchinhalt maßgeblich zur Verbesserung des Buchs beigetragen.

Rico Walde und Tim Philipp Schäfers

# Inhaltsverzeichnis


1 Basiswissen Funknetzwerke ..... 19
1.1 Was ist WLAN? ..... 19
1.1.1 Physikalische Grundlagen ..... 19
1.1.2 Probleme bei drahtloser Datenübertragung ..... 21
1.2 Geschichte des WLAN ..... 22
1.2.1 IEEE 802.11 ..... 23
1.2.2 IEEE 802.11a ..... 23
1.2.3 IEEE 802.11b ..... 24
1.2.4 IEEE 802.11g ..... 24
1.2.5 IEEE 802.11n ..... 24
1.2.6 Weitere historische Standards ..... 25
1.2.7 IEEE 802.11ac ..... 25
1.2.8 IEEE 802.11ad ..... 27
1.2.9 IEEE 802.11ax ..... 28
1.3 WLAN ist nicht nur IEEE 802.11 ..... 28
1.3.1 Bluetooth ..... 28
1.3.2 ZigBee ..... 29
1.3.3 Z-Wave ..... 29
1.3.4 HiperLAN ..... 30
1.3.5 HomeRF ..... 30
1.3.6 WiMAX ..... 30
1.3.7 Li-Fi ..... 30

2 WLAN-Grundlagen ..... 33
2.1 Komponenten in WLAN-Infrastrukturen ..... 33
2.1.1 WNIC: Wireless Network Interface Controller ..... 33
2.1.2 STA: Stations ..... 34
2.1.3 AP: Access Point ..... 34
2.1.4 Authentication Server und Distribution System ..... 35
2.1.5 WLAN-Controller ..... 37
2.2 WLAN-Topologien ..... 37
2.2.1 IBSS: Independent Basic Service Set ..... 37
2.2.2 BBS: Basic Service Set ..... 39
2.2.3 ESS: Extended Service Set ..... 40
2.2.4 WDS: Wireless Distribution System ..... 41
2.2.5 Drahtlose Mesh-Netzwerke ..... 42

**2.3 Bezeichnungen von WLANs ... 44**
2.3.1 SSID: Service Set Identifier ... 46
2.3.2 ESSID: Extended Service Set Identifier ... 51
2.3.3 BSSID und MAC-Adresse ... 51
**2.4 WLAN-Operationen ... 52**
**2.5 Authentifizierungsarten ... 53**
2.5.1 Open System Authentication ... 53
2.5.2 Shared Key Authentication ... 54
**2.6 Layer und Frames bei WLAN ... 55**
2.6.1 Physical Layer ... 56
2.6.2 MAC-Layer ... 58
2.6.3 Arten von WLAN-Frames ... 61

**3 Basiswissen WLAN-Sicherheit ... 69**
**3.1 WEP: Wired Equivalent Privacy Protocol ... 71**
**3.2 WPA (IEEE 802.11i/D3.0) ... 75**
3.2.1 WPA Personal ... 75
3.2.2 WPA Enterprise ... 78
**3.3 WPA2 (IEEE 802.11i/D9.0) ... 82**
3.3.1 Advanced Encryption Standard ... 82
3.3.2 WPA2 Personal ... 82
3.3.3 WPA2 Enterprise ... 83
**3.4 WLAN-Verschlüsselungen ... 84**
**3.5 WPS: Wi-Fi-Protected Setup ... 85**
**3.6 Sonderfall WAPI ... 86**
**3.7 Weitere Sicherheitsfeatures ... 86**
3.7.1 Protected Management Frames (IEEE 802.11w) ... 87
3.7.2 MAC-Filter ... 89
3.7.3 Nutzung von verborgenen SSIDs ... 90

**4 Vorbereitungen und Setup ... 93**
**4.1 Der Angreifer-PC ... 93**
4.1.1 Kali Linux ... 94
4.1.2 Wifislax ... 102
**4.2 Der Opfer-PC ... 105**
4.2.1 Hardware ... 105
4.2.2 WLAN-Router ... 105
4.2.3 OpenWrt ... 108
4.2.4 WLAN-Karten ... 109
4.2.5 WLAN-Antennen ... 116
**4.3 Monitormodus ... 118**
**4.4 Weitere WLAN-Ausstattung ... 120**
4.4.1 WiFi Pineapple ... 120
4.4.2 Einrichtung und erste Schritte ... 123

5 Informationsbeschaffung ..... 135
5.1 Scanning-Methoden ..... 135
5.1.1 Passives Scanning ..... 136
5.1.2 Aktives Scanning ..... 136
5.2 WLANs der Umgebung analysieren ..... 137
5.2.1 airodump-ng ..... 138
5.2.2 MetaGeek inSSIDer ..... 141
5.2.3 Acrylic Wi-Fi Professional ..... 142
5.2.4 Wifi Analyzer ..... 143
5.3 WLAN-Abdeckung überprüfen ..... 146
5.3.1 Acrylic Wi-Fi HeatMaps ..... 146
5.3.2 Ekahau Site Survey ..... 147
5.4 Nicht digitale Informationsbeschaffung ..... 148
5.4.1 Social Engineering ..... 149
5.4.2 Gegenmaßnahmen zum Social Engineering ..... 150
5.5 Ergebnisse dokumentieren ..... 150

6 Sniffing und Analyse ..... 153
6.1 Netzwerkverkehr aufzeichnen ..... 153
6.2 Sniffing mit Remote-Interface ..... 156
6.2.1 Passives Sniffing mit tcpdump ..... 156
6.2.2 Passives Sniffing mit tcpdump und Wireshark ..... 158
6.3 WLAN-Verkehr untersuchen und Netzwerke aufspüren ..... 161
6.4 Verbindungen zu verborgenen SSIDs ..... 164
6.4.1 Ermitteln verborgener SSIDs durch passives Sniffing ..... 168
6.4.2 Ermitteln verborgener SSIDs durch Brute Force ..... 170
6.5 Packet Capture ..... 180

7 Störangriffe auf WLAN ..... 183
7.1 Angriffe auf physikalischer Ebene ..... 183
7.1.1 Experiment: Störangriffe durch Frequenzüberlagerung ..... 183
7.1.2 WLAN-Jammer und Wi-Fi-Jammer ..... 187
7.1.3 Gegenmaßnahmen zu Störangriffen und Wi-Fi-Jammern ..... 188
7.2 Angriffe auf Netzwerkebene ..... 192
7.2.1 DoS durch IP-Adressen-Allokation ..... 192
7.2.2 Gegenmaßnahmen zu Angriffen auf Netzwerkebene ..... 196
7.3 DoS durch Authentication Request Flooding ..... 196
7.3.1 DoS durch Beacon Flooding ..... 202
7.3.2 DoS durch Disassociation Attack ..... 209
7.3.3 DoS durch Deauthentication Flooding ..... 222
7.3.4 DoS durch Disassociation und Deauthentication Flooding ..... 228
7.3.5 DoS durch CTS-Frame-Attacke ..... 229
7.3.6 Gegenmaßnahmen mithilfe des IEEE-802.11-Protokolls ..... 238

8 WLAN-Authentifizierung umgehen ..... 241
8.1 WLAN-Passwörter bei physischem Gerätezugriff auslesen ..... 241
8.1.1 Windows: Passwort auslesen ..... 241
8.1.2 Linux: Passwort auslesen ..... 243
8.1.3 macOS: Passwort auslesen ..... 244
8.1.4 Android: Passwort auslesen ..... 244
8.1.5 iOS: Passwort auslesen ..... 246
8.2 Verwendung von Standardpasswörtern ..... 246
8.3 MAC-Spoofing – Umgehen von MAC-Filtern ..... 259
8.3.1 MAC-Spoofing unter Windows ..... 260
8.3.2 MAC-Spoofing unter Linux ..... 262
8.3.3 MAC-Spoofing unter macOS ..... 263
8.3.4 Beispiele von MAC-Filtern und ihrer Umgehung ..... 263
8.4 Angriffe auf WEP ..... 271
8.4.1 WEP-Schlüssel durch AP und STA(s) ermitteln ..... 271
8.4.2 WEP-Schlüssel nur durch AP ermitteln ..... 280
8.4.3 WEP-Schlüssel durch STA ermitteln (mit Hirte Attack) ..... 292
8.4.4 Empfehlungen zu WEP ..... 299
8.5 Angriffe auf WPS ..... 299
8.5.1 Pixie Dust ..... 302
8.5.2 reaver ..... 304
8.5.3 Wenn der Angriff fehlschlägt ..... 307
8.6 Angriffe auf WPA/WPA2 ..... 313
8.6.1 Access Point und Client in Reichweite ..... 317
8.6.2 Wenn nur der Client verfügbar ist ..... 323
8.6.3 Beschleunigung des Cracking-Vorgangs ..... 331
8.6.4 Kryptografische Angriffe gegen WPA ..... 338
8.6.5 Abwehrmaßnahmen ..... 339
8.7 Angriffe auf WLAN-Infrastrukturen ..... 340
8.7.1 Malicious SSID ..... 340
8.7.2 Rogue Access Points ..... 341
8.7.3 Fake-AP unter Kali Linux ..... 344
8.7.4 Evil-Twin-Angriff ..... 356
8.7.5 Evil Twin in der Praxis ..... 358

9 Fortgeschrittene Angriffsszenarien ..... 373
9.1 WLAN-Verkehr mitschneiden und entschlüsseln ..... 373
9.1.1 Gegenmaßnahmen zu Sniffing ..... 381
9.2 DNS-Spoofing ..... 383
9.3 Windows-Rechner im WLAN übernehmen ..... 398
9.4 Verbindung von einzelnen Endgeräten trennen ..... 406

10 WLAN-Security-Monitoring ..... 415
10.1 WIDS/WIPS-Infrastruktur ..... 415
10.1.1 WIDS/WIPS-Komponenten ..... 415

**10.2 Analyse mithilfe von WIDS/WIPS ... 419**
10.2.1 Geräteklassifizierung ... 420
10.2.2 Signaturanalyse ... 420
10.2.3 Verhaltensanalyse ... 421
10.2.4 Protokollanalyse ... 421
10.2.5 Spektrumanalyse und Performanceanalyse ... 423
10.2.6 Vorgehen bei Alarm und Mitteilung ... 423

**11 WLAN-Security-Audits durchführen ... 425**
**11.1 Möglicher Ablauf eines WLAN-Security-Audits ... 425**
11.1.1 Layer-1-Audit ... 425
11.1.2 Layer-2-Audit ... 427
11.1.3 Penetration Testing ... 428
11.1.4 Social Engineering ... 428
11.1.5 Sonstige Überprüfungen ... 428
**11.2 Sicherheitsempfehlungen nach einem Audit ... 429**
11.2.1 Einsatz starker Verschlüsselung ... 429
11.2.2 Durchgängig sichere Authentifizierung ... 429
11.2.3 Sensibilisierung der Mitarbeiter ... 430
11.2.4 Empfehlung einer WLAN-Policy ... 430
11.2.5 Empfehlungen zum Monitoring ... 430
11.2.6 Empfehlungen zur physischen Sicherheit ... 430
**11.3 Ausrüstung für einen WLAN-Security-Audit ... 431**

**12 Kleinere Hacks und Tricks ... 433**
**12.1 Umgehung von Vorschaltseiten ... 433**
**12.2 WLAN-Adapter-Tuning ... 439**
**12.3 Wardriving ... 446**
12.3.1 Wardriving in der Praxis ... 448
**12.4 Störerhaftung – oder was davon übrig ist ... 452**
**12.5 Freifunk, die nicht kommerzielle Initiative ... 454**
**12.6 Alternative Router-Firmware ... 455**
12.6.1 Freifunk ... 457
12.6.2 OpenWrt ... 459
12.6.3 DD-WRT ... 463
12.6.4 Freetz ... 469
12.6.5 Stock-Firmware wiederherstellen ... 470
12.6.6 Notfall-Recovery ... 475
12.6.7 Weitere alternative Firmware ... 478
**12.7 Der Angreifer und seine Motive ... 479**
12.7.1 Die Angreifer ... 479
12.7.2 Die Motive ... 481
**12.8 Abwehrmaßnahmen kompakt ... 483**
12.8.1 Die zehn wichtigsten Regeln beim Betrieb eines WLAN ... 483
12.8.2 Die fünf wichtigsten Regeln für eine stabile Heim-WLAN-Infrastruktur ... 484

12.8.4 Sicherheit Ihres Access Point ..... 484
12.8.5 Sicherheit Ihrer WLAN-Clients ..... 485

**13 Epilog ..... 487**

**14 Anhang ..... 489**
**14.1 Wireshark-Filter ..... 489**
14.1.1 Logische Operatoren ..... 489
14.1.2 Verknüpfungsoperatoren ..... 490
14.1.3 Filter nach Frame-Typ und Frame-Subtyp ..... 490
14.1.4 Weitere nützliche Filter ..... 490
14.1.5 Wildcards ..... 491
**14.2 Abkürzungsverzeichnis ..... 491**
**14.3 Buchempfehlungen ..... 494**

**15 Literaturverzeichnis ..... 497**

**Stichwortverzeichnis ..... 503**

# Einleitung

WLAN ist für die meisten Anwender heute nicht mehr wegzudenken. Die Einsatzmöglichkeiten zur bequemen Übertragung von Daten sind schier unbegrenzt – neben dem klassischen Infrastrukturbetrieb zur Versorgung von Endgeräten findet WLAN mittlerweile auch in einigen anderen wichtigen Lebensbereichen Anwendung. Diese sind sehr vielfältig und uns oft gar nicht bewusst – darunter fallen die Aufnahme von Bestellungen in Restaurants, die Übermittlung von Kreditkartendaten an POS-Systeme und PDAs (*Personal Digital Assistants*) im Bereich der Lagerlogistik, um nur einige Beispiele zu nennen.

Mit der steigenden Verbreitung von mobilen Endgeräten (wie Smartphones, Tablets oder Smartwatches) hat WLAN seinen hegemonialen Standpunkt im Bereich des Infrastrukturbetriebs weiter gefestigt. Der Verband der deutschen Internetwirtschaft e. V. hat in einer Erhebung ermittelt, dass es Ende 2013 mit einer Zahl von 7,5 Milliarden erstmals mehr WLAN-fähige Geräte als Menschen gab. Eine Prognose aus dieser Erhebung geht zudem davon aus, dass sich dieser Wert bis Ende 2017 mehr als verdoppeln und auf über 20 Milliarden ansteigen wird. [1] Dies wird unter anderem durch eine gestiegene Marktdurchdringung von besonders günstigen Endgeräten aus dem chinesischen Markt begünstigt.

Tatsächlich ist es erstaunlich, in welchen Geräten heutzutage WLAN-Chips eingebaut werden. In Laptops, Smartphones oder Fernsehern scheint diese Funktion noch recht nützlich, ob sich allerdings der Einbau in Kühlschränken[1], Thermostaten oder Waschmaschinen durchsetzen wird, erscheint fraglich. Konzepte wie »Smart Home« oder »Smart City« lassen allerdings bereits erahnen, dass WLAN auch in Zukunft eine bedeutende Rolle in unser aller Leben spielen wird.

Umso wichtiger ist es, dass wir uns mit dieser Technologie beschäftigen, um gemeinsam zu erkennen, wie sicher sich der Einsatz dieser Technologie gestalten lässt und wo deren Stärken und Schwächen liegen.

## Der Ansatz des Buchs

Dieses Buch soll Ihnen die Möglichkeit bieten, WLAN und dessen (Un-)Sicherheit besser zu verstehen. Mit praktischen Beispielen, die anhand von Tools für Sie zu Hause selbst

1 Im Januar 2014 wurde bekannt, dass Kriminelle offenbar bewusst Sicherheitslücken in solchen sogenannten „Embedded Devices" aus Haushaltsgeräten genutzt haben, um im großen Stil Werbe-E-Mails (Spam) zu verschicken (*http://www.spiegel.de/netzwelt/web/kuehlschrank-verschickt-spam-botnet-angriff-aus-dem-internet-der-dinge-a-944030.html*).

nachvollziehbar werden, möchten wir Ihnen zeigen, wie Sie drahtlose Netzwerke auf Ihre Sicherheit überprüfen können. Neben praxisnahen Beispielen wird auch der theoretische Hintergrund erläutert, um ein Verständnis der Technologien zu ermöglichen: wie WLAN und Verschlüsselungstechniken funktionieren, die Historie von WLAN etc. Auch wenn wir an verschiedensten Stellen Aspekte aus dem Enterprise-Umfeld erwähnen oder sogar erklären, liegt der Fokus dieses Buchs eher auf dem Heimnetzwerkbereich. Wir wollen Ihnen als Privatperson das Thema WLAN-Hacking näherbringen.

Der Begriff Hacking wurde in den letzten Jahren durch die Medien sehr einseitig geprägt. Im Volksmund verbindet man damit nur noch das Einbrechen sowie das Ausspionieren oder sogar Zerstören digitaler Infrastruktur. Im ursprünglichen Sinn und in der eigentlichen Hackerszene ist dieser Begriff aber anders besetzt. Hacking beschreibt grundsätzlich einfach den kreativen Umgang mit Technik. Der Bereich der »Offensive Security« ist sicherlich ein Teilgebiet davon, aber längst nicht alles. Deswegen wird es in unserem Buch zwar um das »Hacken« in andere WLAN-Netze gehen, jedoch versuchen wir auch, Hacking im eigentlichen Sinne zu behandeln. Das reicht von »Wie tune ich meinen WLAN-Adapter?« und »Wie spiele ich eine alternative Firmware auf meinen Router auf?« über Freifunk bis zum Wardriving. Wir hoffen, euch damit den Blick zu öffnen für das, was der Begriff Hacking eigentlich einmal bedeutete.

Die wichtigsten Fachbegriffe sind **fett** hervorgehoben, wenn sie das erste Mal genannt und erläutert werden.

Dieses Buch richtet sich gleichermaßen an Hobbyfunker und IT-Professionals. Es ist für Anfänger und Fortgeschrittene im Bereich WLAN-Sicherheit geeignet. Es fängt bei den WLAN-Grundlagen an und erklärt sie auf anschauliche Art und Weise. Durch detaillierte Hintergrundinformationen soll gesichert werden, dass auch das Verständnis der im hinteren Teil des Buchs vorgestellten komplexeren Angriffsvektoren möglich ist. Wenn Sie sich schon länger und wirklich intensiv mit dem Thema WLAN-Sicherheit auseinandergesetzt haben, lernen Sie in diesem Buch vermutlich eher wenig Neues.

Wie Sie dem Ansatz bereits entnehmen konnten, geht es darum, praktisches Wissen zur Sicherheit von WLAN zu vermitteln. Dazu benötigen Sie Vorwissen im Bereich IT und zumindest Grundlagen zu Drahtlosnetzwerken. Wir werden an geeigneten Stellen allerdings immer wieder wissenswerte Hintergrundinformationen einbinden oder anschauliche Grafiken zur Darstellung verwenden. Insofern sollten alle Beispiele aus dem Buch für Sie nachvollziehbar und verständlich sein – auch ohne immense Praxiserfahrung.

Nach der Lektüre dieses Buchs sollten Sie in der Lage sein, Angriffe auf drahtlose Netzwerke zu verstehen und selbst durchzuführen. Dieses Wissen lässt sich zum einen dazu nutzen, WLAN-Infrastruktur auf Sicherheit zu testen, zum anderen können Sie sie dann auch vor den bestmöglich kennengelernten Angriffe schützen. Wir bitten eindringlich darum, das verwendete Wissen für ethisches Hacking zu verwenden, denn das Eindringen in fremde Drahtlosnetzwerke ist in Deutschland ohne Erlaubnis des Besitzers verboten.

## Der Aufbau des Buchs

Wir hoffen, mit diesem Buch einen strukturierten Ansatz geschaffen zu haben, durch den aufeinander aufbauendes Wissen vermittelt werden kann, sodass wir auch Einsteigern eine Chance geben, sich das Thema anzueignen. Wir haben das Buch dabei grob in drei grundlegende Bereiche gegliedert.

- **Teil I** – Hier stellen wir Ihnen die Geschichte und die Entwicklung von WLAN vor, wir zeigen auf, welche Standards es gibt und welche drahtlosen Funknetzwerke neben dem alles überschattenden IEEE-802.11-Standard existieren. Danach erfahren Sie die theoretischen Grundlagen von WLAN und WLAN-Sicherheit. Hier werden auch die verschiedenen Verschlüsselungstechnologien erklärt. Dieser Teil ist überwiegend theoretischer Natur und dient der Vorbereitung, damit die später vorgestellten Angriffsvektoren auch verstanden werden.
- **Teil II** – Dies ist der erste von zwei sehr praxisorientierten Teilen. Als Erstes schauen wir uns an, wie wir ein gutes Setup einrichten, um mit dem WLAN-Hacking zu starten. Wir gehen kurz auf die Installation von Kali ein und zeigen, welche Hardware benötigt wird. Im folgenden Kapitel möchten wir Ihnen beibringen, wie man am besten Informationen über sein Zielnetzwerk sammelt bzw. die WLAN-Umgebung auskundschaftet. Danach schauen wir, wie man Netzwerkverkehr abfängt und wie man versteckte SSIDs ermittelt. Anschließend geht es über das Stören von WLAN zu dem längsten Kapitel mit dem wohl typischsten Thema für ein WLAN-Hacking-Buch: das Umgehen von WLAN-Authentifizierung. Hier lernen Sie alle gängigen Angriffsvektoren kennen, um sich in ein fremdes WLAN reinzuhacken und Schutzmaßnahmen zu umgehen.
- **Teil III** – Sobald man die Authentifizierung eines fremden Netzwerks umgangen und sich mit diesem verbunden hat, kann man darüber z. B. auf das Internet zugreifen. Das ist aber längst nicht alles. Im dritten Teil stellen wir Folgeangriffe dar und erklären, wie man nach dem erfolgreichen Knacken des Passworts das Netzwerk und seine Teilnehmer weitergehend angreifen kann. Wie es gelingen kann, solche Angriffe im Businessumfeld abzuwehren, erklären wir im Anschluss unter dem Thema WLAN-Security-Monitoring und -Audits. Im letzten Kapitel wird es um weitere kreative Hacks gehen, die in der bisherigen Struktur keinen Platz gefunden haben. Dies reicht von Wardriving über das Aufspielen von alternativer Firmware auf Router bis zu einer rechtlichen Erläuterung der Störerhaftung.

## Rechtsgrundlagen

Der Einsatz von funkbasierten Netzen im 2,4-GHz- und 5-GHz-Frequenzband sind in den IEEE-802.11-Normen festgelegt. Die Nutzung von Frequenzbändern ist international durch verschiedene Stellen geregelt. In Europa ist das ETSI, das *European Telecommunications Standards Institute* mit Sitz in Sophia Antipolis, Frankreich, zuständig. In Deutschland ist die Bundesnetzagentur für die Frequenzordnung und Überwachung der

Frequenzbänder verantwortlich, das heißt, sie bestimmt, wer wo wie stark Funksignale aussenden darf. Genau geregelt ist das in der Bundesrepublik im sogenannten Frequenzplan. [2]

Unter anderem steht dort, dass der Betrieb von WLANs innerhalb der spezifizierten Frequenzen gebühren- und genehmigungsfrei ist. Jeder darf also WLAN-Infrastruktur aufbauen. Die im Fachhandel erhältlichen Geräte halten die entsprechenden Vorschriften zu Frequenz und Strahlungsintensität ab Werk ein. Da wir hier WLAN jedoch aus der Sicherheitsperspektive betrachten, müssen wir anmerken, dass beim Penetration Testing von WLAN-Netzwerken mehr beachtet werden muss. Prinzipiell gilt: Greife nur Infrastruktur an, die dir gehört oder für die du eine ausdrückliche Genehmigung zum Penetration Testing hast. Diese sollte in Schriftform vorliegen und den genauen Auftrag beinhalten. Außerdem sollte spezifiziert werden, wann und inwieweit der produktive Betrieb der Infrastruktur durch das Testen beeinflusst oder lahmgelegt werden darf.

Allgemein gilt bei Angriffen auf fremde WLANs § 303b StGB[2] Computersabotage, der eine Freiheitsstrafe von bis zu drei Jahren oder eine Geldstrafe vorsieht, wenn eine »Datenverarbeitungsanlage«, zu der man einen WLAN-Router zählen müsste, zerstört, beschädigt, unbrauchbar gemacht, beseitigt oder verändert wird. »Erbeutet« man Daten, die nicht für einen bestimmt waren, wird § 202a StGB interessant, der ebenfalls eine Freiheitsstrafe von drei Jahren oder eine Geldstrafe vorsieht. Dieser Paragraf ist gemeinhin als »Hackerparagraf« bekannt. Darüber hinaus könnte ein Opfer zivilrechtlich gegen Sie vorgehen, wenn man ihm oder seiner Firma nachweislich Schaden zugefügt hat. Das kann von Unterlassungserklärungen bis zu Schadensersatzforderungen reichen.

**Haftungsausschluss**

Sie als Leser sind in jedem Fall selbst für die Folgen Ihres Handelns verantwortlich! Wir übernehmen keinerlei Haftung für die von Ihnen angerichteten Schäden und bieten auch keine Rechtsbeihilfe in einem solchen Fall an. Dieses Buch soll keine Anleitung dazu darstellen, ohne Erlaubnis fremde WLAN-Netzwerke zu hacken, sondern dazu dienen, geeignete Abwehrmaßnahmen gegen Angreifer zu finden und den Leser für den Bereich der WLAN-Sicherheit zu sensibilisieren.

2 *https://www.gesetze-im-internet.de/stgb/__303b.html*

# 1 Basiswissen Funknetzwerke

## 1.1 Was ist WLAN?

**WLAN** steht für *Wireless Local Area Network*, ist also ein kabelloses lokales Netzwerk zum Übermitteln von Daten. In der Regel wird es für die drahtlose Übertragung im Internet eingesetzt. Das allzu häufig synonym gebrauchte Wort **Wi-Fi** ist hingegen ein Markenbegriff – erfunden von der Wi-Fi Alliance –, mit dem WLAN-Geräte zertifiziert werden, die dem IEEE-802.11-Standard entsprechen und somit Kompatibilität zwischen sich und anderen Wi-Fi-Produkten gewährleisten.

**IEEE** ist das *Institute of Electrical and Electronics Engineers*, ein weltweiter Fachverband von Ingenieuren, die für die Standardisierung von Techniken, Hardware und Software zuständig sind. Wi-Fi basiert auf elektromagnetischen Wellen im 2,4-GHz- und 5-GHz-Spektrum (und bald auch im 60-GHz-Frequenzbereich).[1] Dieses Buch fokussiert sich auf Wi-Fi, die Begriffe werden auch hier meist synonym verwendet.

### 1.1.1 Physikalische Grundlagen

Eine elektromagnetische Welle ist eine gekoppelte elektrische und magnetische Transversalwelle, die im freien Raum bzw. im Raum-Zeit-Kontinuum übertragen wird.[2] Um »WLAN-Wellen« besser einordnen zu können, schauen wir uns folgende Übersicht des elektromagnetischen Spektrums an:

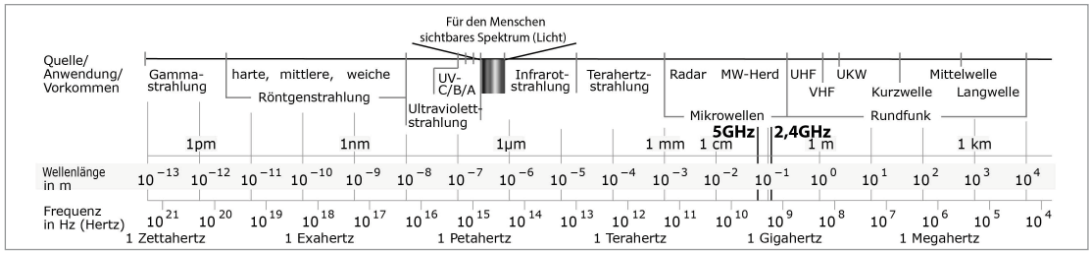



**Bild 1.1:** Das elektromagnetische Spektrum.[3]

---

1 Abgesehen von einem Sonderfall im 802.11a-Standard, der die Datenübertragung über Infrarot spezifiziert.

2 Die weitverbreitete Annahme, die Luft diene als notwendiges Übertragungsmedium, ist falsch. EM-Wellen können auch übertragen werden, wenn gar kein Medium vorhanden ist, z. B. im Weltall, also im Vakuum. Ein Medium wie Luft etc. stört eine Übertragung viel mehr.

3 Angelehnt an Horst Frank/Phrood/Anony, 2009, *https://commons.wikimedia.org/wiki/File:Electromagnetic_spectrum_c.svg, CC BY-SA 3.0.*

Auch wenn das Spektrum in beide Richtungen weiterläuft, sieht man hier den für uns relevanten Teil der elektromagnetischen Wellen. Die Wellenlänge λ (Lambda) ist dabei indirekt proportional zur Frequenz f. Der Zusammenhang lässt sich mit folgender Formel beschreiben:

```
c = λ * f <-> λ = c / f
```

Die Ausbreitungsgeschwindigkeit bei elektromagnetischen Wellen ist die Lichtgeschwindigkeit c mit 299.792.458 m/s.[4] Je weiter nach links man sich in der Skala bewegt, desto höher wird die Frequenz und damit auch die Energie der elektromagnetischen Welle. Es gilt E = h * f, wobei h für das plancksche Wirkungsquantum, eine Naturkonstante mit 6,626 * 10 - 34 Joulesekunden (Js), steht. Links der »gewöhnlichen« Gammastrahlung würde sich die kosmische Gammastrahlung mit Frequenzen von bis zu 10.000 Yotahertz ansiedeln. Hier haben wir also die hochenergetische Strahlung[5], mit der man nicht unbedingt in direkten Kontakt kommen möchte. Auf der anderen Seite der Skala befindet sich das Niederfrequenzband, Megameterwellen (1 Mm = 1000 km).

Vereinfacht kann man sagen, dass mit steigender Frequenz die übertragbare Energie, aber auch (in der Informatik) die Datenrate, steigt, die Reichweite aber abnimmt. Der Reichweitenverlust lässt sich so erklären: Je höher die Frequenz, desto höher ist auch die Wahrscheinlichkeit, dass die Welle auf ihrem Weg mit einem Atom des Mediums, das es durchqueren muss (z. B. Luft oder Beton), kollidiert und dort ihre Energie abgibt. Je höher die Dichte des Mediums, desto höher ist die Kollisionswahrscheinlichkeit. Bei einer Kollision gehen entsprechend Daten verloren. So erklärt sich auch die höhere Reichweite von Funkwellen bei direkter Sicht gegenüber jener innerhalb eines Gebäudes (Dichte Beton 200 kg/m$^3$, Dichte Luft 1,2 kg/m$^3$). Um die steigende Datenrate bei steigender Frequenz zu erklären, muss man etwas ausgeholen.

Wir wissen noch, dass die Frequenz indirekt proportional zur Wellenlänge steht. Irgendwie müssen über diese Welle Informationen übertragen werden. Da wir uns im digitalen Zeitalter befinden, blenden wir analoge Übertragungstechniken hier aus. Daten werden digital mit Nullen und Einsen gespeichert, also z. B.:

Strom an = 1, aus = 0

Vertiefung = 1, keine Vertiefung = 0 (optischer Datenträger, z. B. CD)[6]

Hochpunkt einer (EM-)Welle = 1, Tiefpunkt = 0

Je häufiger also der Phasenwechsel pro Zeit stattfindet, desto mehr Einsen und Nullen können in dieser Zeit übertragen werden und desto höher ist daher die Datenrate.

Natürlich lässt sich hier noch optimieren, und man müsste zwischen verschiedenen Modulationsverfahren unterscheiden, aber um die grundlegenden physikalischen Hin-

---

[4] Ausbreitungsgeschwindigkeit des Lichts im Vakuum. In anderen Medien variiert sie gemäß der optischen Dichte, dem Brechungsindex.

[5] Genau genommen ist die Strahlungsleistung noch abhängig vom Quantenstrom.

[6] Eigentlich ist hier die Kante zwischen Pit und Land 1 und Land & Pit selbst 0, aber das macht mein Beispiel kaputt ;)

tergründe von Datenübertragung mittels EM-Wellen zu verstehen, die für dieses Buch benötigt werden, lassen wir es in dieser vereinfachten Form erst einmal stehen. Wer sich stärker für Modulationsverfahren und den theoretischen Hintergrund interessiert, dem sei das Buch Wireless LANs von Jörg Rech empfohlen (siehe Literaturempfehlung [3]).

Es lässt sich erkennen, dass man bei der Wahl der Frequenz für die Datenübertragung per EM-Wellen immer einen Kompromiss aus Reichweite und Datenrate finden muss (von den gesetzlichen Bestimmungen einmal ganz abgesehen). Bei WLAN liegt dieser Kompromiss bei 2,4 bzw. 5 GHz und ist damit im niederfrequenten Mikrowellenspektrum angesiedelt. Ein herkömmlicher Mikrowellenherd »sendet« übrigens im gleichen Spektrum – bei 2,455 GHz. Dies ist einer der Gründe dafür, dass manche Menschen Gesundheitsbedenken bei WLAN anmelden. Jedoch ist die Sendeleistung in Europa auf 100 mWatt beschränkt, sodass eine Gesundheitsschädigung unwahrscheinlich ist.

Es gibt mittlerweile viele wissenschaftliche Studien, die entweder das eine oder das andere behaupten. Aus wissenschaftlicher Sicht ist dies also noch nicht endgültig geklärt. Jedoch sei anzumerken, dass z. B. Mobilfunk eine bis zu 20-fach stärkere Strahlungsintensität in Deutschland aufweisen darf und entsprechende Geräte direkt am Kopf bzw. Ohr verwendet werden, während beim WLAN-Gebrauch das Endgerät meist in ca. 60 Zentimetern Abstand benutzt wird. Verglichen mit GSM ist WLAN also geradezu harmlos. Dies ist aber hier nicht das Thema, und da es den Autoren zum Zeitpunkt des Verfassens dieses Buchs gesundheitlich trotz intensiver WLAN-Nutzung noch ganz gut geht, soll uns das hier nicht weiter kümmern.

Zusammenfassend kann man sagen, dass man eine elektromagnetische Welle in einem bestimmten Frequenzbereich nimmt und gewisse Phasen als 1 und 0 definiert, um drahtlos Daten zu übertragen.

### 1.1.2 Probleme bei drahtloser Datenübertragung

Drahtlose Datenübertragung ist einigen Randbedingungen ausgesetzt, gegen die sie geschützt werden muss. Es gibt auch keine direkte physische Abgrenzung des Signals, sodass die Trägerwelle meist in alle Richtungen streut und schnell an Intensität verliert. Je weiter man sich vom Sender entfernt, umso schwächer wird das Signal. Dies ist durch die Luftabsorption und die Freiraumdämpfung[7] bedingt. Des Weiteren gibt es Störungen durch Reflexion. Eine EM-Welle reflektiert an Materialien mit hohen Dämpfungswerten, sodass Wellen in alle Richtungen streuen. Diese interferieren miteinander, wodurch das Signal geschwächt wird. Hinzu kommt, dass durch die Reflexion ein und dasselbe Datenpaket mehrere Male am Router ankommen kann.

Vergleicht man drahtlose mit kabelgebundener Datenübertragung, sind vor allem die Felder der Störanfälligkeit, der Sicherheit und der erzielbaren Datenraten wesentlich komplexer. Auch gegenüber externen Einflüssen sind die Daten deutlich störanfälliger,

[7] Die Freiraumdämpfung beschreibt die Reduzierung der Leistungsdichte bei Ausbreitung elektromagnetischer Wellen im freien Raum gemäß Abstandsgesetz.

da das Signal durch nichts von potenziellen Störeinflüssen abgeschirmt ist. Jede elektromagnetische Welle kann das Signal überdecken oder mit ihm interferieren. Als Störquellen kommen alle Geräte mit einer größeren elektrischen Leistungsaufnahme infrage. Allein bei Haushaltsgeräten wären das z. B. Mixer, Mikrowellen (besonders gravierend, da gleiche Frequenz), Kühlschränke oder Rasenmäher.

Des Weiteren ist das zu durchquerende Medium, meistens Luft, ein »Shared-Medium«. Das bedeutet, dass es neben WLAN-Signalen noch eine ganze Menge anderer Signale im elektromagnetischen Spektrum und im besagten 2,4-GHz- und 5-GHz-Band gibt. Da diese Frequenzbänder fast überall auf der Welt auch noch gebühren- und genehmigungsfrei sind (siehe den Abschnitt, »Rechtsgrundlagen«), funkt hier neben WLAN und dem bereits benannten Mikrowellenherd noch sehr viel mehr. Einige Beispiele sind: Bluetooth (IEEE 802.15.1), Wireless USB, ZigBee (Heimautomation, Sensornetzwerke, IEEE 802.15.4), drahtlose Mikrofone, Funkfernsteuerung von Modellautos, -booten, -flugzeugen, -hubschraubern oder Funkkameras. Demnach muss bei drahtlosen Netzwerken eine gewisse Fehlererkennung oder Fehlervermeidung implementiert werden. Fehlerhafte Daten müssen teilweise erneut gesendet werden, sodass die effektive Datenrate sinkt.

Da wir keine physikalische Eingrenzung des Signals in ein geschütztes Medium wie ein abgeschirmtes Kupferkabel haben, kann auch jederzeit ein Unbefugter das Signal abfangen und versuchen, gesendete Daten mitzulesen oder sogar zu manipulieren. Die übertragenen Daten dürfen also keineswegs im Klartext vorliegen, sondern müssen durch Algorithmen verschlüsselt werden. Bei den Endgeräten ergibt sich dadurch die Notwendigkeit der Ver- und Entschlüsselung, es wird also Rechenleistung benötigt. Auch kann durch die Verschlüsselung ein gewisser Overhead entstehen, der sich wieder negativ auf die Performance auswirkt. [3] Zudem sind meistens mehrere User in einem WLAN eingewählt, sodass sich die Nettodatenrate nochmals teilt.

Aufgrund dieser Probleme und der Beschränkung auf das vorgegebene Frequenzband konnten in den Anfängen des WLAN nur wenige MBit/s übertragen werden. Mithilfe immer komplexerer Verfahren und Algorithmen konnte man diese Problematik jedoch überwinden, sodass wir heute selbst in der Praxis Datenraten von mehreren Hundert MBit/s realisieren können, sodass WLANs den etablierten 1000Base-T-Ethernet-Kabeln immer ebenbürtiger werden. Dazu war eine lange Entwicklung notwendig, die im folgenden Kapitel erläutert werden soll.

## 1.2 Geschichte des WLAN

WLAN war nicht immer so verbreitet und selbstverständlich wie heute. Eine wirkliche Ausdehnung fand es erst in diesem Jahrtausend. Doch bereits 1940 wurde von Hedy Lamarr und George Antheil das sogenannte **Frequency Hopping** erfunden. Lamarr war eine Schauspielerin, Antheil ein Komponist und Pianist. Wie man der Jahreszahl entnehmen kann, wurde es damals für das Militär entwickelt. Es sollte Torpedos vor der gegnerischen Entdeckung von Steuer- und Störsignalen schützen.

Der nächste nennenswerte Schritt Richtung Wi-Fi war die Entwicklung des **Aloha-Net**. Dieses Funknetzwerk verband verschiedene Standorte der Universität von Hawaii miteinander, sodass man von überall auf den Zentralrechner zugreifen konnte. Die Universität ist über mehrere Inseln verteilt. Dort war bereits eine Collision-Avoidance-(CA-) Funktion implementiert, die dafür sorgte, dass bei Kollisionen einer der Kanäle sein Datenpaket nach einer zufälligen Zeitspanne erneut sendete (der deutsche Begriff Kollisionsvermeidung ist nicht gebräuchlich).

1988 entwickelte COMTEN die **WaveLAN**-Produktfamilie, die durch NCR, AT&T und Lucent vertrieben wurde. Diese Technologie ist gut mit dem heutigen Wi-Fi zu vergleichen, da sie im 900-MHz- oder 2,4-GHz-Bereich arbeitete. Da es für diese Art von Funknetzwerk noch keinen Standard gab, legte man das Protokoll dem IEEE 802 LAN/MAN Standards Committee vor, das daraus den 802.11-Standard entwickelte und 1997 verabschiedete. Damit war Wi-Fi geboren.

### 1.2.1 IEEE 802.11

Der am 26.06.1997 verabschiedete ursprüngliche WLAN-Standard spezifizierte erstmals den **PHY-** und den **MAC-Layer** für lokale Funknetzwerke. Der PHY-Layer entspricht dem Physical Layer (1. Schicht) aus dem ISO-OSI-Schichtenmodell. Er beschreibt, wie das Signal auf physikalischer Ebene übertragen, codiert und moduliert wird, während der MAC-Layer dem Data-Link-Layer (2. Schicht) im ISO-OSI-Modell zugeordnet werden kann. Dieser dient der Verbindungssicherung, sichert mit CRC-Codes[8] die korrekte Datenübertragung, bestimmt das Format eines WLAN-Frames sowie dessen Fragmentierung und implementiert Managementfunktionen. Alle 802.11-Standards spezifizieren und operieren jeweils auf diesen beiden Schichten. Beim ursprünglichen 802.11-Standard gab es zwei Spreizspektrumsverfahren für die Übertragung per Radiowellen im 2,4-GHz-Band und ein Infrarotverfahren (PHY-Layer). Der Standard erlaubte eine maximale Bruttodatenrate von 2 MBit/s. Es wurden auch erstmals die Kommunikationsmodi Ad-hoc und Infrastruktur definiert (siehe Kapitel 2.2, »WLAN-Topologien«).

### 1.2.2 IEEE 802.11a

1999 folgten zwei Erweiterungen. Eine davon war der 802.11a-Standard, der am 16.09. veröffentlicht wurde. Er arbeitete erstmals im 5-GHz-Bereich und konnte bereits 54 MBit/s übertragen. Es nutzte, ebenfalls erstmalig, das Modulierungsverfahren *Orthogonal Frequency-Divison Multiplexing* (OFDM), das eine Sonderform des *Frequency-Divison Multiplexing* (FDM) darstellt. Dieser Standard fand keine große Verbreitung. In Deutschland durften 802.11a-Geräte wegen rechtlicher Hürden auch nur sehr eingeschränkt verwendet werden, woraus 2002 die Anpassung in IEEE 802.11h hervorging.

[8] Ein Verfahren, das eine Prüfsumme errechnet, um Fehler bei Datenübertragungen zu erkennen.

### 1.2.3 IEEE 802.11b

Die zweite Erweiterung wurde am 09.12.1999 veröffentlicht und steigerte die Bruttodatenrate auf 11 MBit/s im damals gebräuchlicheren 2,4-GHz-Band. In der Praxis wurden bei TCP etwa 5,9 MBit/s und 7,1 MBit/s bei UDP erreicht. Die Performancesteigerung gelang durch ein Redesign im Physical Layer. Dieser Standard setzte sich schnell durch und wurde auch im Apple iBook implementiert.

### 1.2.4 IEEE 802.11g

Obwohl auch der am 12.06.2003 veröffentlichte g-Standard nur Datenraten von 54 MBit/s bot, stellte er einen gewaltigen Schritt nach vorne dar und erfuhr schnell eine starke Verbreitung. Dadurch, dass er das 2,4-GHz-Band nutzte, gab es auch in Europa und Deutschland wenig rechtliche Einschränkungen, sodass er schnell in entsprechender Hardware umgesetzt werden konnte. Als Übertragungsverfahrung kam weiterhin OFDM zum Einsatz. Auch das erste iPhone hatte neben 802.11b diesen Standard implementiert. Er half maßgeblich bei der Verbreitung von WLAN.

### 1.2.5 IEEE 802.11n

Mit diesem Standard wurde das erste WLAN spezifiziert, das auch unter heutigen Gesichtspunkten noch als schnell gelten kann. Der am 11.09.2009 veröffentliche Standard, auch als High-Throughput-Erweiterung bekannt, führte Veränderungen im Physical und im MAC-Layer ein. Einer der Gründe für die drastisch gestiegene Performance ist die Einführung der **MIMO**-Technologie – *Multiple Input and Multiple Output*. Diese erlaubt das gleichzeitige Senden mehrerer Signale zwischen zwei WLAN-fähigen Geräten, wodurch sich die Datenrate entsprechend vervielfacht.

Der Standard erlaubt 4x4 MIMO, dabei steht die erste Zahl für die maximale Anzahl von sendenden und die zweite für die empfangenden Antennen. Manchmal findet man noch eine dritte Zahl 4x4:4, die für die Anzahl von einzelnen unabhängigen Datenströmen, auch **Spatial Streams** genannt, steht. Außerdem funkt der Standard im 2,4-GHz- und im 5-GHz-Bereich, was als **Dual Band** bezeichnet wird.

Das 5-GHz-Band bietet den Vorteil, viel mehr Frequenzen und damit viele nicht überschneidende Bänder zu besitzen. Dies hat vor allem in dicht besiedelten Gebieten große Vorteile, da das 2,4-GHz-Netz mit lediglich drei bis vier nicht überlappenden Channels (je nach Land unterschiedlich) schnell überlastet ist. Außerdem ermöglicht eine höhere Frequenz auch eine höhere Datenrate.

Auch können mit WLAN 40-MHz-Channels (statt 20 MHz) genutzt werden, und eine bessere Codierung mit weniger Overhead erlaubt allgemein mehr Bits/Hertz als bei vorausgegangenen Standards. Maximal können mit diesem Standard 600 MBit/s übertragen werden. Wie in jedem Standard ist das ein in der Praxis nicht zu erreichender Optimalwert. Jedoch reicht die Datenrate auch in der Praxis erstmals für die Übertragung hochauflösender Videos aus.

### 1.2.6 Weitere historische Standards

Neben den bekannten a/b/g/n-Standards gibt es weitere Standards, die keine abgeschlossene WLAN-Entwicklungsstufe darstellen, sondern lediglich kleinere Verbesserungen der bestehenden Standards beinhalten.

| *Arbeitsgruppe* | *Beschreibung* |
|---|---|
| IEEE 802.1x | Authentifizierung bei IEEE-802-Netzen mittels RADIUS-Server. |
| IEEE 802.11d | Bietet länderspezifischen Informationsaustausch für internationales Roaming. |
| IEEE 802.11e | MAC-Erweiterung für die Implementierung von Quality of Service (QoS) und einer Performanceverbesserung. |
| IEEE 802.11f | Definition des Inter Acces Point Protocol (IAPP). |
| IEEE 802.11h | Dynamic Frequency Selection (DFS) & Transmit Power Control (TPC). |
| IEEE 802.11i | MAC-Erweiterung zur Verbesserung der Datensicherheit. |
| IEEE 802.11p | Optimierung für Datenaustausch bei Fahrzeugen. |
| IEEE 802.11r | Optimierung des Roamings (Fast Roaming). |
| IEEE 802.11s | Definition eines drahtlosen Mesh-Netzwerks. |
| IEEE 802.11w | Protected Management Frames. |

802.11-Arbeitsgruppen und -Standarderweiterungen [4]

2007 und 2012 wurden alle bis dahin entstandenen Standards unter den Standards **IEEE 802.11-2007** und **IEEE 802.11-2012** zusammengefasst. So konnte man durch ein einziges Dokument an alle relevanten Informationen gelangen.

Die Standards können unter folgender Adresse abgerufen werden:

- IEEE 802.11-2007: *http://bit.ly/2niBlKs*
- IEEE 802.11-2012: *http://bit.ly/1LuCLC0*

### 1.2.7 IEEE 802.11ac

Willkommen in der Gegenwart. Der im Dezember 2013 veröffentlichte AC-Standard stellt den momentanen Stand der Technik dar. Im Endzustand könnten bis zu 6,9 GByte/s erreicht werden. Da der neue Standard aber im Vergleich zum Vorgänger viele komplexe Verbesserungen und Veränderungen enthält, hat sich die IEEE entschieden, den Standard in verschiedenen Wellen (meist Wave genannt) auszurollen. So haben Hardwarehersteller eine Chance, zeitnah entsprechende Hardware zu entwickeln. Der Standard arbeitet nur noch im 5-GHz-Bereich – wie früher einmal 802.11a. Der 2,4-GHz-Bereich ist wegen der geringen Breite des verfügbaren Spektrums und der physikalisch

bedingten geringeren Übertragungsrate im Very-High-Throughput-Bereich weniger relevant geworden.

Um genügend Reichweite zu generieren, kombinieren WLAN-Router und Endgeräte die ac- und n-Standards. Auch die Kanalbreite ist weiter gestiegen. Während in der ersten Wave (Wave 1) noch 80 MHz Standard waren (maximale Datenrate 1,3 GBit/s), gibt es ab Wave 2 die Möglichkeit, 160 MHz breite Kanäle zu erstellen. Hier wären dann selbst im 5-GHz-Spektrum (in Europa) nur noch zwei nicht überlappende Channels möglich. Auch wird MIMO jetzt mit bis zu 8x8 mit acht Spatial Streams unterstützt. Sogar **MU-MIMO** (*Multi User MIMO*) ist jetzt möglich, das bei verschiedenen Clients gleichzeitiges MIMO, also eine Übertragung mehrerer Spatial Streams, ermöglicht.

Eine weitere Neuerung ist das **Beamforming**. Auch wenn es erstmals im n-Standard spezifiziert wurde, fand es bei ac-WLAN das erste Mal auch in der Praxis Anwendung. Hierbei wird das Signal wie bei einer Richtantenne so verändert, dass es in eine Richtung (vorzugsweise Richtung Client) stärker strahlt. Noch ist die Auswahl Beamforming-fähiger Endgeräte aber überschaubar. Als letzte nennenswerte Neuerung wurde ein verbessertes Modulationsverfahren eingeführt. Genau genommen wurden mehrere Modulationsverfahren eingeführt, wobei abhängig von der Übertragungsqualität, also von Abstand und Störquellen, das am besten geeignete Verfahren angewandt wird. Wenn die Übertragungsqualität sehr gut ist, wird ein Verfahren gewählt, bei dem besonders viele Bits pro Übertragungsschritt, viele Nutzdaten und kaum Sicherungsdaten übertragen werden. In der höchstmöglichen Stufe (MCS 9) wird mit QAM256 8bit/Übertragungsschritt mit einer Coderate (Nutzdaten/Gesamtdaten) von 5/6 angewandt.

Einige Hersteller fangen mittlerweile sogar an, QAM1024 in ihre Router zu implementieren (10 Bit proSchritt). Dies entspricht nicht mehr dem Standard, sondern ist ein Vorstoß von Broadcom, genannt NitroQAM. Dafür werden noch höhere Datenraten möglich. Da aber bereits für QAM256 die Verbindungsqualität nahezu perfekt sein muss, ist es unrealistisch, dass QAM1024 in der Praxis Anwendung finden wird. Um auf die anfangs genannte maximale Datenrate von 6,9 GBit/s zu kommen, muss 8x8 MIMO mit 160-MHz-Kanälen und 256QAM verwendet werden. Auch wenn in naher Zukunft entsprechende Hardware erhältlich ist, wird man in der Praxis nie solche Werte erreichen. Zurzeit mangelt es sogar noch an guten Wave-2-WLAN-Adaptern.

Während es schon genügend Wave-2-WLAN-Router gibt, ist momentan (Stand April 2017) der ASUS PCE-AC88 der einzige Dual-Band-Wireless-AC-Adapter, der 4x4 MU-MIMO ermöglicht. Er benötigt jedoch einen PCIe-Steckplatz. In Laptops sind in der Regel nur 2x2-Adapter eingebaut, auch in Smartphones ist meistens kein MIMO möglich. Lediglich die neueren Qualcomm-Chips unterstützen 2x2 MIMO. Da der Standard schon seit einigen Jahren veröffentlicht ist, sind jetzt die Hersteller dran, auch entsprechende Clienthardware zu liefern. Vor allem durch das enorme Platzproblem eines 4x4-Antennendesigns bei Smartphones dürfte dies aber noch einige Zeit dauern.

### 1.2.8 IEEE 802.11ad

Der ad-Standard, auch als *Wireless Gigabit* (WiGig) bezeichnet, ist der erste WLAN-Standard, der im 60-GHz-Bereich arbeitet. Der am 28.12.2012 veröffentlichte Standard zeugt nicht nur davon, dass die VHT Group offensichtlich keine Weihnachtsferien kennt[9], sondern er ist damit auch chronologisch eigentlich vor dem ac-Standard anzusiedeln. Da die Verbreitung und Entwicklung von entsprechenden Geräten aber deutlich nach der von ac-Geräten stattfand, wird er hier auch nach dem ac-Standard gelistet. Besonders ist, dass er im Bereich von 57 bis 66 GHz mit einer Kanalbreite von 2,16 GHz arbeitet, sodass vier Kanäle zur Verfügung stehen.

Durch unterschiedliche Regulatorien in verschiedenen Ländern differiert die tatsächlich zur Verfügung stehende Frequenzbreite stark. So ist in Australien z. B. nur ein einziger Kanal nutzbar (erlaubte Frequenzen 59,4 bis 62,9 GHz), während in der EU und in Japan alle Kanäle zur Verfügung stehen. Trotz eines Maximums von vier Kanälen dürfte das Problem des »überfüllten Luftraums« des 2,4-GHz-Spektrums hier so gut wie vernachlässigbar sein. Bedingt durch die hohe Frequenz von 60 GHz, findet durch die Luftabsorption und die Freiraumdämpfung eine so starke Signaldämpfung statt, dass selbst unter optimalen Bedingungen und bei Sichtkontakt maximal 20 m Reichweite realisiert werden können.

Innerhalb von Gebäuden beschränkt sich eine ad-Funkzelle auf einen Raum, da Türen und Wände so gut wie gar nicht durchdrungen werden. Hieran sieht man, dass die Grenzen zwischen WLAN und WPAN (*Wireless Personal Area Network*) schwimmend sind. Dafür sind aber auch Datenraten von bis zu 6,757 GHz möglich. Der Standard ermöglicht wie schon ac WLAN-Beamforming, unterstützt jedoch kein MIMO. Des Weiteren wurde ein Power-Management zum Energiesparen implementiert. Aufgrund der hohen Datenrate und der geringen Reichweite eignet sich dieser Standard eher für die Drahtlosanbindung von Computerperipherie statt als Ersatz der alten Standards. So könnte man sogar drahtlose 4k-HDR-Videoübertragung mit 60 fps ermöglichen.

Noch verlockender ist die Ablösung des bisherigen Kabelgewirrs an Maus, Tastatur, Drucker und Boxen. Auch drahtlose USB-3.0-Hubs könnten so realisiert werden. Obwohl der Standard schon einige Jahre verabschiedet ist, gibt es bisher so gut wie keine entsprechende Hardware. 2016 kamen mit dem TP-Link Talon AD7200 und dem Netgear Nighthawk X10 erstmals zwei ad-fähige WLAN-Router auf den Markt. Auf Clientseite unterstützt der Qualcomm Snapdragon 835 erstmals ad-WLAN, sodass man in nächster Zeit wohl Smartphones mit Tri-Band-WLAN (2,4 + 5 + 60 GHz) erwarten kann.

[9] Vielleicht war man aber auch auf dem 29C3

### 1.2.9 IEEE 802.11ax

Dieser Standard befindet sich in Entwicklung und soll später einmal eine Verbesserung des 2,4-GHz- und des 5-GHz-Bands ermöglichen. Er wird damit die Nachfolge von n/ac-WLAN antreten. Der Standard strebt folgende drei Ziele an: verbesserter Datendurchsatz, bessere Reichweite und neue Stromsparfeatures. Es sind Datenraten von 10 GByte/s geplant. Dies soll durch die Unterstützung von QAM1024, einem neuen Modulationsverfahren OFDMA (*Orthogonal Frequency Division Multiple Access*), einem bidirektionalen MU-MIMO sowie weitere Verbesserungen erreicht werden.

Der Standard soll auch mit kleinen Embedded Devices oder IoT-Devices, die nur 20-MHz-Channels unterstützen, kompatibel bleiben. Der seit Mai 2013 entwickelte Standard befindet sich momentan noch im Entwurfsstadium. Planmäßig sollte im Mai 2017 Entwurf 2.0 veröffentlicht werden. Wegen der hohen Anzahl von Kommentaren am Entwurf 1.0 könnte sich das noch etwas verzögern.

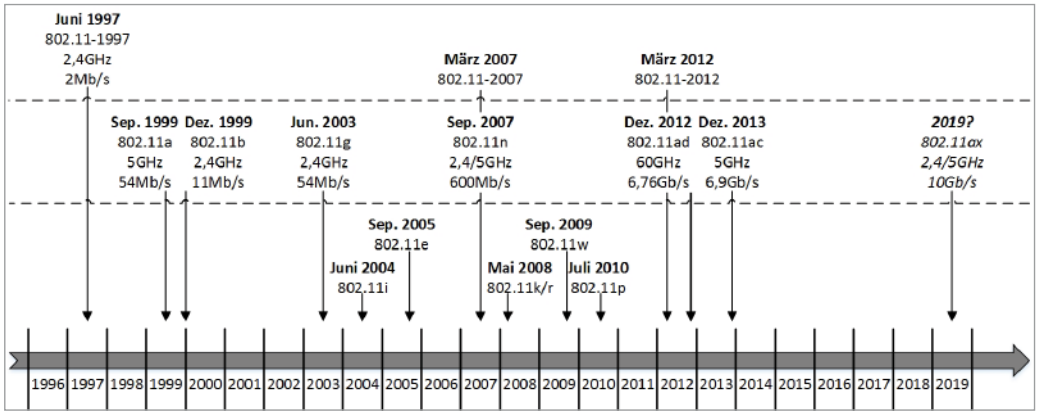



**Bild 1.1:** Zeitstrahl zu Spezifikationen der WLAN-Technologie.

## 1.3 WLAN ist nicht nur IEEE 802.11

Dies ist ein Überblick über WLAN-Technologien, die parallel zu Wi-Fi existieren. In diesem Buch werden wir uns jedoch auf Wi-Fi fokussieren. Da der Übergang zwischen WPAN, WLAN und WMAN fließend ist, werden hier auch Technologien gelistet, die man neben WLAN den beiden anderen Netzwerken zuordnen könnte.

### 1.3.1 Bluetooth

Meistens als WPAN (*Wireless Personal Area Network*), manchmal als WLAN bezeichnet, ist Bluetooth der einzige Standard, der neben Wi-Fi eine größere Bedeutung hat. Er

wurde in den 1990ern von der Bluetooth Special Interest Group entwickelt und unter dem IEEE-Standard 802.15.1 veröffentlicht. Möglich sind verbindungslose sowie verbindungsbehaftete Übertragungen von Punkt zu Punkt und Ad-hoc- oder Piconetze. Bluetooth wird bei drahtlosen Mäusen und Tastaturen eingesetzt. Hier bietet sich verglichen mit herkömmlichen Funkmäusen der Vorteil, dass sich (bei eingebautem Bluetooth-Empfänger) ein USB-Port für den Empfänger sparen lässt.

Auch lassen sich über Bluetooth Daten zwischen Smartphones übertragen. Seltener implementieren Spiele-Apps einen Mehrspielermodus über Bluetooth. Auch gibt es Bluetooth-Chatprogramme. Obwohl der aktuelle Bluetooth-Standard 5 bis zu 20 m (100 mW) weit sendet und seine Reichweite damit deutlich über ad-WLAN liegt, wird es meist als WPAN bezeichnet – daher wird in diesem Buch nicht näher darauf eingegangen. Dies liegt unter anderem daran, dass Bluetooth viel im Low-Energy-Bereich eingesetzt wird, um kleinere Devices miteinander zu verbinden. Da maximal 2 MBit/s an Datenrate verfügbar sind, ergibt sich ein etwas anderes Anwendungsgebiet als beim herkömmlichen WLAN bzw. Wi-Fi.

Bluetooth benutzt wie WLAN das zulassungsfreie 2,4-GHz-Spektrum, genau genommen liegt es zwischen 2,402 und 2,480 GHz. Das hat zur Folge, dass Bluetooth-Geräte in unmittelbarer Nähe zu WLAN-Sendern/-Empfängern die Empfangsqualität beeinflussen können.

### 1.3.2 ZigBee

ZigBee ist ein drahtloses Netzwerk, das vor allem in der Hausautomation eingesetzt wird. Es unterstützt nur geringe Datenraten und hat erst durch das Aufkommen von Smart Homes an Bedeutung gewonnen. Seitdem erscheinen regelmäßig neue ZigBee-kompatible Geräte (z. B. smarte Thermostate, fernsteuerbare Steckdosen und Sensoren). Es hat eine ähnliche Reichweite wie Wi-Fi (10 bis 100 m) und funkt im 2,4-GHz- (weltweit), 868-MHz- (Europa) und 915-MHz-Bereich (USA). Dabei bietet es eine maximale Datenrate von 250 KByte/s. Es ist unter der Norm IEEE 802.15.4 spezifiziert, die trotz der Reichweite als WPAN gilt.

### 1.3.3 Z-Wave

Z-Wave ist ein Standard der Firma Sigma Designs und der Z-Wave Alliance, der für Heimautomation entwickelt wurde. Damit ist er ein direkter Konkurrent von ZigBee. Er funkt im 800-MHz-Spektrum und erreicht geringe Datenraten von 100 KByte/s . Trotz der niedrigen Frequenz hat Z-Wave nur eine Reichweite von maximal 150 m, da es eine geringe Sendeleistung von 25 mW spezifiziert. Das hat den Vorteil, dass das Signal zwar Türen und Wände durchdringt, jedoch kaum über die eigene Wohnung hinausreicht. Da bei Heimautomation bisher nur wenige Daten erforderlich sind, stört die kleine Datenrate nicht. Z-Wave ist ein aktiver Standard, zu dem regelmäßig neue Geräte erscheinen.

### 1.3.4 HiperLAN

HiperLAN wurde ab 1991 als Wi-Fi-Alternative entwickelt und ist damit ausnahmsweise mal eindeutig ein WLAN. Die erste Version erschien 1996. Es wurden drei weitere Versionen entwickelt, die allerdings alle gleichermaßen keine Verbreitung fanden. Jedoch wurde der Physical Layer von HiperLAN/2 (Februar 2000) größtenteils in IEEE 802.11a übernommen, sodass ein Teil dieser Technologie weiterlebt. Beide Technologien basieren auf 5-GHz-EM-Wellen mit maximal 54 MByte/s Übertragungsrate, wodurch sich die Ähnlichkeit erklärt.

### 1.3.5 HomeRF

Eine weitere tote Technologie ist HomeRF, die eine Kreuzung von DECT und Wi-Fi darstellt. Sie wurde zwischen 1998 und 2003 entwickelt und war auf Privathaushalte zugeschnitten. HomeRF verwendet das 2,4-GHz-Spektrum, und es wurden Geräte mit bis zu 10 MBit/s Datenrate entwickelt.

### 1.3.6 WiMAX

WiMAX ist im IEEE-802.16-Standard spezifiziert und wurde bzw. wird vom WiMAX-Forum entwickelt. Es funkt im Frequenzbereich zwischen 2 und 66 GHz und bietet im aktuellen 802.16m-Standard bis zu 1 GByte/s Datenrate. Es operiert wie WLAN auf dem PHY- und dem MAC-Layer, eine WiMAX-Basisstation darf aber mit bis zu 30 Watt senden. So ist eine Reichweite von bis zu 50 km möglich wird. WiMAX lässt sich also auch als *Wireless Metropolitan Area Network* (WMAN) bezeichnen.

Es stellt also eher eine Alternative zu 3G/4G als zu Wi-Fi dar. Möchte man eine Datenrate von mindestens 10 MByte/s bereitstellen, sind maximal zehn Kilometer Reichweite drin. Hohe Datenraten sind erst bei einer Entfernung von unter einem Kilometer möglich. Es wird vor allem für die Datenübertragung in Städten zwischen entfernten Gebäuden über Dachantennen verwendet. Darüber hinaus gibt es auch WiMAX-USB-Adapter, die aber mit entsprechend geringerer Sendeleistung funken. Obwohl WiMAX eine eher unwesentliche Verbreitung hat und schon oftmals für tot erklärt wurde, wird es von der 802.16 Group immer noch weiterentwickelt.

### 1.3.7 Li-Fi

Neben der Datenübertragung im Mikrowellenbereich gibt es auch Ansätze, Daten im Spektralbereich des sichtbaren Lichts zu übertragen. Bereits 1955 kam die erste Fernbedienung für Fernseher auf den Markt, die Zenith Flash-Matic, die über Lichtblitze das Programm wechseln und den Fernseher ein- und ausschalten konnte. Jedem bekannt dürfte die Datenübertragung per Infrarot in der Prä-Smartphone-Ära sein. Man erinnere sich, wie in jeder Pause Schüler allen Alters auf dem Schulhof standen und die neuesten Klingeltöne des Jamba-Spar-Abos per Infrarot auf die Handys der Mitschüler

übertrugen. Heutzutage fristet das Thema drahtlose Datenübertragung über sichtbares Licht ein wenig relevantes Nischendasein.

Im weiteren Sinn ist jeder Umgebungslichtsensor ein Instrument, um (unidirektional) »Daten« per sichtbares Licht zu übertragen. Im engeren Sinn ist hier vor allem das Li-Fi-Konsortium zu erwähnen, das sich auf professionellem Niveau mit Technologie und Anwendung von optischer Datenübertragung auf kurzer Distanz beschäftigt. Das 2011 von Harald Haas gegründete Konsortium beschäftigt sich mit dem Austausch von Forschung, aber auch mit der Entwicklung von Technologien, die eine Alternative zu WiGig-WLAN (802.11ad) darstellen könnten. Serienreife Produkte sind bisher jedoch nicht erschienen (*http://www.lificonsortium.org/*).

# 14 Anhang

## 14.1 Wireshark-Filter

In den Beispielen dieses Buchs kommen an vielen Stellen Wireshark und dessen Displayfilterfunktion zum Einsatz. In diesem Kapitel haben wir die wichtigsten Displayfilter im WLAN-Kontext zusammengefasst, damit Sie sie bequem an einer Stelle nachschlagen können. Der Displayfilter schränkt nur die Anzeige der empfangenen Pakete ein. Um die Pakete bereits beim Empfang zu filtern, sind sogenannte **CaptureFilters** notwendig. Mehr dazu finden Sie im Wireshark-Wiki:

*https://wiki.wireshark.org/CaptureFilters*

Viele Menschen nutzen in Wireshark überwiegend simple Filter und sind sich nicht darüber im Klaren, wie viele Filtermöglichkeiten es gibt, um sehr exakte Ergebnisse zu erhalten. Wir haben bereits an einigen Stellen im Buch komplexere Filter verwendet, um ganz nebenbei auf die »Mächtigkeit« von Wireshark aufmerksam zu machen. Hier ist das gesamte Wissen noch einmal in kompakter Form zusammengefasst.

### 14.1.1 Logische Operatoren

Hier finden Sie sämtliche Operatoren von Wireshark im Überblick:

| *Deutsch* | *Englisch* | *C-Operation* |
|---|---|---|
| Gleich | eq | == |
| Ungleich | ne | != |
| Größer | gt | › |
| Kleiner | lt | ‹ |
| Größer gleich | ge | ›= |
| Kleiner gleich | le | ‹= |
| Enthält | contains | |
| Gleicht | matches | ~ |
| Bitweises UND | bitwise_and | & |

### 14.1.2 Verknüpfungsoperatoren

| *Beschreibung* | *Englisch* | *C-Operation* |
|---|---|---|
| Negation | not | ! |
| Logische UND-Verknüpfung | and | && |
| Logische ODER-Verknüpfung | or | \|\| |

### 14.1.3 Filter nach Frame-Typ und Frame-Subtyp

| *Frame-Typ* | *Filter* |
|---|---|
| Management-Frames | wlan.fc.type eq 0 |
| Control-Frames | wlan.fc.type eq 1 |
| Data-Frames | wlan.fc.type eq 2 |

| *Frame-Subtyp* | *Filter* |
|---|---|
| Association Request | wlan.fc.type_subtype eq 0 |
| Association Response | wlan.fc.type_subtype eq 1 |
| Probe Request | wlan.fc.type_subtype eq 4 |
| Probe Response | wlan.fc.type_subtype eq 5 |
| Beacon | wlan.fc.type_subtype eq 8 |
| Authentication | wlan.fc.type_subtype eq 11 |
| Deauthentication | wlan.fc.type_subtype eq 12 |

Statt »eq« kann auch »==« verwendet werden.

### 14.1.4 Weitere nützliche Filter

| *Zweck* | *Filter* |
|---|---|
| Selektion von Frames durch MAC-Adresse. | wlan.addr==xx:xx:xx:xx:xx:xx |
| Nur Pakete eines Protokolls anzeigen lassen. | protokollname (Kleinbuchstaben) |
| Zeigt den Vier-Wege-Handshake an. | eapol |
| Nach einer Absender-(Source-)IP filtern. | ip.src == xxx.xxx.xxx.xxx |
| Nach einer Ziel-(Destination-)IP filtern. | ip.dst == xxx.xxx.xxx.xxx |
| Nach Website filtern. | http.host==»genauer.Website.tld« |

### 14.1.5 Wildcards

Bei Wireshark werden leider nicht die klassischen Wildcards wie Asterisk und Prozent verwendet. Stattdessen gibt es für unterschiedliche Zwecke verschiedene Schreibweisen und Filter. Um z. B. nach allen IPs zu filtern, die mit `192` beginnen, kann man nicht `ip.dst == 192*` schreiben, sondern verwendet die CIDR-Schreibweise (*Classless Inter Domain Routing*):

```
ip.dst == 192.0.0.0/8
```

Um nach allen Paketen zu filtern, die von einer Website kommen, wird die `contains`-Funktion benutzt:

```
http.host contains "teil.der.website.tld"
```

Alle Filter aus Wireshark zu WLAN lassen sich in der Dokumentation von Wireshark finden: *https://www.wireshark.org/docs/dfref/w/wlan.html*.

## 14.2 Abkürzungsverzeichnis

In diesem Buch tauchen zahlreiche Abkürzungen auf, und wir waren sehr bemüht, die Abkürzung bei initialer Nennung zu erläutern. Das mag uns nicht immer gelungen sein, deshalb haben wir hier alle wichtigen Abkürzungen und ihre Bedeutung in einer Übersicht gesammelt:

| | |
|---|---|
| ACK | Acknowledgement |
| AES | Advanced Encryption Standard |
| AP | Access Point |
| ASCII | American Standard Code for Information Interchange |
| BGH | Bundesgerichtshof |
| BNetzA | Bundesnetzagentur |
| BSSID | Basic Service Set Identification |
| CCMP | Counter Mode Cipher Block Chaining Message Authentication Code Protocol |
| CISO | Chief Information Security Officer |
| CRC | Cyclic Redundancy Check |
| CSMA/CA | Carrier Sensing Multiple Access/Collision Avoidance |
| CTS | Call to Send |
| DFS | Dynamic Frequency Selection |
| DHCP | Dynamic Host Control Protocol |
| DIP-Schalter | Dual In-line Package-Schalter |

| | |
|---|---|
| DNS | Domain Name System (Protocol) |
| EAP | Extensible Authentication Protocol |
| ESSID | Extended Service Set Identifier |
| ETSI | European Telecommunications Standards Institute |
| EULA | End User License Agreement |
| FF | Freifunk |
| GPL | GNU Public License |
| HTTP | Hyper Text Transport Protocol |
| IDS | Intrusion Detection System |
| IEEE | Institute of Electrical and Electronics Engineers |
| IETF | Internet Engineering Task Force |
| ISO | International Organization for Standardization |
| IPS | Intrusion Prevention System |
| IV | Initialisierungsvektor |
| KMU | kleine und mittlere Unternehmen |
| LAN | Local Area Network |
| LDAP | Lightweight Directory Access Protocol |
| LEAP | Lightwight Extensible Authentication Protocol |
| LEDE | Linux Embedded Development Environment |
| MAC | Media Access Control |
| MBR | Master Boot Record |
| MD5 | Message-Digest Algorithm 5 |
| MIC | Message Integrity Check |
| MIMO | Multiple Input Multiple Output |
| MU-MIMO | Multi User MIMO |
| NFC | Near Field Communication |
| OSI-Modell | Open Systems Interconnection Model |
| PBKDF2 | Password-Based Derivation Function 2 |
| PC | Personal Computer |
| PDA | Personal Digital Assistant |
| PEAP | Protected Extensible Authentication Protocol |
| POS | Point of Sale |
| PSK | Pre-Shared Key |
| RA | Receiver Address |

| | |
|---|---|
| RADIUS | Remote Authentication Dial-In User Service |
| RC4 | Ron's Code 4 |
| RFC | Request for Comment |
| RTS | Request to Send |
| SDMA | Space Division Multiple Access |
| SNMP | Simple Network Management Protocol |
| SSH | Secure Shell |
| SSID | Service Set Identifier |
| SSL | Secure Sockets Layer |
| STA | Station |
| StGB | Strafgesetzbuch |
| StVO | Straßenverkehrsordnung |
| TA | Transmitter Address |
| TCP/IP | Transmission Control Protocol/Internet Protocol |
| TFTP | Trivial File Transfer Protocol |
| TKIP | Temporal Key Integrity Protocol |
| TLS | Transport Layer Security |
| TMG | Telemediengesetz |
| TPC | Transmit Power Control |
| USB | Universal Serial Bus |
| WEP | Wired Equivalent Privacy |
| WIDS | Wireless Intrusion Detection System |
| WiGig | Wireless Gigabit |
| WIPS | Wireless Intrusion Prevention System |
| WLAN | Wireless Local Area Network |
| WMAN | Wireless Metropolitan Area Network |
| WNIC | Wireless Network Interface Controller |
| WPA | Wi-Fi Protected Access |
| WPAN | Wireless Personal Area Network |
| WPS | Wi-Fi Protected Setup |
| WRAP | Wireless Robust Authentication Protocol |
| WWW | World Wide Web |
| VPN | Virtual Private Network |
| XSS | Cross-Site-Scripting |

## 14.3 Buchempfehlungen

[1] Schnelleinstieg Ubuntu

Walter Immler

Dieses Buch ist der ideale Guide für blutige Linux-Anfänger, um sich mit diesem Betriebssystem auseinanderzusetzen und ein fundiertes Grundwissen zu erwerben.

[2] Hacking mit Kali

Andreas Weyert

Andreas Weyert schrieb schon den Franzis-Bestseller »Netzwerk-Hacking«. Mit diesem Werk verfasste er ein gedrucktes Wiki und Tutorial für Kali und dessen Tools. Beginnend mit der simplen Installation des Debian-Derivats, führt das Buch über die Vorstellung der wichtigsten Kali-Tools zu ihren Einsatz in der Praxis.

[3] Wireless LANs

Jörg Rech

Der Autor vermittelt umfassendes Grundwissen der WLAN-Technologie. Praxisorientiert werden die Details des WLAN-Standards für eine konkrete Umsetzung herangezogen und alle Fragen zum Einsatz von WLANs beantwortet. Dabei wird sehr genau auf den technischen Hintergrund eingegangen.

[4] Die Kunst der Täuschung: Risikofaktor Mensch

Kevin D. Mitnick, William Simon

Mitnick führt den Leser in die Denk- und Handlungsweise des Social Engineering ein, beschreibt konkrete Betrugsszenarien und zeigt hervorragend die dramatischen Konsequenzen, die sich daraus ergeben. Dabei nimmt Mitnick sowohl die Perspektive des Angreifers als auch die des Opfers ein und zeigt damit sehr eindrucksvoll, wieso die Täuschung so erfolgreich war – und wie man sich effektiv dagegen schützen kann.

[5] Wireshark 101: Einführung in die Protokollanalyse

Laura Chappell

Dieses Buch richtet sich an angehende Netzwerkanalysten und bietet einen idealen Einstieg in das Thema, wenn Sie sich für die Analyse des Datenverkehrs interessieren – sei es, weil Sie verstehen wollen, wie ein bestimmtes Programm arbeitet, sei es, weil Sie die zu geringe Geschwindigkeit des Netzwerks beheben möchten, oder sei es, weil Sie feststellen wollen, ob ein Computer mit Schadsoftware verseucht ist.

[6] Hacking mit Metasploit: Das umfassende Handbuch zu Penetration Testing und Metasploit

Michael Messner

Messner hat mit seinem Werk »Hacking mit Metasploit« eines der wenigen deutschen Bücher im Bereich Metasploit veröffentlicht. In seinem Buch stellt er das Metasploit-Framework detailliert vor und zeigt anhand vieler Praxisbeispiele, wie man das Tool im Rahmen von Penetrationstests sinnvoll einsetzt.

[7] Social Engineering enttarnt: Sicherheitsrisiko Mensch

Christopher Hadnagy, Paul Ekman

Social Engineers sind Experten in der Manipulation ihres Gegenübers und wissen, mit welchen Mitteln sie ihr Ziel erreichen können. Mit diesem Buch werden Sie verstehen lernen, was jemand wirklich denkt, auch wenn er Sie etwas anderes glauben lassen möchte. Gleichzeitig lernen Sie, wie Sie Menschen durch Mimik und Gestik dazu bringen, Ihnen zu vertrauen.

# Stichwortverzeichnis


## Symbole

2,4-GHz-Frequenzbereich 17, 19, 22, 113, 144, 148, 183, 257, 417, 426, 427, 463
5-GHz-Frequenzbereich 19, 22, 112, 144, 148, 183, 257, 417, 426
60-GHz-Frequenzbereich 19
802.11 radio information 213
IEEE 802.1X 75

## A

Abwehrmaßnahmen 483
Access Point 34, 39, 135, 230
ACK 67
Acknowledgement Frames 227
Acknowledgement Frames (ACK) 62, 67
Acrylic Wi-Fi HeatMaps 146
Acrylic Wi-Fi Professional 206
Address Resolution Protocol (ARP) 274, 289, 338, 407
  ARP-Poisoning 395
  ARP-Replay-Angriff 271
  ARP-Requests 478
  ARP-Tabelle 409
Ad-hoc 23, 207, 427
Ad-hoc-Netzwerk 29, 37
Advanced Encryption Standard (AES) 70, 82, 86, 313, 429
AiCloud 106
AiDisk 106
airbase-ng 326
aircrack-ng 109, 289, 415
aircrack-ng-Suite 93
  airmon-ng 119
aircrack-Suite 120, 138
airdecap-ng 377
airmon-ng 211
airodump-ng 138, 140
airplay-ng 227
Aktives Scanning 136
ALFA AWUS036H 110
ALFA AWUS051NH 110
ALFA AWUS052NH 110
Aloha-Net 23
AndIodine 438
Android, WLAN-Passwort auslesen 244
Anerkennung 482
Angreifer 136
  Cyberkriminelle 481
  DAU 479
  Hacker 481
  IT-Professional 480
  Motive 479
  Normalanwender 480
  Poweruser 480
  Skriptkiddies 480
Angreifer-PC 93
Angreifer-STA 285
ANonce 316, 325, 328, 332, 381
AP 34
ARP 285
ARP-Anfragen 281
ARP-Paket 275

ARP-Poisoning 397
ARP-Replay-Attacke 277
ARP-Request 281
AS 35
ASCII 76, 83, 279, 314, 378
Association Frames 62
Association Request Frame 62, 65, 87
Association Response Frame 62, 65, 87
Audit 425, 431
Authentication 63, 87
Authentication Frame 62, 63
Authentication Request Flooding 238
Authentication Requests 196
Authentication Server 35, 53
Authentifizierungsarten 53
Authentizität 70

B
BackTrack 94
Basic Service Set 39
Basic Service Set Identifier 51
BBSID 51
Beacon 50, 52, 62, 87, 161, 490
Beacon Flooding 202, 239
Beacon Frame 62, 161
Beamforming 26
Betriebsarten 37
Bluetooth 22, 28, 427, 447
  Smartphone 29
Bootloader 475
Broadcast 51, 63
Broadcom-Chipsatz 300
Brute Force 170
BSS 39
BSS Id 212
BSSID 89
bully 311

C
Cafe Latte Attack 297
Captive Portal 433, 452
  Hacking 434
CA-Zertifikat 180
CCMP 80, 82
Challenge-Response-Verfahren 74
ChopChop 286
ChopChop-Angriff 271, 280
CISO 430
Clear to Send 62, 67, 230
Clients 135
Computersabotage 18
COMTEN 23
Control-Frames 66
Counter Mode Cipher Block Chaining
  Message Authentication Code Protocol
  82, 429
cowpatty 332
Cracking 333
CTS 67
CTS-Attacken 240
CTS-Frame-Attacke 229
Cyberkriminelle 481
Cypherpunks 71

D
Data-Frames 62, 67
Datenrate 20
DAU 479
DDoS-Attacken 82
DD-WRT 463
Deauthentication 64
Deauthentication Flooding 222, 227,
  228, 239, 364
Deauthentication Frame 62, 64
DECT 30, 107, 426
Destination Address 61
DHCP-Server 192
Dictionary-Angriff 170
Disassociation Attack 209, 228, 239
Disassociation Frame 62, 65, 212

Distribution System 36
dnsspoof 387
DNS-Spoofing 383, 398
DoS 202, 209, 222, 228, 229
DoS-Attacke 222
Drahtlose Datenübertragung, Probleme 21
DS 36
Dual Band 24
Dumpper 313

**E**

EAP 78
EAP-Failure 79
EAP-Request 79
EAP-Response 79
EAP-Success 79
Elektromagnetisches Spektrum 19
Elektromagnetische Welle 19
ESS 40
ESSID 51
Ethernet 36, 39, 89, 119, 125, 154, 235, 301
ettercap 215, 344, 354, 355, 387, 393, 407
Evil Twin 481
  Linset 358
Evil-Twin-Angriff 105, 356
EV-Zertifikat 353
Exploit 400
Extended Service Set 40
Extended Service Set Identifier 51
Extensible Authentication Protocol 78

**F**

Fake-AP 293, 344
FAKEDNS 367
FCS 59, 216
Fibre Channel 36
file.pcap 237
Firmware 478
  Router 455
Frame Body 61
Frame Check Sequence 59, 61, 212
Frame Control 60
Frame-Typ 60
Freetz 469
Freifunk 43, 454
Frequency Hopping 22
FRITZ!Box 7490 107
Furcht 482

**G**

Gargoyle 479
genpmk 331
George Antheil 22
Geräteklassifizierung 420
Geräte-Tracking 422
Gluon 107
Gluon-Firmware 457
GRUB 100

**H**

Hacker 481
Hackerparagraf 18
Hacking 16
Hashcat 333
Hedy Lamarr 22
hexeditor 233
Hidden SSID 165, 270
HiperLAN 30
Hirte Attack 292
HomeRF 30

**I**

IANA 385
IBSS 37
ICV 72
IEEE 19, 33, 36
  IEEE 802.1x 25
  IEEE 802.11-2007 25
  IEEE 802.11-2012 25
  IEEE 802.11d 25

IEEE 802.11e 25
IEEE 802.11f 25
IEEE 802.11h 25
IEEE 802.11i 25
IEEE 802.11p 25
IEEE 802.11r 25
IEEE 802.11s 25
IEEE 802.11w 25
IEEE 802.15.1 29
IEEE 802.15.4 29
IEEE 802.16 30
IEEE 802.11 23, 54, 71
IEEE 802.11-2007 53
IEEE 802.11a 23, 30
IEEE 802.11ad 27
IEEE 802.11ax 28
IEEE 802.11b 24
IEEE 802.11g 24
IEEE 802.11i 82
IEEE 802.11n 24
IEEE 802.11w 87, 239
IEEE 802.15.1 22
IEEE-Standards 55
ifconfig 262
Independent Basic Service Set 37
Informationsbeschaffung 135
Infrarot 30
Infrastrukturbetrieb 39
Integrität 70
Integrity Check Value 72
Interferenz 426
Breitband-Interferenz 426
Gesamtband-Interferenz 426
Schmalband-Interferenz 426
Internet Assigned Numbers Authority 385
iOS, WLAN-Passwort auslesen 246
IP-Adresse 192, 386
iptables 348
IT-Professional 480
IV-Kollision 272
iwlist 50, 162, 163, 199

**J**

John the Ripper 333

**K**

Kali Linux 94, 392, 445
KeePass 339

**L**

Langeweile 482
LEAP-Methode 80
LEDE 479
Li-Fi 30
Linset 358
Linux Live USB Creator 98
Linux, WLAN-Passwort auslesen 243
LLC 59
Logical Link Control 59

**M**

MAC-Adresse 51, 85, 89, 259
macchanger 262, 310
MAC-Filter 89, 259, 263, 265, 373
MAC-Header 59
MAC-Layer 58
MAC, Media Access Control 51
macOS, WLAN-Passwort auslesen 244
MAC-Spoofing 199, 227, 259, 263
Linux 262
Malformed Packets 409, 437
Malicious SSID 340
Management-Frames 62, 87
Man-in-the-Middle 395
Man-in-the-Middle-Angriff 344
Materielle Interessen 482
mdk3 171, 199, 268
mdk3-Secret Destruction Mode 308

Media Access Control, MAC 51
Mesh-Netzwerk 42, 454
Message Integrity Check 76
MetaGeek inSSIDer 141
Metasploit 106, 132, 404
Metasploit-Konsole 399
MIC 76
Michael 76
MIMO 24
Mirai-Botnetz 105
Monitoring-Modus 231
Monitormodus 118, 119, 139
Motiv
  Anerkennung 482
  Angreifer 481
  Furcht 482
  Langeweile 482
  materielle Interessen 482
  Neid 482
  Neugier 482
  Rache 482
  Spaß 482
MSI US54EX 110
MU-MIMO 26

**N**

Neid 482
NetCut 406
NetCut Defender 411
Network Address Translation 348
Netzwerke aufspüren 161
Netzwerkverkehr aufzeichnen 153
Neugier 482
nmap 132, 341
Normalanwender 480

**O**

oclHashcat 333
OPEN Auth 53
Open System Authentication 53
OpenWrt 107, 108, 459
Opfer-PC 105
Oracle VirtualBox 95
OSI-ISO-Schichtmodel 55

**P**

Packet Capture 180
PAM 344
Passives Scanning 136
Performanceanalyse 423
PHY 56
Physical Layer 55, 56
Physical Layer Convergence Procedure 57
Piconetz 29
Ping 220, 226
PIN-Methode 299
Pixie Dust 302
Pixie-Dust-Angriff 300
PLCP 57
PLCP-Header 59
PMF 88
Poweruser 480
Preamble 59
Priviledge Access Management 344
Probe Frames 62
Probe Request 63, 87
Probe Request Frame 62, 63
Probe Response 63, 87
Probe Response Frame 62, 63
Protected Management Frames 87, 239
Protokollanalyse 422
Protokollversion 60
Providerprivileg 453
Push-Button-Methode 299
PuTTY 132, 468
Pyrit 333

## R

Rache 482
RADIUS-Server 79
Ralink-Chipsatz 300
Raspberry Pi 156
RC4 71
Realtek-Chipsatz 300
Reassociation Request 87
Reassociation Request Frame 62, 65
Reassociation Response 87
Reassociation Response Frame 62, 65
Reaver 302, 304
Receiver 212
Receiver Address 61, 216, 232
Rechtsgrundlagen 17
Reichweite 20
Remote-Interface 156
Request to Send 62, 66, 230
Resource Allocation Attack 192
Roaming 40
Robust Secure Network 80
Rogue Access Point 341
Routerkeygen 257
RSN 80
RTS 66

## S

Scanning 135
  aktives 162
scp 158, 278
Security by Obscurity 71
Sensoren 416
Serpent 70
Service Set Identifier 46, 340
Shared Key Authentication 54
Signaturanalyse 420
Site Survey 146
Skriptkiddie 480
Slackware 102
SNonce 316
Social Engineering 94, 149, 371, 428
Source 212
Source Address 61
Spaß 482
Spatial Streams 24
Spektrumanalyse 423
SSID 46, 90, 164
  verborgene 164
SSID Cloaking 90
sslstrip 132, 344, 350
STA 34
Standardpasswörter 246
Station 34, 37, 39, 43, 50, 52, 54, 60, 63, 64, 65, 74, 76
Stock-Firmware 455
Störangriffe 183
Störerhaftung 452

## T

tcpdump 156, 180, 215, 265, 478
tcpreplay 219, 220
Temporal Key Integrity Protocol 76
TFTP 475
TKIP 76
Tomato 479
Topologien 37
TP-LINK TL-WN722N 110
Transmitter Address 61
Trivial File Transfer Protocol 475
TrueCrypt 100
Twofish 70

## U

USB-Creator 98
UTF-8-Zeichen 47

## V

VeraCrypt 100
Verborgene SSID 90
Verfügbarkeit 70

Verhaltensanalyse 421
Verschlüsselungsverfahren 84
Vertraulichkeit 69
Vier-Wege-Handshake 73, 83, 314, 315, 319, 324, 332, 363, 490
Virtuelle Maschine 95
VM 95
Vorschaltseiten 452

## W

WAP 34
WAPI 86
Wardriving 446
  Praxis 448
  rechtlich 452
Warwalk 452
wash 301
Wave-2-WLAN-Adapter 26
WDS 41
WEP 60, 71
  Angriffe 271
  Empfehlungen 299
WEP-Algorithmus 72
WEP-Schlüssel 72, 271
WIDS 137, 164, 415
WIDS-Server 419
Wi-Fi Alliance 85
Wi-Fi-Alternative 30
Wifi Analyzer 144
Wi-Fi-Jammer 188
WiFi Key Recovery 244
Wifiphisher 371
WiFi Pineapple 156, 157, 159, 206, 289, 318, 340
Wi-Fi Protected Access 75
Wi-Fi-Protected Setup 85
Wifislax 102, 138, 156, 247, 256, 303, 345, 358, 392
WiGig 27
WiMAX 30
Windows, WLAN-Passwort auslesen 241
WinSCP 158, 278, 291
WIPS 164
WIPS-Server 419
Wired Equivalent Privacy Protocol 71
Wireless Access Point 34
Wireless Distribution System 41
Wireless Gigabit 27
WirelessKeyView 243
Wireless Metropolitan Area Network 30
Wireless Network Interface Controller 33, 63, 183, 199, 200, 203, 220, 269, 292, 308, 417, 455
Wireless Personal Area Network 28
wireless-regdb 441
Wireless Transmission Message 58
Wireshark 154, 161, 208, 489, 491
Wirtschaftsspionage 344
WLAN 15, 19, 21, 28
  Geschichte 22
  Grundlagen 33
  IEEE 802.11 28
WLAN-Controller 37
WLAN-Frames 61
WLAN-Infrastruktur 33
WLAN-Jammer 187
WLAN-Karte 109
WLAN-Policy 430
WLAN-Repeater 41
WLAN-Router 105, 455
WLAN-Security-Audit 425, 431
WLAN-Security-Monitoring 415
WLAN-Sicherheit 483
WLAN-Sniffing 135
WLAN-Verkehr
  entschlüsseln 373
  mitschneiden 373
WMAN 28, 30
WNIC 33, 220, 292
WPA 75

WPA2 82
  WPA2 Enterprise 83
  WPA2 Personal 82
WPA Enterprise 78
WPAN 27, 28
WPA Personal 75
WPA-PSK 75
WPS 85
  Angriffe 299
WRAP 83
WRT3200ACM 107

**X**

X.509-Standard 86
XOR 76
XOR-Verknüpfung 71

**Z**

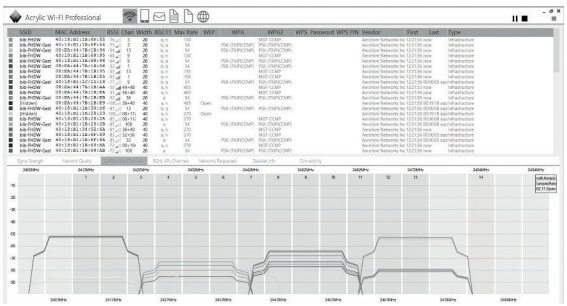
ZigBee 29
Z-Wave 29

Tim Philipp Schäfers / Rico Walde

# WLAN Hacking

**Drahtlose Netzwerke sind heute allgegenwärtig und werden im Zuge von Entwicklungen wie dem „Smart Home“ und dem „Internet of Things“ in Zukunft eine noch wichtigere Schlüsselrolle bei der Informationsvermittlung spielen. Folglich steht und fällt die Zuverlässigkeit unserer Infrastruktur nicht zuletzt mit der Sicherheit von WLAN-Technologien.**

Das Buch vermittelt seinen Leserinnen und Lesern das nötige Wissen, um WLAN-Umgebungen wirksam gegen Angriffe abzusichern. Zahlreiche praxisnahe Beispiele helfen sowohl Anfängern als auch Fortgeschrittenen dabei, verschiedene Angriffsszenarien nachzuvollziehen, um sich effektiv vor Hackern schützen zu können.



*Lernen Sie Experten-Tools wie Acrylic Wi-Fi Professional zum Erkunden von Netzwerkumgebungen kennen*

Vom Auskundschaften einer WLAN-Umgebung bis zur Umgehung von Authentifizierungsverfahren geben die Autoren einen umfassenden Einblick in alle gängigen Angriffswege auf drahtlose Datenübertragungstechnologien. Rechtliche und gesellschaftliche Aspekte wie Störerhaftung und Freifunk runden das Buch ab und machen es zu einem unverzichtbaren Lern- und Nachschlagewerk für alle, denen die Sicherheit ihrer Funknetze am Herzen liegt.

## Aus dem Inhalt:

- Basiswissen WLAN-Sicherheit: WEP, WPA(2) und WPS
- WLAN-Topologien: IBSS, BBS, ESS, WDS
- Operationen und Authentifizierungsarten
- Scanning-Methoden zur Informationsbeschaffung
- Tools für Sniffing und Analyse
- Angriffe auf physikalischer und auf Netzwerkebene
- Daten mitschneiden und entschlüsseln
- DoS durch Authentication Request Flooding
- WLAN-Authentifizierung umgehen
- Security Monitoring mit WIDS/WIPS
- WLAN-Security-Audits durchführen
- Wardriving in der Praxis
- Alternative Router-Firmware

## Über die Autoren:

**Tim Philipp Schäfers** ist bereits seit dem Abitur als Security Consultant tätig und berät Firmen im Bereich Informations- und Websicherheit. Er entlarvte gravierende Sicherheitslücken bei IT-Größen wie Google, Facebook, PayPal, der Deutschen Telekom und vielen weiteren Unternehmen. Er ist Mitgründer des Projektes Internetwache.org und freier Autor zu den Themen IT-Sicherheit und -Privatsphäre.

**Rico Walde** arbeitet seit 2013 als selbstständiger IT-Consultant und studiert Wirtschaftsinformatik an der FHDW Paderborn. Zudem hält er Vorträge im Bereich der IT-Security und ist als Freifunker aktiv. Er ist zertifiziert als Offensive Security Wireless Professional (OSWP) und bloggt zusammen mit Tim Philipp Schäfers unter **www.wlan-hacking.de** über aktuelle Themen im Bereich WLAN-Security.

9 783645 605236

**40,– EUR** [D]
ISBN 978-3-645-60523-6

Besuchen Sie
unsere Website
**www.franzis.de**

FRANZIS