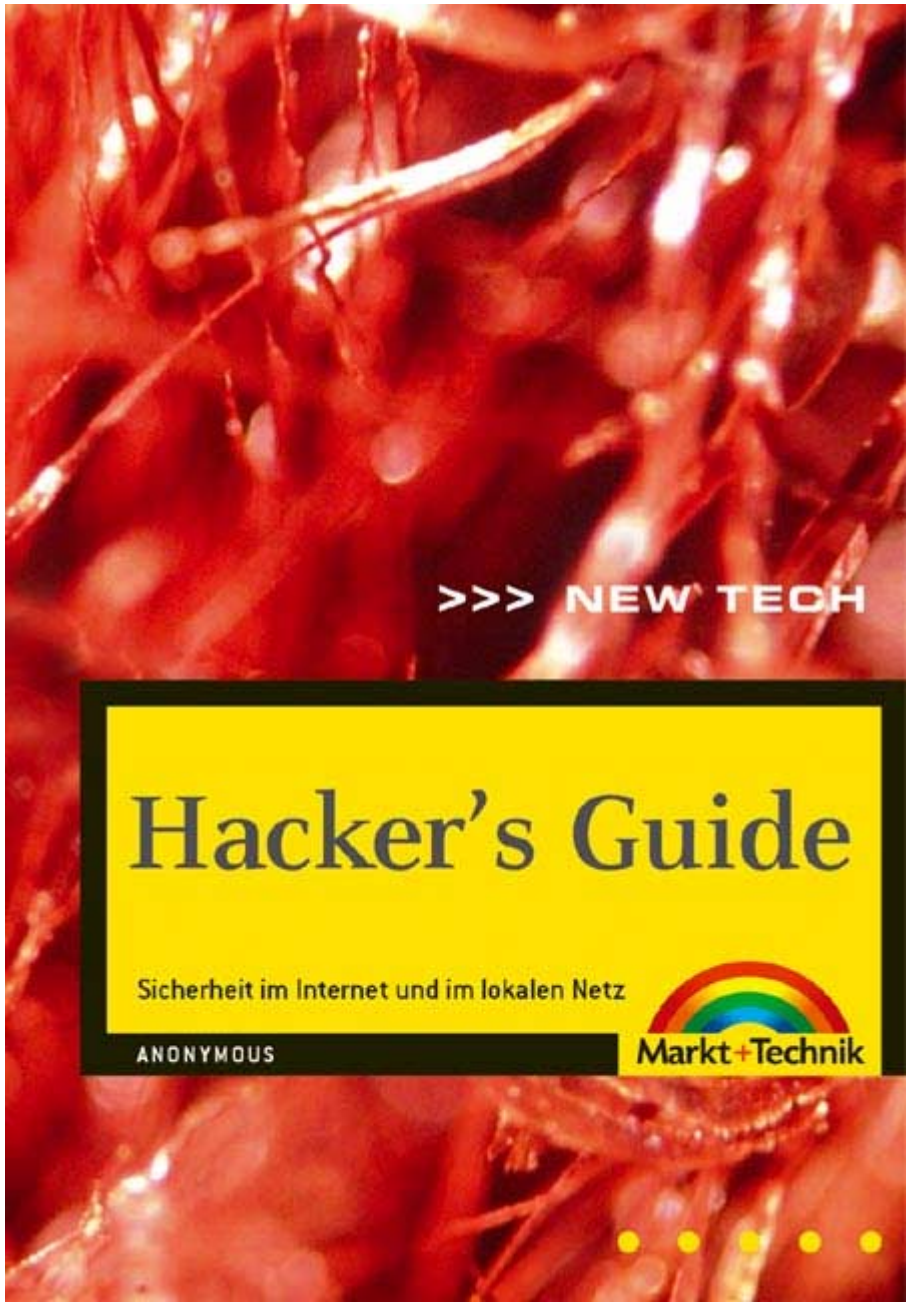
Hacker’s Guide

Anonymous



Kapitel 27
Sicherheit in Funknetzen

»Es ist Freitagnacht – heute passiert's … nachdem wir uns getroffen haben, stehlen wir uns fort in die Dunkelheit, und die Kälte der Nacht geißelt uns mit Urgewalt. Heute fegen wir über Dallas hinweg.

Wir hocken zusammengedrängt in einem aufgemotzten Geländewagen, mit Armaturenbrett aus Ebenholz und getönten Fenstern, der mit seinem bizarren Aufbau aus hochragenden Antennen aussieht wie ein riesiges Insekt. Wir kriechen durch den Telecom Corridor von Richardson[1], unsere Gesichter totenblass im Schein des Laptops. Es beginnt unversehens – die Schutzmauern der Netzwerke um uns herum schmelzen wie Eis. Innerhalb von wenigen Sekunden stehen uns die größten Netzwerke offen. Nortel mit seinen 28 Access-Points: ein Scheunentor. Wir fahren ein bisschen weiter, unsere Antenne beginnt zu summen. Fujitsu, Ericsson, Alcatel … Hunderte ungesicherter Portale stürzen wie ein Wasserfall auf dem Display unseres Laptops hinunter. Einige wenige sind verschlüsselt – aber nur schwach –, die meisten aber sind noch nicht einmal durch ein Kennwort geschützt. Und wir wissen: Das alles gehört jetzt uns. Wir sind Riesen, erheben uns haushoch über all diesen Türmen aus Stahl und Glas, und wie Götter schauen wir hinab auf sie mit Hohn und Spott. Und dann treten wir ein…«

– Aus dem Windows .NET Server Security Handbook

Die WLAN-Technologie (Wireless LAN, Funk-LAN) und die Internetsicherheit sind nach Angaben eines führenden Datensicherheitsmagazins zwei Technologiefelder mit exzellenten Wachstumsraten. Beide Bereiche haben sich allerdings völlig getrennt voneinander entwickelt (bzw. einander ignoriert), und als sie schließlich miteinander kollidierten, waren die Folgen fatal. Deswegen werden wir in diesem Kapitel die WLAN-Technologie unter dem Gesichtspunkt Sicherheit betrachten. Wir werden insbesondere auf das Phänomen des War-Drivings eingehen. Dieser Begriff beschreibt den Einbruch in Funknetze mithilfe mobiler Geräte. Angesichts der explosionsartigen Ausbreitung von Funknetzen und der hohen Wahrscheinlichkeit, dass diese den traditionellen Internetprovidern möglicherweise bald die Herrschaft streitig machen werden, wird offensichtlich, warum dieses Thema von entscheidender Bedeutung ist.

1. Anmerkung des Übersetzers: Der Begriff »Telecom Corridor« bezeichnet die nördlichen Vororte von Dallas im amerikanischen Bundesstaat Texas, zu denen auch die Städte Richardson und Plano zählen. Hier haben zahlreiche Telekommunikationsunternehmen wie Nortel, Alcatel und Ericsson Ihre amerikanischen Firmensitze.

Dieses Kapitel soll eher praktischer Natur sein. Ich werde Ihnen zeigen, wie Sie bei der Auswahl Ihrer Hardware vorgehen, ein Testfeld einrichten und mit der Überwachung Ihres Funknetzes beginnen. Ferner soll kurz darauf eingegangen werden, wie man den WEP-Algorithmus (Wired Equivalent Privacy) knackt, der Bestandteil des Standards 802.11 für Funk-LANs ist.

Die hier vorgestellten Informationen sind oft Prüfungsstoff für das WSEC (Wireless Security Expert Certification, Zertifizierung zum Sicherheitsexperten für Funknetze) wieder. Die WSEC-Prüfung ist die schwierigste, aber auch anerkannteste (und Respekt gebietendste) Prüfung zur Sicherheit in Funknetzen weltweit. Deswegen kann das hier vorgestellte Material zur Vorbereitung auf diese Prüfung sehr hilfreich sein. Informationen über diese Zertifizierung finden sie unter `http://www.cwne.com/cwsp/index.html`.

HINWEIS

Ähnlich wie beim MSCE (Microsoft Certified Systems Engineer) von Microsoft gibt es im Bereich der Funknetze unterschiedliche Stufen der Ausbildung und Zertifizierung:

- CWNA (Certified Wireless Network Administrator)
- CWSP (Certified Wireless Security Professional)
- CWNI (Certified Wireless Network Integrator)
- CWNE (Certified Wireless Networking Expert)

Weitere Informationen finden Sie unter `http://www.cwne.com/`.

In den folgenden Abschnitten widmen wir uns zunächst den empfehlenswertesten Hardwarekomponenten, die in einem typischen Funk-LAN eingesetzt werden, also Access-Points, WLAN-Karten, Antennen und PDAs. Anschließend wird das War-Driving aus der Sicht anerkannter Experten beschrieben.

Noch eine letzte Bemerkung, bevor wir anfangen: Beachten Sie, dass alle in diesem Kapitel vorgestellten Programme kostenlos im Internet zu haben sind und zum Rüstzeug von Crackern und kriminellen Elementen gehören. Ich fasse diese Informationen hier lediglich zusammen, damit der rechtschaffene Administrator zumindest eine Chance hat, sein Netzwerk zu schützen. Suchen Sie also die notwendigen Gerätschaften heraus, und fangen Sie an, Ihr Netzwerk zu überprüfen, bevor es von jemand anderem angezapft wird, der nichts Gutes im Schilde führt!

27.1 WLAN-Topologie

Die Topologie eines WLANs unterscheidet sich von der traditioneller, leitungsgestützter Ethernetnetze – wenn auch nicht allzu sehr. Die Voraussetzungen für WLANs ähneln denen ihrer verkabelten Ebenbilder, weisen aber ein paar kleinere Abweichungen auf. Fangen wir mit den Peer-Funknetzen an.

Peer-Netzwerke werden meistens in kleinerem Rahmen eingesetzt, d.h. in Umgebungen, in denen nur wenige Clients relativ nah beieinander existieren. Diese Art von Netzwerk lässt sich durchaus mit einem P2P-Netzwerk (Peer-to-Peer-Netzwerk) vergleichen, bei dem es keinen zentralen Verwaltungspunkt gibt und alle Clients bei der Kommunikation miteinander auf sich gestellt sind. In einer Peer-Topologie kommunizieren die Clients direkt mit anderen Clients, d.h. ohne Vermittlungsstellen (diesen Modus nennt man auch Ad-hoc-Modus). Diese Art von WLAN wird häufig als Alternative zu Infrarotverbindungen eingesetzt, wenn zwei Leute Dateien zwischen zwei Systemen austauschen wollen, oder wenn lediglich eine sehr kleine Gruppe von Leuten kostengünstig vernetzt werden soll.

Größere Unternehmensumgebungen benötigen zusätzlich eine zentrale Steuereinrichtung und Funktionalitäten zur effizienteren Verwaltung von Clients. All dies ermöglicht eine Infrastrukturtopologie. Wenn Funkclients in den Infrastrukturmodus versetzt werden, dann suchen sie nach einem als Access-Point (Zugangspunkt) bezeichneten Gerät, das sie zum Versand von Daten an andere vernetzte Clients benutzen. Sie können einen Access-Point in etwa mit einem Hub im leitungsgestützten Netzwerk vergleichen. Der Access-Point empfängt wie der Hub Daten von mehreren Clients, dient aber gleichzeitig als Gateway, das den WLAN-Clients den Zugriff auf das zugrunde liegende Festnetzwerk gestattet. Dies funktioniert auch umgekehrt, d. h., Access-Points ermöglichen den Zugriff vom leitungsgestützten Netzwerk auf das Funknetz. Es gibt sogar einige Access-Points, die eine erweiterte Funktionalität bieten, z.B. NAT oder einfache Paketfilter.

Ein Access-Point ist normalerweise ein statisches Gerät. Da sich mobile Geräte wie z.B. Laptops frei bewegen können, kommt es häufig vor, dass eine solche mobile Station den Sendebereich (die Zelle) ihres Access-Points verlässt und sich in einer anderen Zelle anmelden muss. Der im Folgenden Beschriebene Prozess läuft natürlich auch ab, wenn sich ein mobiles Gerät erstmalig anmeldet.

Jede Zelle und jeder Access-Point besitzen eine eindeutige Adressierung, wobei die Adresse des Access-Points mit der Adresse der zu verwalteten Zelle übereinstimmt. Über diese Adressierung kann sich nun ein mobiles Gerät eindeutig einer Zelle zuordnen. Da jedoch das Gerät keinen Überblick über die in Reichweite befindlichen Gegenstellen hat, muss ein Scanning durchgeführt werden. Es gibt sowohl passives als auch aktives Scanning. Beim erstgenannten Verfahren werden sogenannte Beacon-Frames von einem Access Point ausgesendet. Anhand dieser kann eine mobile Station feststellen, wie viele und welche Access-Points in Reichweite sind. Die Signalstärke ist dabei ein Gradmesser der Erreichbarkeit.

Eine weitere Möglichkeit stellt das aktive Scanning dar, bei der das mobile Gerät selber Beacon-Frames versendet. Empfängt in diesem Fall ein Access-Point solche Frames, so übermittelt er an den Sender eine Antwort. Aus allen empfangenen Antworten kann dann die günstigste Gegenstelle ausgewählt werden. Um nun endgültig der Zelle beizutreten, muss sich das Gerät bei dem betreffenden Access-Point anmelden. Dies geschieht mit sogenannten Manage-

ment-Frames. Das Gerät kann verständlicherweise jedoch nur in einer Zelle registriert sein. Erhält das mobile Gerät nun eine bessere Verbindung zu einem anderen Access-Point, so kann es sich in der bisherigen Zelle durch ein Management-Frame ab- und in der neuen anmelden. Auf diese Weise ist ein Wechsel der Zellen problemlos möglich.

Hat sich der Client nun authentifiziert – und wurde er vom Access-Point autorisiert –, dann entspricht die resultierende Verbindung exakt einer Ethernetverbindung in einem Festnetzwerk. Sofern keine anderen Beschränkungen implementiert wurden, stehen den Funkclients nun alle Möglichkeiten offen, die ihnen auch über eine Kabelverbindung geboten würden.

Eine Infrastrukturtopologie bedingt nicht unbedingt das Vorhandensein einer Verbindung zu einem größeren Festnetzwerk; vielmehr wird diese Art der Topologie durchaus häufig eingesetzt, um mehreren Clients in einem Funknetz ohne leitungsgestützte Geräte den Zugriff auf gemeinsame Ressourcen zu ermöglichen.

Funknetze im Infrastrukturmodus können praktisch überall in die reguläre Netzwerktopologie eines Unternehmens eingefügt werden. Es ist allerdings zu beachten, dass Clients im Peer-Modus keine Möglichkeit zum Zugriff auf die Ressourcen des zugrunde liegenden Festnetzes haben, sofern keine weiteren Routing-Geräte implementiert sind. Ferner ist zu beachten, dass Clients im Peer-Modus physisch relativ nah beieinander sein müssen, während Clients im Infrastrukturmodus nur durch die Beschränkungen des Fest- oder Funknetzes gebunden sind, zu dem sie gehören.

Wenn Sie Funknetze analysieren (oder ein Hacker mit Verantwortungsbewusstsein sind), dann erleichtert eine gute Antenne Ihre Aufgabe erheblich. Man unterscheidet hier zwei grundlegende Typen:

- **Omnidirektionale Antennen.** Diese Antennen haben einen Sende- und Empfangswinkel von 360°. Sie sind in Fällen nützlich, in denen die Übertragung innerhalb eines relativ großen Gebietes möglich sein soll oder generell eine sehr große Betriebsreichweite gefordert ist. Entgegen landläufiger Meinung bieten echte omnidirektionale Antennen keinen Leistungsgewinn. Die meisten Antennen, die als omnidirektionale Antennen verkauft werden, sind nicht in der Lage, in alle Richtungen Funkwellen zu senden. Aufgrund ihres Aufbaus senkt eine solche Antenne das Signal auf der Y-Achse vollständig ab und konzentriert ihre Sendeleistung auf der X-Achse.
- **Richtantennen.** Diese auch als direktional bezeichneten Antennen fokussieren die Funkfrequenzenergie in eine bestimmte Richtung. Der Unterschied ähnelt dem zwischen einer Glühbirne und einer Taschenlampe: Während die omnidirektionale Antenne ihre Signale – wie die Glühbirne ihr Licht – in alle Richtungen abstrahlt –, bündelt die Richtantenne – wie eine Taschenlampe – ihre Energie in eine bestimmte Richtung. Richtantennen sind nützlich bei der Einrichtung von P2P-Funknetzen oder in anderen Fällen, in denen Sie das abgestrahlte Signal in eine exakte Richtung führen wollen.

In den folgenden Abschnitten werde ich Ihnen WLAN-Hardware zeigen, die ich persönlich empfehle. Die Ergebnisse basieren auf Tests, die für das Buch »Maximum Wireless Security« (SAMS, 2002) durchgeführt wurden. Wenden wir uns zunächst den Access-Points zu, die ein wesentliches Element von WLANs bilden.

27.2 Access-Points

Es gibt viele verschiedene Hersteller von Access-Points, und all ihre Erzeugnisse bieten mehr oder minder die gleiche Funktionalität an. Bezüglich der Produktsicherheit und -merkmale jedoch gibt es wesentliche Unterschiede zwischen den einzelnen Anbietern. Einige Access-Points können beispielsweise Verbindungsanfragen basierend auf der MAC-Adresse (d.h. anhand der eindeutigen Produktkennung der WLAN-Netzwerkkarte) abweisen, andere wieder sind in der Lage, Beacon-Frames abzuschalten, um den Access-Point für Crackerprogramme unsichtbar zu machen. Zum Glück werden solche erweiterten Sicherheitsmerkmale immer mehr zum Standard auch für Access-Points, die zum Einsatz in SOHO-Umgebungen vorgesehen sind. Allerdings gibt es inzwischen auch Programme, die an die veränderten Bedingungen angepasst wurden und sich die nötigen Informationen auf anderen Wegen (beispielsweise aus abgehörtem Netzwerkverkehr mit einer schon in der Zelle registrierten Station) besorgen.

In unserer Feldstudie im Jahr 2002, in der wir mehr als 1.300 Access-Points in fünf Städten untersuchten, stand Cisco mit 39,7% aller eingesetzten Geräte quantitativ an der Spitze. Es folgten Lucent mit 19,2% und Linksys mit 17,1%; die verbleibenden 24% teilten sich diverse andere Hersteller. Interessant war die Tatsache, dass die Access-Points von Linksys, die eigentlich für SOHO-Umgebungen konzipiert sind, mit erstaunlicher Geschwindigkeit Eingang in den Bereich der Unternehmen finden. Dies könnte an ihrem niedrigen Preis, ihrer hohen Verfügbarkeit, der Implementierung einer MAC-basierten Verbindungsabweisung und ihrer Fähigkeit liegen festzustellen, ob eine Netzwerkkarte Broadcasts versendet. Da die – teureren – Access-Points von Cisco allerdings nach wie vor in der Mehrheit sind, können wir davon ausgehen, dass den Kunden der Aufbau und die Erweiterung interner Firmenfunknetze gutes Geld wert sind.

Die folgenden Abschnitte beschreiben Access-Points, die ich aus eigener Erfahrung guten Gewissens empfehlen kann. Bevor Sie sich allerdings für ein Gerät entscheiden, sollten Sie im Internet nach aktuellen Sicherheitslücken suchen, die Ihr Wunschgerät betreffen, und Erkundigungen darüber einziehen, ob der Hersteller für solche Sicherheitslücken Softwareupdates anbietet. Als Beispiel für solche Verwundbarkeiten von Access-Points sei ein Exploit genannt, der im November 2002 von SecurityFocus.com veröffentlicht wurde. Mit Hilfe dieses Exploits war es möglich, das Administratorkennwort und den WEP-Schlüssel für die verschlüsselte Datenübertragung einer ganzen Reihe von Access-Points in Erfahrung zu bringen.

HINWEIS

Genaueres über diesen Exploit können Sie unter http://online.securityfocus.com/archive/1/298432 und http://www.heise.de/newsticker/data/ea-08.11.02-000/ nachlesen.

27.2.1 Linksys WAP11

URL: http://www.linksys.com

Der WAP11 von Linksys ist ein kostengünstiger Access-Point mit guter Leistung. Ein früherer Erfolg war ihm aufgrund fehlender Sicherheitsmerkmale verwehrt, aber dieses Problem wurde mittlerweile gelöst: Ab Firmwareversion 1.4i.1 verfügt das Gerät über mehrere neue Funktionen beispielsweise zur Deaktivierung von Beacons und zur Beschränkung von Verbindungen, die auf der MAC-Adresse des Clients basiert.

Die Administration des WAP11 erfolgt mithilfe einer clientbasierten Software über die USB-Schnittstelle oder – via SNMP – über eine leitungsbasierte Ethernetverbindung. Als ich beim Support von Linksys anfragte, warum die Merkmale nicht über beide Schnittstellen konfigurierbar seien, erhielt ich keine zufrieden stellende Antwort; man teilte mir lediglich mit, dass sich das auch in Zukunft nicht ändern werde. Nichtsdestoweniger sind die Navigation und Konfiguration über die Administrationsoberfläche in beiden Fällen die reine Freude.

Der WAP11 bietet zwei Antennen, die als Sende- bzw. Empfangsantenne konfiguriert werden können. Standardmäßig ist der Access-Point so eingestellt, dass über beide Antennen sowohl empfangen als auch gesendet wird. Dank der Konfigurationsmöglichkeiten für die beiden Antennen lässt sich der WAP11 optimal in praktisch jede Betriebsumgebung integrieren. Die Antennen sind über Standardanschlüsse mit dem Gerät verbunden, d. h., die serienmäßigen Antennen lassen sich bei Bedarf durch Drittanbieterantennen mit anderem Gewinnwert ersetzen. Dies kann beispielsweise nützlich sein, wenn man die Betriebsreichweite auf einen bestimmten Bereich beschränken oder die Richtcharakteristik ändern will. Weitere Informationen zu diesem Thema finden Sie in Abschnitt 27.3, »Antennen«.

Technische Daten

- SSID (Vorgabe): Linksys
- IP-Adresse (Vorgabe): 192.168.1.250
- Kanal (Vorgabe): 6
- Verschlüsselung: 40/128 Bits, WEP-kompatibel
- Clients: 32
- Abmessungen (B × H × T): 12,7 × 22,6 × 4,1 cm
- Gewicht: ca. 340 g

27.2.2 NetGear ME102

URL: `http://www.netgear.com`

Der ME102 von NetGear ist ein Access-Point mit umfassender Funktionalität und sehr geringen Abmessungen; es handelt sich beim ME102 um eines der kleinsten Geräte auf dem Markt, d. h., er ist ideal für den Einsatz unterwegs oder in sehr beengten Umgebungen. Lassen Sie sich aber von der Größe nicht täuschen: Mit dem Firmware-Upgrade 1.4h3 unterstützt der ME102 eine WEP-Verschlüsselung mit 128 Bit, P2P- und P2MP-Konfigurationen und erweiterte Clientfunktionalitäten mit MAC-Filterung.

Die Administration des ME102 erfolgt mithilfe einer clientbasierten Software über die USB-Schnittstelle oder – via SNMP – über eine leitungsbasierte Ethernetverbindung. Um die MAC-Filterung aufrufen und konfigurieren zu können, müssen Sie die SNMP-Schnittstelle verwenden. Ebenfalls über SNMP ist eine Statistikseite verfügbar, die verschiedene Statistiken zu den einzelnen Funk- und Ethernetschnittstellen am Access-Point anzeigt. Ein weiteres nützliches Merkmal des ME102 ist die Möglichkeit, mehrere Kennwörter für die Administrationsoberfläche zu konfigurieren. Auf diese Weise kann ein Administrator den Benutzern erlauben, die Konfigurationen des Access-Points zu überprüfen, ohne sein eigenes Kennwort preisgeben zu müssen. Wenn Sie als einfacher Benutzer angemeldet sind, können Sie sich alle Konfigurationen anzeigen lassen, jedoch keine Veränderungen vornehmen.

In mehreren Tests hat der ME102 meine Erwartungen bezüglich Funktionalität und Einsatzfähigkeit mehr als übertroffen. Es handelt sich hierbei um einen sehr leistungsfähigen Access-Point, der für viele Situationen die perfekte Lösung ist. Er spielt zwar nicht in einer Liga mit den Access-Points der Industrieklasse, aber Sie erhalten hier für Ihr Geld wahrlich einen tollen Gegenwert.

Technische Daten

- SSID (Vorgabe): Wireless
- IP-Adresse (Vorgabe): 192.168.0.5
- Kanal (Vorgabe): 6
- Verschlüsselung: 40/128 Bits, WEP-kompatibel
- Clients: 32
- Abmessungen (B × H × T): 14,2 × 16,3 × 2,8 cm
- Gewicht: ca. 35 g

27.3 Antennen

Fast jeder Mensch nutzt täglich die eine oder andere Antenne. Auch Sie werden, ob Sie es merken oder nicht, in Ihrem täglichen Leben für viele Zwecke Antennen verwenden. Einrichtungen wie beispielsweise Automatiktüren, Satellitenfernsehen, Pager, Funktelefone und Funknetze benötigen Antennen. Und

doch wissen nur sehr wenige Benutzer dieser Antennen, wie und warum diese funktionieren. Werfen wir also einen kurzen Blick auf die Technologie, die den Einsatz von Antennen möglich macht, und beantworten wir die Frage, was Antennen in Hochfrequenznetzwerken (d.h. Funknetzen) zu suchen haben.

Antennen sind zunächst einmal nur Erweiterungen eines Funkempfängers oder -senders. Ein von einem Funkgerät (Radio etc.) erzeugtes Signal wird an die Antenne weitergeleitet und von dort durch den Raum gesendet. Dieses Signal wird dann von einer anderen Antenne aufgefangen und an eine andere Funkeinrichtung weitergeleitet. Das erzeugte und übertragene Signal wird in Hertz (Hz) gemessen, einer Maßeinheit, die die Anzahl der Signalzyklen pro Sekunde angibt. Verständlicher formulieren kann man dies als die Zeit, die eine Funkwelle benötigt, um einen vollständigen Zyklus zu durchlaufen.

Stellen Sie sich einmal vor, Sie würden eine Spiralfeder auf eine ebene Fläche stellen und ein Ende am Boden befestigen. Wenn Sie die Feder nun anstupsen, beginnt sich diese zu bewegen – Sie erzeugen Wellen. Diese Wellen ähneln der Hochfrequenzenergie, die durch den Raum übertragen wird. Wenn Sie Ihre Hand langsam von einer Seite zur anderen und wieder zurück bewegen, dann erzeugen Sie Wellen mit niedriger Frequenz; beschleunigen Sie diese Bewegung, so erzeugen Sie kürzere Wellen, die aber häufiger auftreten: Sie haben die Frequenz erhöht. Tieffrequente Wellen können große Distanzen überwinden, sind aber sehr anfällig für Störungen, die durch blockierende Objekte (Häuser, Bäume usw.) erzeugt werden. Hochfrequente Wellen hingegen können Gebäude und andere Hindernisse besser durchdringen, aber ihre Reichweite ist beschränkt.

Nehmen wir beispielsweise einmal Ihren regionalen UKW-Sender. Wenn dieser sein Signal auf 103,5 MHz sendet, dann bedeutet dies, dass eine Welle mit 103.500.000 Zyklen pro Sekunde übertragen wird. Diese Ultrakurzwelle ist in der ganzen Region – auch im Innern von Gebäuden – in guter Qualität hörbar. Ein Mittelwellensender hingegen, der vielleicht 200 Kilometer entfernt auf einer Wellenlänge von 1.320 kHz (d.h. 1.320.000 Zyklen pro Sekunde) sendet, kann mit einer Außenantenne zwar noch in brauchbarer Qualität empfangen werden, aber dafür muss die Antenne korrekt ausgerichtet sein.

Antennen sind wesentliche Komponenten der Übertragung von Hochfrequenzen. In vielen Fällen ist die Übertragungsqualität eines schwachen Signals, das über eine gute Antenne gesendet wird, besser als die Qualität eines starken Signals, das mit einer schlechten Antenne übertragen wird.

Antennen werden nach ihrem Gewinn klassifiziert. Unter dem Gewinn (auch Verstärkung genannt) versteht man den durch Verwendung einer Richtantenne erzielbaren Leistungsanstieg. Der Gesamtgewinn wird mit einer Isotropantenne verglichen. Eine solche Antenne ist hypothetisch, weil sie in der realen Welt nicht vorkommt; trotzdem ist sie die allgemein anerkannte Referenz.

Eine Dipolantenne mit 0 dBd (»Dezibel über Dipol«) hat einen Gewinn von 2,14 dB weniger als eine Isotropantenne mit 0 dBi (»Dezibel über Isotropenstrahler«); wird der Gewinn also in dBd statt dBi angegeben, so sind zu diesem Wert 2,15 dB hinzuzuaddieren, um den dBi-Gewinn zu erhalten. Wird der

Gewinn einer Antenne nur in dB angegeben, so müssen Sie sich beim Hersteller erkundigen, ob dBi oder dBd gemeint sind; kann er Ihnen das nicht sagen (oder weiß er es nicht einmal), dann sollten Sie sich das Geld sparen und sich an jemanden wenden, der sich damit auskennt.

Wie bereits erwähnt wurde, werden für die meisten Antennen dBi-Werte angegeben. Dies ist aber nicht der einzige Faktor, der bei der Bewertung der Gesamtleistung eine Rolle spielt. Beispielsweise muss auch die Leistung der Antenne beachtet werden. Die meisten 802.11b-kompatiblen Funknetzkarten senden mit einer Leistung von 32 mW. Wenn Sie einen Blick auf die Umwandlungstabelle (siehe Tabelle 27.1) werfen, dann stellen Sie fest, dass 32 mW einem Wert von 15 dBm entsprechen. Der dBm-Wert wird anhand der folgenden Formel berechnet:

$$dBm = 10 \log (32\ mW \div 1)$$

dBm	Sendeleistung	dBm	Sendeleistung
53	200 W	25	320 mW
50	100 W	24	250 mW
49	80 W	23	200 mW
48	64 W	22	160 mW
47	50 W	21	125 mW
46	40 W	20	100 mW
45	32 W	19	80 mW
44	25 W	18	64 mW
43	20 W	17	50 mW
42	16 W	16	40 mW
41	12,5 W	15	32 mW
40	10 W	14	25 mW
39	8 W	13	20 mW
38	6,4 W	12	16 mW
37	5 W	11	12,5 mW
36	4,0 W	10	10 mW
35	3,2 W	9	8 mW
34	2,5 W	8	6,4 mW
33	2 W	7	5 mW
32	1,6 W	6	4 mW
31	1,25 W	5	3,2 mW
30	1,0 W	4	2,5 mW
29	800 mW	3	2,0 mW

Tabelle 27.1: Tabelle zur Konvertierung von dBm in Leistung

dBm	Sendeleistung	dBm	Sendeleistung
28	640 mW	2	1,6 mW
27	500 mW	1	1,25 mW
26	400 mW	0	1,0 mW

Tabelle 27.1: Tabelle zur Konvertierung von dBm in Leistung (Forts.)

Warum sind diese Zahlen wichtig? Nun, Sie erlauben die Berechnung der EIRP (Effective Isotropic Radiated Power, kürzer auch ERP, Effective Radiated Power). EIRP ist die Leistung, die von der Antenne tatsächlich gesendet wird, und dieser Wert ist zur Berechnung der Effizienz eines Antennensystems wichtig.

Wenn Sie eine typische Funknetzkarte haben, die mit 15 dBm sendet, und beispielsweise eine 3-dBi-Antenne verwenden wollen, dann können Sie die EIRP mit folgender Formel berechnen:

15 dBm + 3 dBi = 18 dBm (64mW) EIRP

In den Vereinigten Staaten begrenzt die FCC[2] mobile 802.11-kompatible Stationen auf eine Sendeleistung von 1 W (30 dBm EIRP). Feststationen dürfen diese Einschränkung in gewissen Grenzen überschreiten. Bei der Berechnung des Wertes für Feststationen muss für jede 3 dB, die der Antennengewinn um mehr als 6 dB überschritten wird, ein dB abgezogen werden. Das folgende Beispiel demonstriert dies für einen WAP11-Access-Point von Linksys und eine Antenne mit 24 dBi:

20 dBm + 24 dBi = 44 dBm = 25 W
(44 dBm – ((24 dBi – 6 dB) ÷ 3)) = EIRP
(44 dBm – (18 dBi ÷ 3)) = EIRP
(44 dBm – 6 dBi) = EIRP
EIRP – 38 dBm (6,4W)

Neben Gewinn und Sendeleistung sollten Sie auch ein Auge auf die Größenunterschiede von Antennen haben. Es stehen abhängig von Frequenz und Antennentyp verschiedene Größen zur Auswahl. Die Antennengröße steht dabei in direktem Zusammenhang mit der Sendefrequenz. Ein CB-Funkgerät etwa, das in einem Kraftfahrzeug installiert ist, operiert in einem Band zwischen 26,965 MHz (Kanal 1) und 27,405 MHz (Kanal 40). Wenn Sie eine Antenne mit voller Wellenlänge für Kanal 1 wünschen, müsste diese 11,13 m lang sein. Dieser Wert berechnet sich wie folgt:

L (in m) = 300 ÷ f (in MHz)
L = 300 ÷ 26,965MHz
L ˜ 11,13 m

2. Die FFC (Federal Communication Commision) ist eine US-Bundesbehörde, die Richtlinien für Kommunikationsgeräte und anderes elektronisches Equipment entwickelt.

Vergleichen wir nun die Länge dieser CB-Antenne mit der einer entsprechenden Antenne, über die ein (amerikanischer) Polizist mit seiner Einsatzstelle kommuniziert; die Wellenlänge beträgt in diesem Fall 460,175 MHz:

L (in m) = 300 ÷ f (in MHz)
L = 300 ÷ 460,175 MHz
L ˜ 65 cm

Wie man sehen kann, beträgt der Unterschied zwischen diesen beiden Antennen knapp zehneinhalb Meter. Zum Glück operieren 802.11b-Funknetze im Frequenzbereich von 2,4 GHz (2.400 MHz), d. h., die Antennen sind sehr kurz:

L (in m) = 300 ÷ f (in MHz)
L = 300 ÷ 2400 MHz
L ˜ 13 cm

Im folgenden Abschnitt werden Antennen beschrieben, die für Sie nützlich sein können, wenn Sie ein Funknetz aufbauen oder überwachen. Ich habe diese Antennen selbst eingesetzt und getestet und kann sie Ihnen wirklich ans Herz legen.

27.3.1 HyperLink HG2415Y

URL: `http://www.hyperlinktech.com`

Bei der HG2415Y handelt es sich um eine hochwertige Yagi-Antenne mit sehr hoher Leistungsfähigkeit (eine Yagi-Antenne ist eine spezielle Richtantenne, die gleichzeitig in zwei Richtungen abstrahlen, um Funkkontakt mit zwei unterschiedlichen Bezugsstationen aufnehmen zu können). Die Antenne wiegt etwa 820 Gramm, ist also sehr leicht und gut zu installieren. Sie wird komplett mit zwei Bügelschraubenhalterungen ausgeliefert, mit denen sie an einem Antennenmast mit einem Durchmesser von bis zu 6 cm befestigt werden kann.

Das Anschlusskabel der Antenne ist ca. 60 cm lang, unterschiedliche Anschlussstecker sind lieferbar. Ich habe die Antenne an eine ORiNOCO-Karte (PCMCIA) angeschlossen. Erste Tests zeigten, dass ich mithilfe dieser Antenne eine Verbindung mit dem Access-Point aus einer Entfernung herstellen konnte, die *dreimal* so groß war wie die Reichweite der mit dem Access-Point mitgelieferten Antennen.

Diese Antenne eignet sich hervorragend für Peer-Verbindungen, und sie ist ausgesprochen widerstandsfähig. Sie ist für Windgeschwindigkeiten von mehr als 200 km/h ausgelegt, bringt also auch unter extremen Bedingungen ihre Leistung. Diese Antenne ist meine persönliche Empfehlung und sollte auch bei Ihnen die erste Wahl sein.

Technische Daten

- Bandbereich: 2.400…2.500 MHz
- Gewinn: 14,5 dBi

- Öffnungswinkel (–3 dB): 30°
- Impedanz: 50 Ohm
- Eingangsleistung (max.): 50 W
- Stehwellenverhältnis: <1,5:1 (typ.)
- Gewicht: ca. 820 g
- Abmessungen (L × Ø): 48,2 × 7,62 cm
- Polarisierung: vertikal
- Windgeschwindigkeit (max.): > 240 km/h

HINWEIS

Der Begriff »Stehwellenverhältnis« beschreibt das Verhältnis der Abstrahlleistung (Leistung, die tatsächlich in die Antenne gelangt) zur Rückstrahlleistung (Leistung, die an das Funkgerät zurückgestrahlt wird).

27.3.2 HyperLink HG2419G

URL: `http://www.hyperlinktech.com`

Auch die HG2419G ist ein Hochleistungsgerät. Diese Antenne mit exzellenten Gewinnwerten ist extrem effizient und hervorragend gefertigt. Sie besteht aus haltbarem, galvanisierten und geschweißten Stahl, der mit einer hellgrauen UV-resistenten Pulverbeschichtung versehen ist, was die Antenne nicht nur robust macht, sondern ihr Äußeres auch ansprechend gestaltet.

HyperLink stellt drei Versionen dieser Antenne vor: eine mit 15 dBi Gewinn, eine mit 19 dBi Gewinn (die ich für dieses Buch getestet habe) und den Urvater dieser beiden, ein Modell mit 24 dBi. Diese Antenne bietet nicht nur viel Gewinn, sondern arbeitet auch ausgesprochen trennscharf. Der Öffnungswinkel von 8° beim 24-dBi-Modell unterdrückt Störungen effizient und maximiert gleichzeitig die Leistung. Wie die meisten Richtantennen eignet sich auch diese Antenne am besten für Peer-Verbindungen, die mehrere Netzwerke aneinander anbinden. Bei meinen Tests mit der HG2419G konnte ich auch mit dieser Antenne die Reichweite im Vergleich zum unverstärkten Signal am Access-Point mit seinen werksseitig ausgelieferten Antennen um den Faktor 3 vergrößern.

Die HG2419G kann an einen Standardmast mit einem Durchmesser von bis zu 6,35 cm montiert werden, und der Neigungswinkel beträgt maximal 15°. Diese Eigenschaften erlauben den Einsatz der Antenne in einer Vielzahl von Szenarien und macht sie ideal für die Dachmontage. Dank der wahlweise horizontal oder vertikal einstellbaren Polarisierung, der hohen Gewinnwerte, des schmalen Öffnungswinkels und der robusten Konstruktion ist diese Antenne eine der besten auf dem Markt.

Technische Daten

- Bandbereich: 2.400…2.500 MHz
- Gewinn: 19 dBi
- Öffnungswinkel (–3 dB): 17°
- Impedanz: 50 Ohm
- Eingangsleistung (max.): 50 W
- Stehwellenverhältnis: <1.5:1 (typ.)
- Gewicht: 1,77 kg.
- Abmessungen (L × Ø): 42,42 × 59,94 cm
- Polarisierung: vertikal oder horizontal
- Windgeschwindigkeit (max.): > 240 km/h

27.3.3 Signull SMISMCO10

URL: `http://www.signull.com`

Die SMISMCO10 ist eine omnidirektionale Antenne, die für Mehrpunktanwendungen mit mittelgroßen bis großen Reichweiten gedacht ist. Noch nicht einmal einen Meter hoch und leichter als ein halbes Kilo, bringt diese Antenne für ihre Größe eine beträchtliche Leistungsfähigkeit mit.

Signull bietet drei Varianten dieser Antenne an: eine 10-dBi-Version (die ich für dieses Kapitel getestet habe), eine Version mit 8 dBi und eine mit 5 dBi. All diese Antennen eignen sich hervorragend zur Reichweitenvergrößerung von Access-Points oder Knoten im Firmenfunknetz. Sie lassen sich im Innenbereich problemlos montieren und bieten genug Reichweite beispielsweise für einen Landwirtschaftsbetrieb oder eine Lagerhalle (z.B. zur Anbindung funkgestützter Inventurgeräte). Auch die Außenmontage ist möglich, z.B. in Innenhöfen oder auf Parkplätzen.

Beim Test der SMISMCO10 stellte ich fest, dass sie tatsächlich die von Signull versprochene Leistung brachte. Dank ihrer robusten Konstruktion, ihres geringen Gewichts und der überlegenen Performance ist die SMISMCO10 eine nützliche Ergänzung Ihres Funknetzes.

Technische Daten

- Bandbereich: 2.400…2.500 MHz
- Gewinn: 10 dBi
- Öffnungswinkel: 360°
- Impedanz: 50 Ohm
- Eingangsleistung (max.): 50 W
- Stehwellenverhältnis: <1,5:1 (typ.).
- Gewicht: 340 g

- Abmessungen (B × H): 2,22 × 96,52 cm
- Polarisierung: vertikal
- Windgeschwindigkeit (max.): > 160 km/h

27.3.4 Signull SMISMCY12

URL: `http://www.signull.com`

Auch diese Yagi-Zirkularantenne von Signull gehört zu meinen Favoriten. Neben den hervorragenden Leistungswerten weist sie ein wahrhaft stilvolles Design auf. Außerdem können Sie den internen Aufbau der Antenne betrachten, da das Gehäuse durchsichtig ist; Sie können sie also auch zu Demonstrationszwecken benutzen.

Signull bietet auch diese Antenne in drei Varianten an: mit 8 dBi, 12 dBi (das getestete Modell) und 15 dBi. Die 12-dBi-Antenne scheint einen ordentlichen Leistungsschub zu bringen, aber je nach Anwendung können Sie mit der 15-dBi-Version noch besser fahren. Im Verlauf unserer Tests konnte ich, wenn ich diese Antenne auf unseren Access-Point richtete, eine drastische Erhöhung der Signalstärke feststellen.

Das gefällige Äußere der Antenne mit dem transparenten Gehäuse ist aber möglicherweise gleichzeitig auch einer der Nachteile dieses Modells, denn wie es mit seiner Wetterfestigkeit aussieht, konnte ich nicht in Erfahrung bringen. Im Zweifelsfall sollte man sie deswegen eher im Gebäudeinnern oder unter einem Schutzdach montieren. Glücklicherweise aber wirkt sich das ansprechende Design nicht negativ auf die Leistung dieser Antenne aus. Und die SMISMCY12 *ist* leistungsfähig. Sie ist eine gute Wahl zur Erstellung und Anbindung von Funknetzen, und Sie sollten sie auf jeden Fall einmal antesten.

Technische Daten

- Bandbereich: 2.400…2.500 MHz
- Gewinn: 12 dBi
- Öffnungswinkel (–3 dB): 30°
- Impedanz: 50 Ohm
- Eingangsleistung (max.): 50 W
- Stehwellenverhältnis: <1.5:1 (typ.)
- Abmessungen (B × H): 10,16 × 58,42 cm
- Gewicht: ca. 900 g
- Polarisierung: vertikal und horizontal
- Windgeschwindigkeit (max.): >160 km/h

27.3.5 TechnoLab Log Periodic

URL: `http://www.technolab-inc.com`

Die Yagi-Antenne von TechnoLab ist wirklich einmalig. Das niedrige Profil und die geringen Abmessungen prädestinieren sie geradezu für den Einsatz im Gebäudeinnern. Durch Montage an den Außenwänden können Sie außerdem ganz einfach Gebäudeverbindungen herstellen.

Tests offenbarten, dass diese kleine Antenne wirklich gute Arbeit leistet. Ich schloss sie direkt an unseren Test-Access-Point an und versuchte, über eine PCMCIA-Standardkarte (ORiNOCO) eine Verbindung herzustellen. Dabei stellte ich eine gute Trennschärfe und eine auffällige Verbesserung der Signalstärke in der gewünschten Richtung fest.

Ich habe den Access-Point dann auch mit einer Kombination getestet, die aus einer mitgelieferten Antenne und der TechnoLab-Antenne bestand, und habe keinen Leistungsabfall festgestellt. Dies ist wichtig, denn es gibt eine Menge Beispiele für Access-Points, die eine Anbindung nicht nur für Remotebenutzer, sondern auch für das lokale Netzwerk realisieren müssen. Nicht nur ihre geringen Abmessungen und das niedrige Gewicht, sondern auch der breite Bandbereich prädestiniert diese Antenne auch für andere Anwendungen zusätzlich zur Funknetztechnik. Zusammenfassend betrachtet, kann man der Yagi-Antenne von TechnoLab bescheinigen, eine nützliche Antenne zu sein, die Funk- oder Campusnetze hervorragend ergänzt.

Technische Daten

- Bandbereich: 900…2.600 MHz
- Gewinn: 12 dBi
- Öffnungswinkel (–3 dB): 30°
- Impedanz: 50 Ohm
- Eingangsleistung (max.): 10 W
- Stehwellenverhältnis: < 2:1 (typ.)
- Gewicht: 816 g
- Windgeschwindigkeit (max.): keine Angaben

27.4 Funknetzkarten

Funknetzkarten sind zwar einfache, aber doch wesentliche Komponenten der WLAN-Hardware. In diesem Abschnitt werde ich lediglich die ORiNOCO-Karten beschreiben, da diese den Produkten aller anderen Hersteller zum Zeitpunkt unserer Untersuchungen um ein Vielfaches überlegen waren.

27.4.1 ORiNOCO-Karten

URL: http://www.orinocowireless.com

Keine Widerrede: Die ORiNOCO-Funknetzkarten von Proxim sind mit Abstand das Beste, was man für Geld kaufen kann. Die PCMCIA-Karten benötigen einen Steckplatz am Laptop oder einem anderen tragbaren Computer. Es werden zwei Modelle angeboten, nämlich die ORiNOCO Silver und die ORiNOCO Gold. Die Silver-Ausführung bietet WEP-Verschlüsselung mit 64 Bits, die Gold-Variante gleiches mit 128 Bits. Beide Karten bieten Verbindungsraten von bis zu 11 Mbit/s und sind WiFi-kompatibel. Eines der besten Merkmale beider Karten ist die Möglichkeit, eine externe Antenne anzuschließen. Das ist zwar nicht einmalig, aber bei anderen Herstellern doch eher die Ausnahme und bei der WLAN-Überwachung und der Netzwerkverwaltung schnell unentbehrlich. Ferner werden die ORiNOCO-Karten von vielen Betriebssystemen unterstützt, z.B. von Mac OS, Novell, Windows und Linux.

HINWEIS

IEEE802.11b ist der WLAN-Standard der die größte Marktverbreitung gefunden hat; er wird fälschlicherweise oft unter dem Begriff »WiFi« (Wireless Fidelity) vermarktet. Es handelt sich bei WiFi jedoch um ein Warenzeichen, das der Verbreitung der WLAN-Geräte deshalb sehr förderlich ist, weil dieses von der WLANA (Wireless LAN Alliance) vergebene Gütesiegel eine weit reichende Interoperabilität der Geräte über Herstellergrenzen hinweg garantiert. Weitere Informationen finden zur WLANA finden Sie unter http://www.wlana.com

Die Karten können so konfiguriert werden, dass sie wahlweise im Peer- oder im Infrastrukturmodus arbeiten. Der Peer-Modus erlaubt Ihnen die Bildung eines kleinen Netzwerks, in dem die Karten kommunizieren können, ohne dass ein Access-Point vorhanden sein muss. Im Infrastrukturmodus hingegen integriert sich die Karte in große Firmennetze, die zur Weiterleitung von Daten in ein leitungsgestütztes Netzwerk Access-Points verwenden.

Wenn Sie die Anschaffung einer Funknetzkarte in Betracht ziehen, dann sind die beiden Versionen der ORiNOCO-Karten die erste Wahl. Ihre robuste Konstruktion, die Anschlussmöglichkeit für eine externe Antenne und die Unterstützung mehrere Betriebssysteme sind Faktoren, die sie zu der von mir empfohlenen Lösung gemacht haben.

27.5 PDAs

PDAs (Personal Digital Assistants), die auch als Handheld-Geräte bezeichnet werden, haben im Laufe der letzten Zeit rapide an Beliebtheit gewonnen. Mit dem verstärkten Einsatz von PDAs ist auch eine gesteigerte Nachfrage nach der Anbindung an WLANs – und damit nach der Überwachung und Administra-

tion solcher Netzwerke – aufgetreten. Betrachten Sie die Vorteile: Sie können z.B. überall in Ihrem Haus oder Bürokomplex Ihre E-Mails abrufen, indem Sie einfach ein paar Icons mit dem Stift anklicken – und ohne den Zeit raubenden Rechnerstart abwarten zu müssen.

Viele Unternehmen entwickeln bereits hochwertige Produktionsanwendungen für den PDA-Markt. PocketPC beispielsweise (der auf Microsofts integriertes Betriebssystem Windows CE basiert) wird mit dem Microsoft Terminal Server Client ausgeliefert, über den Sie Verbindungen mit Servern praktisch überall in Ihrem Netzwerk herstellen können. Medizinstudenten in den Staaten verwenden heute schon an WLANs angeschlossene PDAs, um Operationen als Streaming-Video zu beobachten. Das Wachstumspotenzial dieses Marktes ist gewaltig.

Traditionell gibt es auf dem Markt für PDA-Betriebssysteme zwei große Anbieter, nämlich Palm mit seinem Palm OS und das Windows CE-basierte PocketPC. Zu dem Zeitpunkt, als dieses Buch geschrieben wurde, gab es von Palm in Bezug auf 802-11b-kompatible Konnektivität noch nicht viel zu vermelden; ganz anders von PocketPC, das exorbitante Möglichkeiten an den Tag legte. Viele Hersteller entwickeln PocketPC-Treiber für ihre Hardware und erweitern auf diese Weise die Fähigkeiten eines bereits sehr funktionellen Produkts. Wie auch bei Desktop- und Laptopcomputern gibt es viele Hardwaremodelle, die PocketPC unterstützen bzw. darunter laufen. Jedes Gerät ist anders und bietet eigene Merkmale und Vorteile. Unterstützung von erweitertem Speicher, hochauflösende Displays oder die Möglichkeit, externe Hardware (wie beispielsweise PCMCIA- oder Compact Flash-Karten) zu verwenden, sind Faktoren, die man bei der Kaufentscheidung berücksichtigen sollte.

Ein Gerät, das diese Aufgaben meiner Ansicht nach besser erfüllt als andere, ist der Compaq iPAQ. Wenn es um die Anbindung an Funknetze und zugehörige Merkmale geht, ist der iPAQ unbestritten der Klassenbeste unter den PDAs. Unternehmen wie ORiNOCO, Network Associates und Cisco setzen bei eigenen Entwicklungen ganz massiv auf den iPAQ als Marktführer im Bereich der Funkkommunikation. Anbieter entwickeln Softwareanwendungen speziell für den iPAQ und seine Fähigkeit, eine Vielzahl externer Hardwaregeräte zu unterstützen.

Auch wenn PDAs nicht so leistungsfähig sind wie ihre großen Brüder, die Desktoprechner, so stellen sie doch eine nützliche Ergänzung für ein Heim- oder Firmennetzwerk dar. Wenn sich die 802.11b-kompatiblen Netzwerke durchgesetzt haben und der Öffentlichkeit kostenlose Netzwerke zur Verfügung stehen, werden Handheld-Geräte unter den Gelegenheitsnutzern allgegenwärtig sein. Außerdem wird auch von einem rapiden Anstieg der Zahl von Heimarbeitern ausgegangen, die mithilfe von PDAs über VPNs mit ihren Firmen kommunizieren.

27.5.1 Compaq iPAQ

URL: `http://www.compaq.de/produkte/handheld/`

Der iPAQ von Compaq ist das derzeit beste Handheld-Gerät mit Funknetzunterstützung, das man bekommen kann. Er ist seiner Konkurrenz derart überlegen, dass ich in diesem Kapitel keinen anderen PDA beschreiben, geschweige denn empfehlen will.

Zwar ist die Basiseinheit bereits vorzüglich, aber Sie können sie durch so genannte Expansion Packs ergänzen. Die auch Sleeves genannten Expansion Packs erweitern die Gesamtfunktionalität des iPAQ. Es gibt viele verschiedene Packs, die den Anschluss unterschiedlichster Hardware – von PCMCIA- und Compact Flash-Karten bis hin zu IBM Microdrives und GPS-Diensten (Global Positioning System, System zur Positionsbestimmung) – ermöglichen. Durch das Aufsetzen eines Sleeves können Sie aus dem iPAQ eine Funknetzworkstation machen; da viele Geräte den PCMCIA-Standard unterstützen, ist das entsprechende Sleeve das wahrscheinlich empfehlenswerteste.

Der iPAQ kann mit einem Funknetzwerk verbunden werden, wenn das PCMCIA-Sleeve montiert und eine Funknetzwerkkarte in das Sleeve eingesteckt ist. Diese Konfiguration ermöglicht es Ihnen, eine Verbindung mit verschiedenen 802.11b-Netzwerken herzustellen und auf eine Reihe von Funktionen zuzugreifen. Dazu gehören der Besuch von Websites (mit der integrierten Version des Internet Explorers) oder die Administration Ihres Remotenetzwerks (über die Terminal Server-Anwendung). Wenn Sie Software wie etwa NetForce von Ruksun oder CENiffer von Epiphan Consulting aufspielen, können Sie die Gesamtfunktionalität und den Nutzen des Geräts erheblich erweitern. Andere Softwarefirmen wie NetStumbler oder Network Associates bieten diverse iPAQ-fähige Produkte an. Dank der wachsenden Anzahl von Hardware- und Softwareerweiterungen und der zunehmenden Verfügbarkeit von Funknetzwerken wird der iPAQ in Zukunft eine dominierende Rolle spielen.

Technische Daten

- Betriebssystem: PocketPC 2002
- Prozessor: Intel StrongArm RISC-Prozessor, 206 MHz, 32 Bit
- Arbeitsspeicher: 32 oder 64 MB
- Display: TFT-LCD, 4.096 Farben
- Auflösung: 240 × 320
- Spannungsversorgung: Lithium-Polymer-Akku, 950 mAh
- Gewicht: ca. 190 g
- Abmessungen (B × H × T): 8,33 × 12,98 × 1,58 cm

27.6 Ein Testfeld für ein Funknetz einrichten

Bevor Sie in Ihrem Unternehmen WLAN-Geräte in Betrieb nehmen, sollten Sie ein Testfeld erstellen und die gewünschte Konfiguration dort ausgiebig prüfen. Testfelder werden auch von WLAN-Experten für die Forschung und Entwicklung benötigt. Ein WLAN-Testfeld unterscheidet sich erheblich von einem gewöhnlichen Computertestfeld, denn es kann nicht räumlich begrenzt werden; vielmehr muss es mobil sein, denn auch seine Benutzer werden mobil sein.

Bei der Aufstellung des Access-Points in Ihrer Umgebung sind verschiedene Faktoren zu beachten. Hierzu gehören:

- **Reichweite.** Wie können Sie die Reichweite optimieren, ohne dass andere Access-Points beeinträchtigt werden?
- **Montage.** Wie wird der Access-Point installiert?
- **Netzwerkverbindung.** Wie wird Ihr Access-Point an das Netzwerk angebunden? Diese Frage kann sich auch auf Ihre Topologie und Ihre Sicherheitskonfiguration auswirken.
- **Spannungsversorgung.** Dies klingt zwar nicht wie ein wesentlicher Faktor, kann aber doch gewaltige Probleme verursachen.

Die Überprüfung der Reichweiten und die Entscheidungen über die Aufstellungsorte können ein wenig schwierig sein, weil es eben etwas unpraktisch ist, einen Access-Point andauernd in einer anderen Zimmerecke an die Decke zu dübeln. Zum Glück gibt es eine bessere Lösung. Besorgen Sie sich einen Handkarren (wie man ihn beispielsweise in Bibliotheken findet), und montieren Sie auf einer Seite einen Teleskopstab. An der Spitze des Teleskoparms befestigen Sie ein flaches Holzbrett oder Stück Plastik (kein Metall!), das groß genug ist, um den Access-Point wie an der Decke zu befestigen. Versetzen Sie das Brett so, dass der Access-Point herunterhängen kann, ohne mit dem Wagen ins Gehege zu kommen. Nun montieren Sie den Access-Point umgedreht auf das Holz- oder Plastikteil. Fahren Sie den Teleskoparm aus, bis er fast in Deckenhöhe ist. Durch Bewegung des Wagens können Sie nun auch den Access-Point hin und her bewegen.

Platzieren Sie eine an einen Wechselrichter angeschlossene Batterie auf dem Wagen, die als Spannungsquelle für den Access-Point dient. Mit einem Laptop oder einem PDA können Sie nun die Verbindung zum Access-Point von verschiedenen Punkten aus prüfen. Ich empfehle ferner, nicht nur im gewünschten Reichweitenbereich zu testen, sondern auch in angrenzenden Bereichen. Auf diese Weise können Sie feststellen, wo die Reichweite eventuell zu groß ist und ungewollt über den gewünschten Bereich hinausgeht.

Am besten erstellen Sie eine Testfeldkonfiguration, die sich möglichst stark an Ihrer Produktionsumgebung orientiert. Außerdem sollte das Testfeld flexibel genug sein, um die Überprüfung neuer Produkte zu ermöglichen und zukünftige Erweiterungen des Netzwerks zu simulieren. Ist das Testfeld fertig eingerichtet, dann können Sie Sicherheitsmaßnahmen zunächst dort testen. Im folgenden Abschnitt werden Ihnen Angriffe gegen WLANs aus der Sicht des

Hackers präsentiert. Mit dem dort vermittelten Wissen können Sie als WLAN-Administrator Ihre eigenen Netzwerke »angreifen«, bevor dies jemand anderes tut.

27.7 Angriffe gegen Funknetze

Die Methoden, die zum Angriff gegen Funknetze eingesetzt werden, sind nicht neu. Tatsächlich basieren sie – von wenigen Unterschieden abgesehen – auf den gleichen Angriffsmethoden, die seit Urzeiten gegen leitungsbasierte Netzwerke eingesetzt wurden. Das Ziel eines Angriffs auf ein Funknetz besteht meist nicht darin, das Funknetz selbst zu knacken, sondern einen Fuß in das dahinter liegende leitungsbasierte Netzwerk zu bekommen.

Nach 30 Jahren kontinuierlicher Angriffshistorie gibt es für traditionelle Festnetzwerke natürlich inzwischen einige durchaus beeindruckende Verteidigungsanlagen. Eine gut konfigurierte Firewall beispielsweise kann die Sicherheit erheblich verbessern. Sie sollten sich allerdings einmal überlegen, was mit einem ungesicherten Access-Point ist, der sich auf der *Innenseite* der Firewall befindet: Sie haben hiermit eine Hintertür durch die Firewall geöffnet. Aus diesem Grund hat die Verbreitung der WLANs den Bereich der Datensicherheit um mehr als zehn Jahre zurückgeworfen (manche würden sogar sagen, bis in die Achtzigerjahre, als Computersysteme Angriffen über Modems oder War-Dialing ungeschützt ausgesetzt waren).

Früher oder später fallen die meisten Funknetze zumindest einer Angriffsform zum Opfer. Diese Angriffe sind auch nicht auf die Unternehmenswelt beschränkt. Funknetze werden *sehr* häufig auch von Privatkunden verwendet, die meist nach einer Möglichkeit suchen, ihre Breitbandverbindung überall im Haus nutzen zu können. Schlimmer noch: Die überwiegende Mehrheit dieser Kunden macht sich über Sicherheitsfragen keinerlei Gedanken. Sie können zwar Access-Points für weniger als 200 € im Computergeschäft um die Ecke bekommen, aber diese weisen natürlich nicht die gleichen Sicherheitsfunktionen auf wie die Unternehmens- oder Profimodelle, für die man 800 € oder mehr bezahlt. Je mehr Benutzer diese preiswerten Access-Points in Heim- oder kleinen Unternehmensnetzwerken einsetzen, desto stärker steigt die Anzahl potenzieller Ziele – derzeit sogar exponentiell.

Es gibt viele verschiedene Modelle 802.11b-kompatibler Funknetzwerkkarten. Ein Aspekt, der ihnen allen gemeinsam ist, ist die Fähigkeit, Infrastruktur- und Peer-Modi zu konfigurieren. Der Infrastrukturmodus ist nach IEEE-Definition ein BSS (Basic Service Set) und dient dazu, einen Client mit einem Access-Point in einem vorhandenen Netzwerk zu verbinden (siehe Abbildung 27.1). Der Peer-Modus hingegen wird als IBSS (Independent Basic Service Set) bezeichnet; dieser Modus wird zur Verbindung zweier oder mehrerer Funknetzeinrichtungen zwecks Bildung eines kleinen Netzwerks ähnlich der P2P-Technologie bei leitungsgestützten Netzwerken verwendet (siehe Abbildung 27.2).

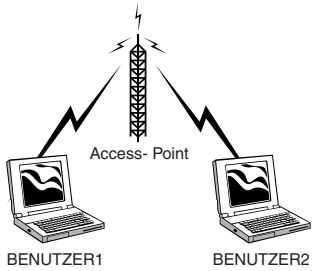


Abbildung 27.1: Übliche Konfiguration im Infrastrukturmodus

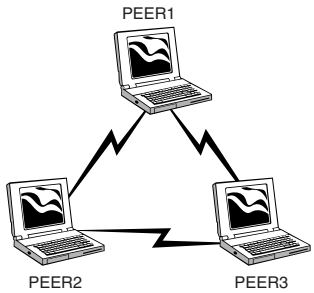


Abbildung 27.2: Übliche Konfiguration im Peer-Modus (Ad-hoc-Modus)

Einer der wesentlichen Nachteile dieses Funknetztyps ist die Tatsache, dass keine zentralen Sicherheitsmechanismen implementiert werden können; im Gegenteil, das vorhandene Maß an Sicherheit ist sehr niedrig. Das größte Problem bei der Ausführung eines Angriffs auf diese Art von Netzwerk ist, dass man ein solches Netzwerk finden muss. Der Betrieb eines solchen Netzes ist informell, d.h. diese Netze tauchen über Nacht auf und sind tags darauf schon wieder verschwunden. Beispiele für solche Netzwerke finden sich auf Kongressen und in Internetcafés, aber auch bei der gemeinsamen Nutzung einer Internetverbindung durch mehrere Benutzer.

27.7.1 Lauschangriff

Es gibt mehrere Ansätze zum Aufspüren eines Funknetzwerks. Die einfachste Methode ist der Lauschangriff. Sie können den Lauschangriff spontan starten, denn er erfordert weder spezielle Hardware noch besondere Vorbereitungen. Und was das Wichtigste ist: Er ist, wenn überhaupt, nur schwer zu erkennen.

Was beinhaltet der Lauschangriff? Nun, Sie beobachten einfach Ihre Umgebung. Und das geht so: Immer, wenn Sie an einen Ort gelangen – egal ob Sie zum ersten oder zum tausendsten Mal dort sind –, sperren Sie die Augen auf und suchen nach Anzeichen von Funknetzgeräten. Dass dort letzte Woche keine derartigen Geräte vorhanden waren, bedeutet nicht, dass sie nicht gestern oder heute dort angebracht wurden. Tabelle 27.2 bietet Reconnaissance-Vorschläge für Funknetze.

Wonach man schauen muss …	… und wo man schauen muss
Antennen	Mauern, Decken, Gänge, Dächer, Fenster
Access-Points	Decken, Mauern, Stützträger, Vorsprünge
Netzwerkkabel	verlaufen an Wänden oder die Decke entlang
neu installierte Unterbauten	Wände, Gänge und Stützträger
Geräte (Sicherheits-Scanner, PDAs usw.)	Mitarbeiter, Empfangs- oder Sicherheitsbereich

Tabelle 27.2: Reconnaissance bei Funknetzen

Das mag alles recht uninspiriert klingen, ist aber immer noch eine sehr effiziente Methode. In manchen Fällen können Sie sogar herausfinden, welches Access-Point-Modell verwendet wird, denn viele Unternehmen stellen ihre Geräte nicht sichtgeschützt auf. Sie können außerdem mit Mitarbeitern reden, die WLAN-Geräte verwenden, und ein paar einfache Fragen zu diesen Geräten stellen. Wahrscheinlich können diese Leute Ihnen nur wenige nützliche Informationen geben, aber sie können zumindest das Vorhandensein eines Funknetzes bestätigen. Gehen Sie bei der Befragung von Mitarbeitern vorsichtig vor, denn schließlich wollen Sie nicht in den Verdacht geraten, einen Angriff zu planen.

ACHTUNG

Auch wenn Sie eine legitime Sicherheitsüberprüfung im eigenen Netzwerk vornehmen, benötigen Sie zuvor eine schriftliche Genehmigung der Unternehmensführung. Ferner sind alle anwendbaren Gesetze und Vorschriften zu beachten.

Während eines Lauschangriffs haben wir beispielsweise die folgenden Bilder aufgenommen:

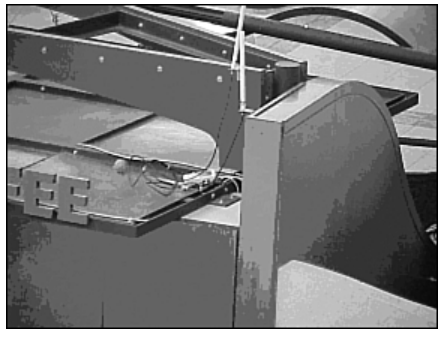


Abbildung 27.3: Bei einem Lauschangriff entdeckte Antenne und Access-Point



Abbildung 27.4: Bei einem Lauschangriff aufgespürte Antennen

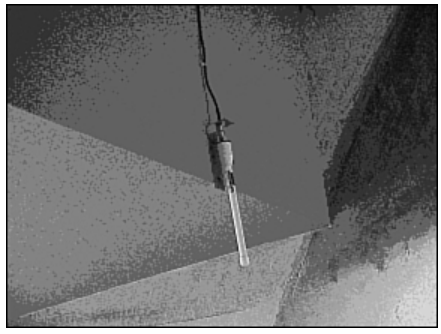


Abbildung 27.5: Noch eine Antenne, die wir bei einem Lauschangriff gesehen haben

Die Abbildungen 27.3 bis 27.5 wurden in einer Filiale einer in ganz Amerika tätigen Cafékette aufgenommen. In Abbildung 27.3 sind zwei Antennen und der Access-Point klar zu erkennen, Abbildung 27.4 und Abbildung 27.5 zeigen an zwei unterschiedlichen Orten installierte Antennen. Diesen Bildern können wir aufgrund unserer Erfahrung entnehmen, dass eine omnidirektionale Antenne mit einem Gewinn von etwa 8 dBi zum Einsatz kommt.

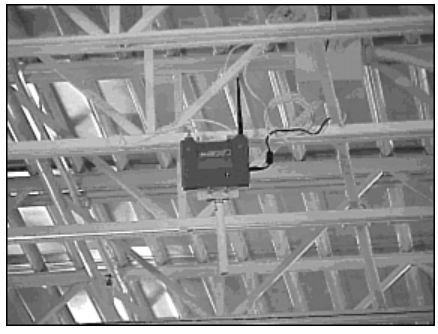


Abbildung 27.6: Bei einem Lauschangriff entdeckter Access-Point

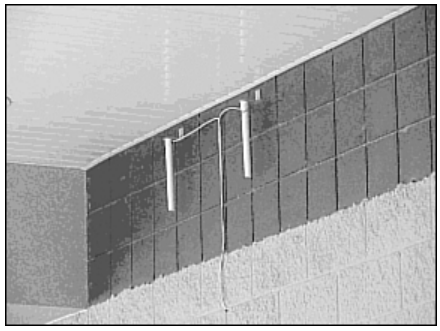


Abbildung 27.7: Bei einem Lauschangriff erspähte Antennen

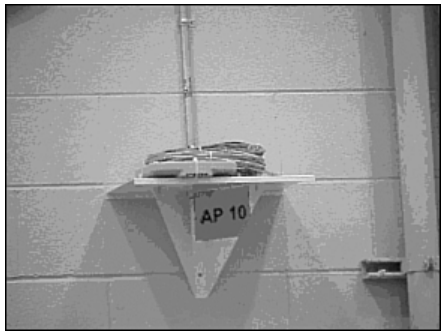


Abbildung 27.8: Bei einem Lauschangriff entdeckter Access-Point

Abbildung 27.6 haben wir in einer Filiale einer Billigschuhkette aufgenommen. Die gezeigte Konfiguration findet man in ähnlicher Form in allen Niederlassungen dieser Kette. Auf dem Bild sind sowohl der Access-Point als auch die beiden Antennen klar zu erkennen. In diesem Fall hat man offensichtlich beschlossen, nur eine 8-dBi-Antenne zu installieren und die andere direkt am Access-Point zu belassen.

Die beiden nächsten Abbildungen wurden in einem Kaufhaus aufgenommen. Abbildung 27.7 zeigt Außenantennen, die an den in Abbildung 27.8 gezeigten, innen montierten Access-Point angeschlossen sind. Dieser Access-Point war wahrlich schwer zu übersehen, prangte doch auf ihm der Aufkleber »AP 10«.

Die Abbildungen 27.9 und 27.10 wurden in einer Filiale einer Lebensmittelkette aufgenommen. Abbildung 27.10 zeigt die Montagehalterung, in die der Access-Point eingesetzt wird. Es sieht so aus, als sei rechts bereits eine Antenne installiert.

Wie Sie sehen, werden immer mehr Access-Points gewerblich eingesetzt; man findet sie nicht nur in Kleinunternehmen und bei Privatanwendern, sondern auch in großen Kaufhäusern. Die Tatsache jedoch, dass ein Cracker den Access-Point eines Unternehmens zu Gesicht bekommt, bedeutet nicht automatisch, dass er auch eine Verbindung mit ihm herstellen kann.

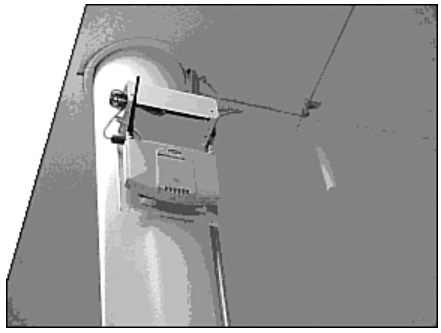


Abbildung 27.9: Bei einem Lauschangriff entdeckter Access-Point und Antennen

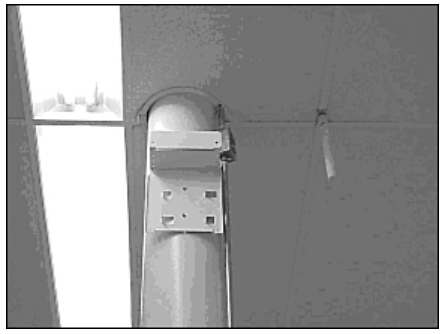


Abbildung 27.10: Bei einem Lauschangriff entdeckte Access-Point-Halterung

Zunächst muss er weitere Informationen sammeln, bevor er auf das Netzwerk zugreifen kann. Außerdem ist ein Lauschangriff nicht immer die beste Option zur Entdeckung eines Funknetzwerks. Da diese Angriffsform extrem zielgerichtet ist, können Tage vergehen, bis ein Angreifer etwas Interessantes zu Gesicht bekommt. Überdies lässt sich ein Lauschangriff nicht realisieren, wenn der Angreifer keinen physischen Zugang zum Gelände des Opfers hat. Aus diesem Grund haben Hacker eine neue Entdeckungsmethode entwickelt: das War-Driving.

27.7.2 War-Driving

Wenn ein Lauschangriff nur schwer oder gar nicht durchzuführen ist, dann ist das War-Driving eine effiziente Alternative. In vielen Situationen ist War-Driving auch die direkte Folge eines Lauschangriffs und dient zur Ermittlung weiterer Informationen. Aber es kommt umgekehrt auch oft vor, dass Informationen, an die man durch ungezieltes War-Driving gelangt ist, zu einem Lauschangriff auf ein aufgestöbertes Opfer führen.

Der Begriff War-Driving ist von einem anderen Terminus abgeleitet, der aus den Achtzigerjahren stammt und eine Methode zum Knacken von Computern über Telefonleitungen beschreibt: das War-Dialing. Beim War-Dialing ging es darum,

Telefonnummern in einem bestimmten Nummernbereich nacheinander durchzuwählen und so Modems aufzuspüren. Diese Methode zum Aufspüren von Modems ist derart effektiv, dass sie auch heute noch von vielen Crackern und Sicherheitsfachleuten eingesetzt wird. Auf ähnliche Weise wird das War-Driving, das heute noch in den Kinderschuhen steckt, in den nächsten Jahren gleichermaßen zum Knacken und zum Sichern von Funknetzwerken verwendet werden.

Das War-Driving erfuhr seinen ersten Popularitätsschub im Jahr 2001, als erste Tools zum Scannen von Funknetzen einer breiteren Öffentlichkeit verfügbar gemacht wurden. Diese von den Crackern benutzten Tools bestanden im Wesentlichen zunächst aus einer einfachen Konfigurationssoftware, die mit Funknetzwerkkarten ausgeliefert wurde. Bei der Entwicklung dieser Software dachte man aber weder an War-Driving noch an ihren Einsatz zur Netzwerksicherung, und deswegen war sie auch nicht besonders effektiv. Man brauchte also eine bessere Alternative. Trotzdem setzen viele War-Driver dieses Programm nach wie vor ein, denn es stellt eine nützliche Ergänzung zu fortschrittlicherer Software dar.

Warum brauchen wir auch auf der guten Seite War-Driver? Viele der großen Unternehmen sind nach eigenen Angaben wenig besorgt; hier geht man davon aus, dass man den Angreifer auf dem Parkplatz erspäht und dann vom eigenen Sicherheitspersonal festnehmen lässt. Das Problem dieser Denkweise besteht darin, dass die Reichweite von Funknetzen nicht nur über den Firmenparkplatz hinausreichen *kann*, sondern dies in der Regel sogar *tut*. Bedenken Sie, dass es sich um eine drahtlose Technologie handelt, und anders als bei normalen leitungsgestützten Netzwerken endet der Weg der Datenpakete nicht am anderen Ende des CAT5-Kabels. Vielmehr können Funknetze, die auf Standardgeräten und Zusatzantennen basieren, sich nachgewiesenermaßen über *mehr als 40 Kilometer* erstrecken. Wenn ein Cracker das weiß, dann kann er sich ein ganzes Stück von Ihrem Parkplatz entfernt aufhalten und sich trotzdem in Ihr Netzwerk eingeschlichen haben.

War-Driving selbst stellt keinen Angriff auf das Netzwerk dar und wird von vielen Rechtsexperten in den Vereinigten Staaten noch nicht einmal als Rechtsbruch angesehen. Diese Meinung muss jedoch erst einmal vor den amerikanischen Gerichten Bestand haben, und wenn es so weit kommt, dann ist ein Urteil über den War-Driver schwer zu fällen. Auch in Deutschland ist War-Driving nicht strafbar, solange man nicht einen besonderen Zugangsschutz überwinden muss, um in ein Netz zu gelangen.

Ein Problem könnte insbesondere sein, dass sich ein Angreifer (oder auch ein ehrlicher Administrator) beim War-Driving auf öffentlichem Grund und Boden aufhält, ja, sogar in einem Auto oder Bus in der Fortbewegung begriffen sein könnte. Die Software auf seinem Computer erlaubt ihm das Abfangen der Beacons, die normalerweise alle zehn Millisekunden von den Access-Points gesendet werden. Wie bereits erwähnt, senden Access-Points diese Beacons als Broadcasts, um ihre Anwesenheit zu signalisieren und das Vorhandensein anderer Access-Points in ihrem Bereich zu erkennen. Auch Clients nutzen Beacon-Frames, um die in ihrem Büro verfügbaren Netzwerke zu identifizieren. Micro-

soft Windows XP kann Ihnen sogar eine Liste mit Funknetzen anzeigen, die Beacons verwenden. Aus diesem Grund ist das War-Driving für sich genommen legal, denn die Access-Points senden ihre Daten ja aus, und Sie *empfangen* sie nur – nicht umgekehrt. Sie sind also, ob Sie wollen oder nicht, nur passiver Empfänger.

Eines der bekanntesten War-Driving-Softwarepakete heißt NetStumbler. NetStumbler wird von seinem Autor Marius Milner kostenlos unter `http://www.netstumbler.com` zum Download angeboten. Das Programm untersucht Beacons und bringt sie dann in ein Darstellungsformat; es achtet insbesondere darauf, diese Frames dem Benutzer nicht in ihrer Rohform zur Verfügung zu stellen. Die folgende Liste zeigt einige der Informationen an, die NetStumbler den Beacons entnimmt:

- BSSID (eine aus sechs Bytes bestehende Hexadezimalzahl, die auf den Access-Point oder die Basisstation verweist, von der der beobachtete Datenverkehr stammt)
- vorhandene oder fehlende WEP-Verschlüsselung
- Gerätetyp (Access-Point oder Peer-Gerät)
- den vom Besitzer vergebenen Namen des Geräts
- den Hersteller des Geräts
- MAC-Adresse des Funknetzgeräts
- Kanal, auf dem das Gerät erkannt wurde
- Signalstärke des Geräts
- Ortskoordinaten (sofern ein GPS-System eingesetzt wird)

Zu keiner Zeit werden Daten- oder Administrations-Frames von der Software abgefangen und dem Benutzer zugänglich gemacht.

Bei vielen Access-Points lässt sich ein Tarnkappenmodus programmieren, bei dem eine Option darin besteht, das Beacon-Broadcasting zu deaktivieren; das bedeutet, dass der Beacon zwar nach wie vor alle zehn Millisekunden gesendet wird, aber ohne BSSID. Wenn ein Netzwerkadministrator diese Option gewählt hat, erkennt NetStumbler das Netzwerk nicht mehr.

Zusammenfassend kann man den Ablauf bei der Verwendung von NetStumbler wie folgt beschreiben:

- Ein War-Driver empfängt einen Broadcast-Frame, der von einem Access-Point oder einem Peer-Gerät gesendet wurde.
- Es wird nur dieser Frame formatiert und dem War-Driver angezeigt.
- Daten- oder Administrations-Frames bekommt der War-Driver nicht zu Gesicht.

Man kann nun fragen, inwieweit sich diese Vorgehensweise vom Einsatz von Sniffern in leitungsbasierten Netzwerken unterscheidet, mit denen Sie beliebige Pakete in einem Netzwerk abfangen können. Bezüglich solcher und ähnlicher Rechtsfragen sollten Sie sich immer über die gültigen Gesetze und Vorschriften

auf dem Laufenden halten, um nicht eines Morgens eine unliebsame Überraschung zu erleben.

HINWEIS

Bezüglich der Rechtslage in Deutschland verweist die Fachzeitschrift c't in ihrer Ausgabe vom März 2003 auf folgenden Sachverhalt:

Wer unbefugt in ein gegen Zugriff gesichertes Netzwerk eindringt und sich dort nicht für ihn bestimmte Informationen beschafft, macht sich nach §202a des Strafgesetzbuches (StGB) des Ausspähens von Daten strafbar. Darauf steht eine Freiheitsstrafe von bis zu drei Jahren.

War-Driving wird normalerweise von einem Fahrzeug aus durchgeführt, also etwa in einem Auto oder Bus. Eine sehr effiziente Möglichkeit des War-Drivings in einer Stadt, die man noch nicht kennt, besteht in einer Fahrt mit den öffentlichen Verkehrsmitteln oder sogar mit einem Sightseeing-Bus. Beide Varianten bieten Ihnen die Möglichkeit, sicher und ungestört mit Ihrem Computer zu arbeiten und alles zu beobachten, was um Sie herum vorgeht – schließlich fahren Sie ja nicht selbst. Viele War-Driver sind allerdings bereits dazu übergegangen, ihre Autos mit unterschiedlichen Aufbauten und Antennen auszurüsten, um ein ununterbrochenes War-Driving durchzuführen.

ACHTUNG

Während der Fahrt sollte man, wenn man seinen Wagen selbst steuert, tunlichst vom War-Driving Abstand nehmen (es sei denn, man lässt seinen PDA oder sein Laptop passiv Daten zur späteren Auswertung sammeln).

Da Mobilelektronik immer populärer und preiswerter wird, stößt man immer häufiger auf solche Einrichtungen. Die folgende Liste enthält eine Reihe von Komponenten, die zum War-Driving eingesetzt werden:

- Funknetzwerkkarte (wieder meine Empfehlung: ORiNOCO-Karte)
- Computer (am besten ein Laptop oder ein PDA)
- Software (NetStumbler oder die Konfigurationssoftware der ORiNOCO-Karte)
- Wechselrichter
- externe Antenne
- GPS

Die letzten drei Elemente sind optional und für das War-Driving nicht unbedingt erforderlich. Ich empfehle sie jedoch trotzdem Anwendern aus den Bereichen der wissenschaftlichen Forschung und der Strafverfolgung sowie aus dem Militärbereich, denn ihr Einsatz wird die Genauigkeit der Untersuchungsergebnisse erheblich verbessern.

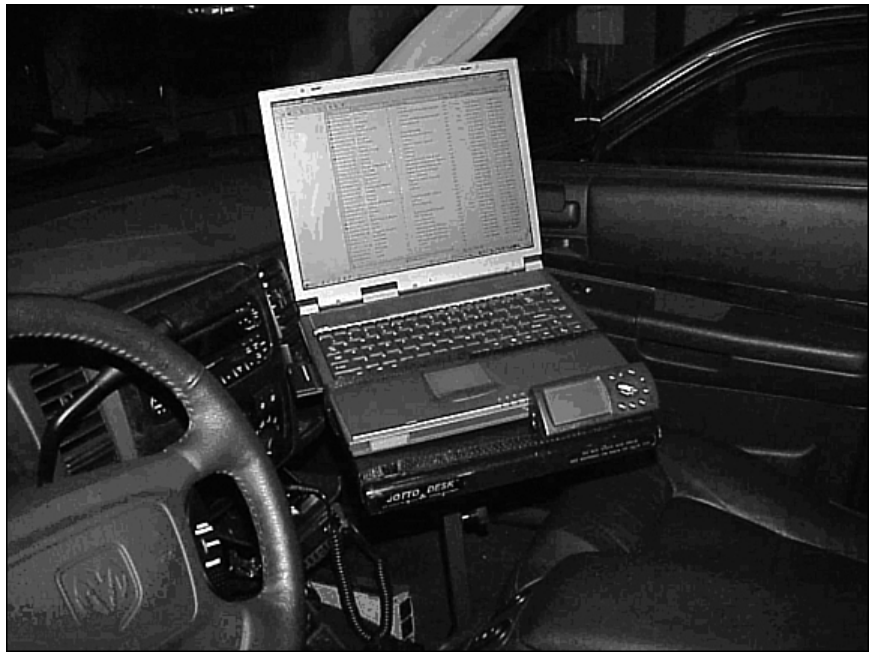


Abbildung 27.11: Für War-Driving ausgerüstetes Fahrzeug

Wenn sich ein Cracker die notwendigen Geräte besorgt hat, kann er mit der Suche nach Funknetzen beginnen. Setzen Sie sich ins Auto, und fahren Sie durch Ihre Wohngegend oder das nächstgelegene Industriegebiet. Städtische Bereiche mit hoher Wohndichte sind empfehlenswerte Orte zum Aufspüren von Netzwerken. Einige dieser Netze gehören wahrscheinlich Privatanwendern, die eine Verbindung zu ihrem DSL- oder Kabelmodem halten, andere gewiss größeren Firmen. Als ich beispielsweise eines Tages von der Arbeit kam und meine Gerätschaften abzuschalten vergessen hatte, stieß ich auf nicht weniger als acht Access-Points, die sämtlichst unverschlüsselt sendeten und mit ihren Broadcasts die große weite Welt einluden. Das Bedenkliche daran aber war die Tatsache, dass alle acht Access-Points aus der Zentrale eines großen Kreditinstitutes sendeten …

Um das War-Driving mithilfe der Software durchzuführen, die der ORiNOCO-Karte beiliegt, gehen Sie wie folgt vor:

1. Installieren Sie Ihre Funknetzkarte in einen Windows-Computer, und konfigurieren Sie sie.
2. Starten Sie den ORiNOCO Client Manager (siehe Abbildung 27.12).
3. Wählen Sie im Menü ACTIONS den Eintrag ADD/EDIT CONFIGURATION PROFILE (siehe Abbildung 27.13).
4. Wählen Sie das Profil *Default,* und klicken Sie auf EDIT PROFILE.

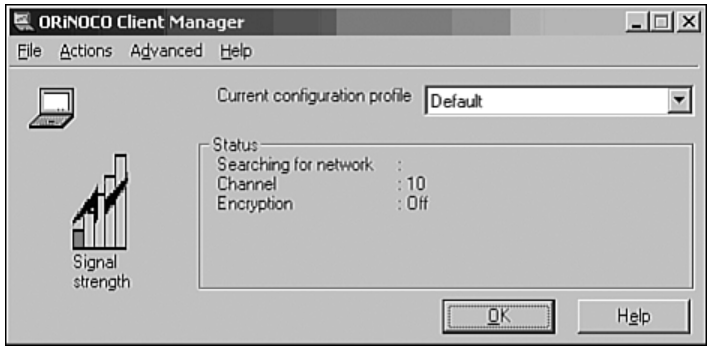


Abbildung 27.12: ORiNOCO-Karte mit dem Client Manager konfigurieren

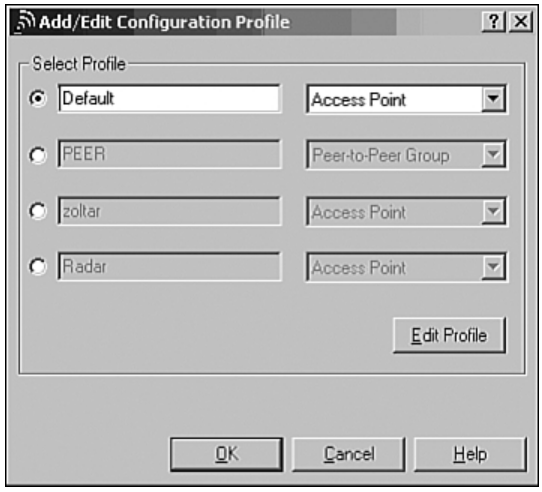


Abbildung 27.13: Konfigurationsprofil editieren

5. Setzen Sie im Feld NETWORK NAME den Wert *ANY*. Dies ist ein reservierter Name, der der Funknetzkarte mitteilt, dass eine Verbindung mit jedem Netzwerk hergestellt werden kann (siehe Abbildung 27.14).

6. Klicken Sie nun auf die Registerkarte ADMIN, und selektieren Sie im Abschnitt MAC ADDRESS das Feld NETWORK ASSIGNED. Diese Einstellung ermöglicht Ihnen die Erkennung und Falschangabe Ihrer MAC-Adresse. Auf diese Weise bleibt Ihre echte MAC-Adresse unerkannt, wenn Sie eine Verbindung mit einem Access-Point herstellen. Praktisch ist dies auch, wenn Sie versuchen, eine Verbindung zu einem System herzustellen, das Ihre MAC-Adresse für Zugriffe gesperrt hat (siehe auch Abschnitt 27.7.3, »P2P-Cracking«). Seien Sie bei der MAC-Adresse ruhig etwas kreativ, und verwenden Sie eine Adresse wie die in Abbildung 27.15 gezeigte.

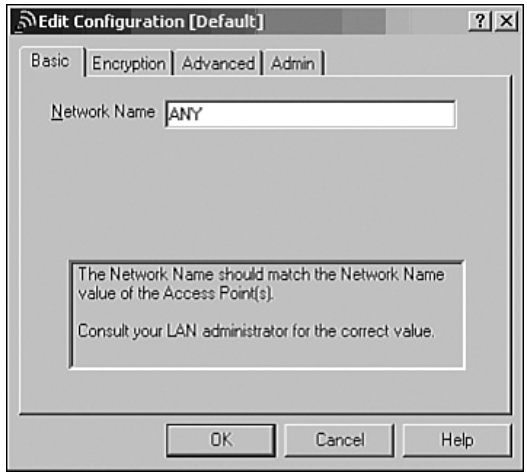


Abbildung 27.14: Netzwerknamen konfigurieren

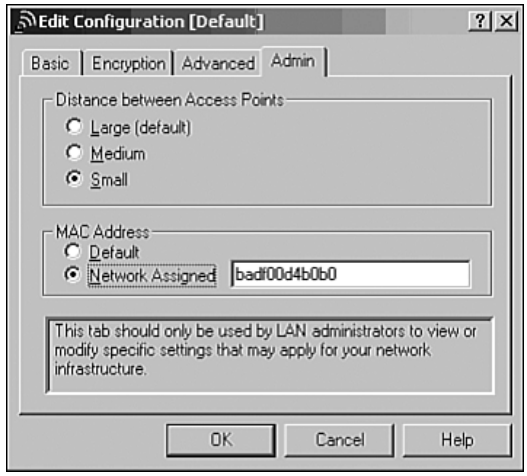


Abbildung 27.15: MAC-Adresse eingeben

Mit diesen Einstellungen können Sie das Vorhandensein verschiedener Funknetze erkennen (siehe Abbildung 27.16). Wenn Sie eine Verbindung hergestellt haben, werden Ihnen die SSID (»zoolander«) und die MAC-Adresse des Access-Points angezeigt. Weitere Informationen über den Assoziationsvorgang finden Sie ebenfalls in Abschnitt »P2P-Cracking«.

Wenn auf dem Access-Point ein DHCP-Dienst (Dynamic Host Configuration Protocol) ausgeführt wird oder Anfragen an das angeschlossene leitungsbasierte Netzwerk weitergeleitet werden, dann kann es sogar sein, dass Ihnen das Zielnetzwerk eine gültige IP-Adresse zuweist! Damit dies funktioniert, muss Ihr Computer so konfiguriert sein, dass er DHCP sowohl für die IP-Adresse als auch für die DNS-Einstellungen verwendet.

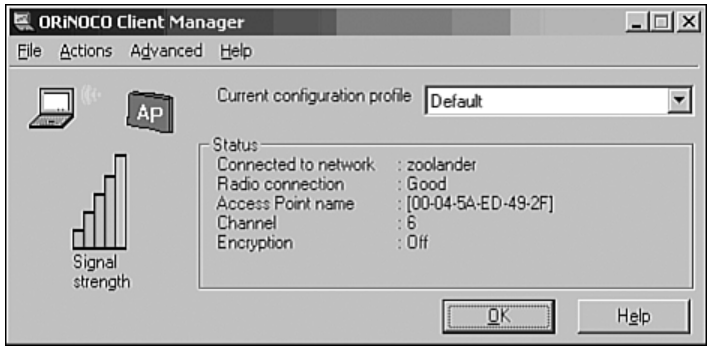


Abbildung 27.16: Erkanntes Netzwerk

Sie werden bald feststellen, dass die Möglichkeiten zur Erkennung von und zur Anmeldung an Funknetzen mit dem ORiNOCO Client Manager sehr begrenzt sind. Aus diesem Grund sind also erweiterte Fähigkeiten notwendig. Eines der Produkte, das solche Funktionen anbietet, ist das weiter oben erwähnte NetStumbler. Dieses Programm wollen wir uns nun einmal näher ansehen:

1. Installieren und konfigurieren Sie Ihre Funknetzwerkkarte mit der vom Hersteller vorgesehenen Software.
2. Laden Sie die aktuelle NetStumbler-Version von `http://www.netstumbler.com` herunter, und installieren Sie sie auf einem Windows-Computer.
3. Verbinden Sie Ihr GPS mit einem seriellen Anschluss des Computers (optional).
4. Starten Sie NetStumbler, und klicken Sie auf die Schaltfläche mit dem grünen Pfeil, der der Wiedergabetaste von CD-Playern ähnelt.

Nun können Sie einsteigen und ein wenig durch Wohn- und Industriegebiete fahren. Angesichts der Tatsache, dass Funknetze mittlerweile fast allgegenwärtig sind, gibt es eigentlich kaum eine Einschränkung potenzieller Suchbereiche. Verschiedene große Hotelketten bieten ihren Gästen in den Lobbys Access-Points zur Nutzung an. Gleiches gilt für Schnellrestaurants oder Flughäfen.

Wenn Sie ein GPS an Ihren Computer angeschlossen haben, können Sie auch aufzeichnen, wo der Access-Point gefunden wurde. Die Ausgabe auf eine Landkarte ist ebenfalls möglich (siehe Abbildung 27.17) – so können Sie alle Netzwerke lokalisieren, die NetStumbler erspäht hat.

Einige Gebäude (z.B. Firmenzentralen) liegen manchmal sehr weit von der Straße entfernt und sind derart groß, dass Sie das Vorhandensein eines Funknetzes auch bei Verwendung einer externen Antenne nur schwer erkennen können. In einer solchen Situation ist es gut, wenn man ein PDA wie etwa den Compaq iPAQ mit angeschlossener Funknetzkarte und eine Kopie des Programms miniStumbler (ebenfalls unter `http://www.netstumbler.com` herunterzuladen) hat. Stecken Sie den iPAQ in die Jackentasche, und begeben Sie sich in das Gebäude. Durchwandern Sie es Stockwerk für Stockwerk. miniStumbler

sammelt dann die Beacons von Funknetzen ein, die Sie von der Straße aus vielleicht nicht erfasst haben. Diese Vorgehensweise ist besonders effizient, wenn Sie Zugang zu einem bestimmten Büro im Gebäudeinnern haben, z.B. durch ein zuvor abgemachtes Treffen oder eine Besprechung. Auf diese Weise können Sie als Sicherheitsfachmann Ihre Untersuchungen verheimlichen, und es ist für die Mitarbeiter auch weniger verwirrend, als wenn Sie mit Antenne und Laptop durch die Gegend laufen.



Abbildung 27.17: Mithilfe eines GPS erstellte Karte mit Access-Points

Erinnern Sie sich noch, wie Sie das letzte Mal jemanden im Fahrstuhl oder auf dem Gang gesehen haben, der einen PDA dabei hatte? Hätten Sie gedacht, dass dieser Jemand mit War-Driving beschäftigt gewesen sein könnte? Oder hat er wirklich nur seine Termine überprüft?

Wenn Sie mit NetStumbler oder miniStumbler genug Informationen gesammelt haben, müssen Sie diese Daten analysieren und interpretieren. Abbildung 27.18 zeigt einen Screenshot von NetStumbler.

Alle möglichen Leute können War-Driver sein. Die verschiedenen Typen, die ich während meiner Untersuchungen getroffen habe, entsprechen so gar nicht dem Bild des Daten stehlenden Hackers. Man würde ja eher Schüler und Studenten damit in Verbindung bringen, die am Wochenende nichts Besseres zu tun haben; zugegeben, auch solche Leute sind dabei, aber die Mehrzahl der War-Driver sind der Schulbank lange entwachsene Spezialisten, die War-Driving ganz legal als Teil Ihrer Arbeit durchführen. Die Zahl der Sicherheitsfachleute, bei denen das War-Driving zu den täglichen Pflichten gehört, wird in den nächsten Jahren stark zunehmen.

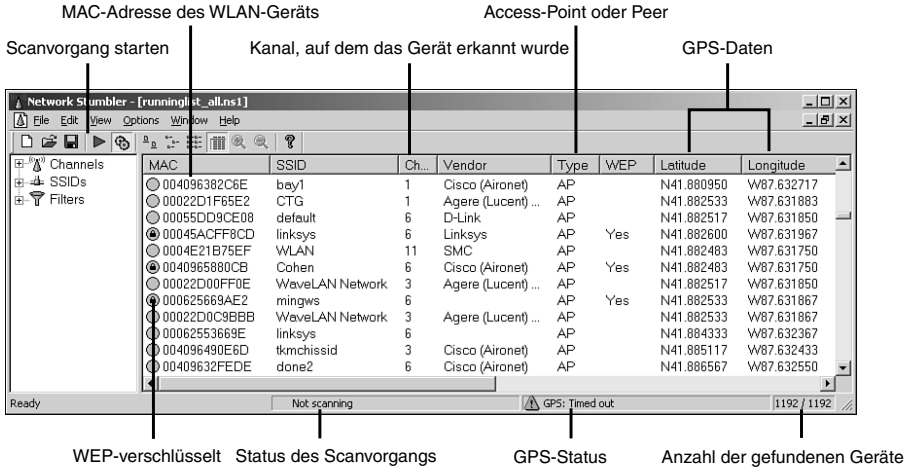


Abbildung 27.18: NetStumbler

Leider werden auch immer mehr Hacker diese Methode zur Erkennung von Funknetzwerken einsetzen. Eine gute Vorbereitung wird sich also auszahlen.

Nun haben wir also unser Zielobjekt ausfindig gemacht. Der Angriff kann beginnen.

27.7.3 P2P-Cracking

Clients gibt es in Funknetzen wie auch in leitungsgebundenen Netzwerken. Ein Client kann in vielerlei Gestalt auftreten, etwa als Drucker, als NAS-Gerät (Network Attached Storage) oder sogar als Server. In einem typischen Ad-hoc-Netzwerk gibt es normalerweise keine Server oder Drucker, sondern nur die Computer von Einzelbenutzern. Da eine Mehrzahl der Benutzer mit Betriebssystemen von Microsoft arbeitet und die meisten Benutzer auf die Sicherheit ihrer Computer recht wenig Wert legen, eröffnen sich in einem solchen Szenario eine Menge Möglichkeiten.

Ein Angreifer kann beispielsweise einen Angriff auf einen Laptop verüben, der über eine Funkverbindung angeschlossen ist. Zwar mag in dem Büro, in dem der Laptop steht, noch gar kein Funknetz implementiert sein, aber er könnte gleichzeitig mit dem Ethernetnetzwerk verbunden sein und über eine im Peer-Modus betriebene Funknetzkarte verfügen. Ferner senden Funknetzkarten im Peer-Modus in bestimmten Intervallen spezielle Datenpakete – die so genannten Probe-Request-Frames – aus, um eine Verbindung mit einem anderen Gerät mit identischer SSID herzustellen. Auf diese Weise könnte man mit einem Funknetz-Sniffer oder dem NetStumbler Funknetzgeräte im Peer-Modus ausfindig machen.

Viele moderne Laptops werden inzwischen mit integrierten WLAN-Karten und -Antennen ausgeliefert. Oft wird diese Funktionalität nicht benötigt, und das Endanwender weiß vielleicht nicht einmal, dass sein Gerät über diese Möglich-

keit verfügt. Wenn ein unaufmerksamer Administrator die WLAN-Komponenten nun beim Aussetzen des Betriebssystems nicht deaktiviert hat, kann dies leicht ausgenutzt werden.

Abbildung 27.19 zeigt einen Probe-Request-Frame, der mit einem Funknetz-Sniffer abgefangen wurde.

```
  Flags:          0x00
  Status:         0x00
  Packet Length:44
  Timestamp:      17:29:13.554563 01/12/1997
  Data Rate:      2  1.0 Mbps
  Channel:        7  2442 MHz
  Signal Level: 90%
802.11 MAC Header
  Version:                0
  Type:                   %00  Management
  Subtype:                %0100  Probe Request
  To DS:                  0
  From DS:                0
  More Frag.:             0
  Retry:                  0
  Power Mgmt:             0
  More Data:              0
  WEP:                    0
  Order:                  0
  Duration:               0  Microseconds
  Destination:            FF:FF:FF:FF:FF:FF  Broadcast
  Source:                 00:A0:F8:8E:E6:3E  SymbolCard
  BSSID:                  FF:FF:FF:FF:FF:FF  Broadcast
  Seq. Number:            1891
  Frag. Number:           0
802.11 Management - Probe Request
  Element ID:             0  SSID
  Length:                 8
  SSID:                   TESTSSID
  Element ID:             1  Supported Rates
  Length:                 4
  Supported Rate:         0x02  1.0 Mbps  (Not BSS Basic Rate)
  Supported Rate:         0x04  2.0 Mbps  (Not BSS Basic Rate)
  Supported Rate:         0x0B  5.5 Mbps  (Not BSS Basic Rate)
  Supported Rate:         0x16  11.0 Mbps  (Not BSS Basic Rate)
FCS - Frame Check Sequence
  FCS (Calculated):       0x6D823EC4
```

Abbildung 27.19: Mit einem Funknetz-Sniffer abgefangener Probe-Request-Frame

Eine solche Vorgehensweise würde es einem Cracker nun erlauben, eine Verbindung mit dem Laptop herzustellen, woraufhin er eine Vielzahl betriebssystemimmanenter Exploits ausnutzen und auf diese Weise Root- bzw. Administratorzugriff auf den Laptop erlangen könnte. Wenn ihm dies gelungen ist, könnte er mithilfe eines intelligent platzierten Trojaners oder eines Tastaturrecorders weiter in das oder die Netzwerksysteme Ihres Unternehmens eindringen. Diese Form des Angriffs kann sogar stattfinden, wenn der Zielbenutzer unterwegs ist und seinen Laptop etwa in einer Hotellobby oder auf einem Flughafen verwendet – unabhängig davon, ob er jetzt seine Funknetzwerkkarte verwendet oder nicht.

Damit ein Funknetzclient Daten an ein Netzwerk senden kann, muss der Client eine Beziehung zum Access-Point herstellen, die als Assoziation bezeichnet wird. Während des Assoziationsvorgangs durchläuft der Client nacheinander drei verschiedene Zustände:

- nicht assoziiert, nicht authentifiziert
- nicht assoziiert, authentifiziert
- assoziiert, authentifiziert

Zunächst muss der Client einen Beacon von einem Access-Point in seiner Reichweite erhalten. Werden Beacons mehrerer Access-Points empfangen, dann wählt der Client selbstständig aus, welchem BSS er beitritt. Der ORiNOCO Client Manager etwa ordnet sich dem ersten erkannten BSS zu, stellt aber eine Liste aller erkannten SSIDs zur Verfügung, auf die man umschalten kann. Benutzern von Windows XP wird eine Liste der SSIDs mit der Aufforderung angezeigt, das gewünschte Netzwerk auszuwählen. Ferner kann der Client einen Probe-Request-Frame als Broadcast an beliebige Access-Points senden.

Wurde nun ein Access-Point entdeckt, dann werden im Zuge der gegenseitigen Authentifizierung eine Reihe von Administrations-Frames ausgetauscht. Zur Durchführung dieser gegenseitigen Authentifizierung gibt es gemäß der 802.11b-Spezifikation zwei Standardmethoden. Die erste ist die so genannte Open-System-Authentifizierung. Die Mehrzahl aller Access-Points wird – insbesondere wenn die Standardeinstellungen nicht geändert werden – diese Methode verwenden. Wie der Name impliziert, handelt es sich hier um ein offenes System, und alle Authentifizierungsanfragen werden bedient.

Die Authentifizierung umfasst zwei Schritte: Zunächst bittet der Sender beim Access-Point (oder einer anderen Station) um Authentifizierung, im zweiten Schritt übermittelt der Empfänger das Ergebnis der Anfrage. Die Anfrage wird nur dann negativ beantwortet, wenn die um Authentifizierung bittende Station im Vorfeld explizit für den Zugriff auf ein WLAN gesperrt worden ist. Daher bietet die Open-System-Authentifizierung keine echte Abwehr gegen unberechtigte Eindringlinge.

Die zweite Variante ist die Shared-Key-Authentifizierung. Diese verwendet zusätzlich zum Standardverfahren (Challenge/Response) einen gemeinsamen Geheimschlüssel. Dieser geheime Schlüssel wird niemals übertragen, sodass er bei allen teilnehmenden Stationen und Access-Points vorher von Hand eingetragen werden muss.

Die Authentifizierung erfolgt in vier Schritten: Zuerst sendet der Client einen Frame mit einer Authentifizierungsanforderung, der angibt, dass er die Shared-Key-Authentifizierung einsetzen will. Empfängt ein Access-Point diese Anforderung, dann antwortet er dem Client, indem er einen Authentifizierungs-Frame sendet, der 128 Bits mit dem Challenge-Text enthält. Der WEP-PRNG (Pseudo-Random Number Generator, d.h. eine Funktion zur Generierung von Pseudozufallszahlen) wird dann zur Erzeugung des Challenge-Textes mit dem gemeinsamen Schlüssel und einem Zufalls-IV (Initialization Vector, Initialisierungsvektor) verwendet. Der Client empfängt den Authentifizierungs-Frame und kopiert den Challenge-Text in einen neuen Frame. Dann wählt er einen neuen IV aus, den er zusammen mit dem kopierten Challenge-Text im Frame ablegt. Der gesamte Frame wird dann (unter Verwendung des gemeinsamen Geheimschlüssels) WEP-verschlüsselt und an den Access-Point übertragen.

Wenn der Access-Point den Frame empfängt, entschlüsselt er ihn und kontrolliert zunächst die Gültigkeit der 32 Bit langen Integritätsprüfsumme. Diese Verifizierung erfolgt durch Vergleich mit dem Challenge-Text, der Bestandteil der ersten gesendeten Nachricht war. Stimmen die Texte überein, dann wird die Authentifizierung als erfolgreich betrachtet. Nun ist aber erst die Hälfte der Strecke zurückgelegt: Client und Access-Point tauschen jetzt die Rollen, und der gesamte Ablauf wiederholt sich. Nach dem Abschluss des Vorgangs wechselt der Client in den zweiten Zustand (nicht assoziiert, aber authentifiziert).

In diesem Status sendet der Client nun einen Frame mit einer Assoziationsanforderung an den Access-Point. Der Access-Point antwortet mit einem entsprechenden Antwortpaket an den Client. Wenn der Client dieses Paket empfängt, wechselt er in den dritten Status (assoziiert und authentifiziert). Nun wird der Client zum Peer, d. h., er kann Daten-Frames in das Netzwerk senden und aus diesem empfangen. Abbildung 27.20 zeigt das Format des Authentifizierungs-Frames, Abbildung 27.21 den prinzipiellen Ablauf des Authentifizierungs- und Assoziationsvorgangs.

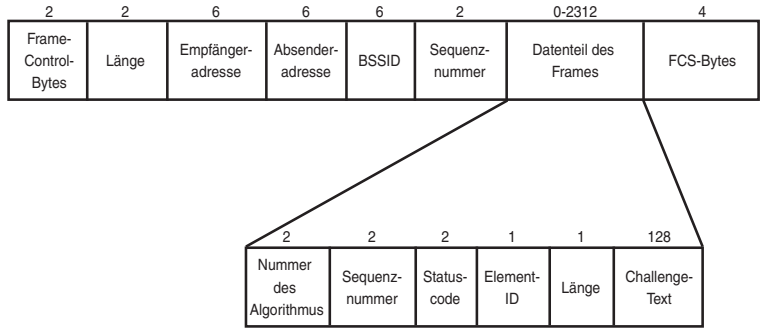


Abbildung 27.20: Authentifizierungs-Frame

Nachdem der Client assoziiert und authentifiziert wurde, sind Sie im Netzwerk. In den meisten Fällen brauchen Sie allerdings eine IP-Adresse, um mit anderen Clients oder Servern im Netzwerk zu kommunizieren. Viele Access-Points sind standardmäßig so konfiguriert, dass sie auch als DHCP-Server agieren. Ist dies der Fall, dann erhalten Sie eine gültige IP-Adresse für das Netzwerk. Ist DHCP dagegen deaktiviert, dann müssen Sie sich selbst eine solche Adresse zuweisen.

Abbildung 27.22 zeigt, wie ein typisches Firmennetzwerk aufgebaut sein könnte. Die Firewall bietet internen Benutzern und Servern Schutz, und alle WLAN-Geräte befinden sich hinter ihr. Der gesamte ein- und ausgehende Internetverkehr wird durch die Firewall gefiltert. Leider konnte sich ein Angreifer an einem Access-Point assoziieren und authentifizieren und kann nun auf alle internen Server und Computer zugreifen. Ferner lässt sich die Internetverbindung nun nutzen, um Angriffe auf andere Netzwerke zu starten.

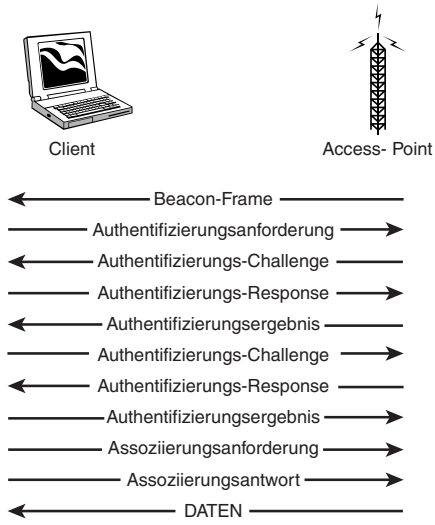


Abbildung 27.21: Der Authentifizierungs- und Assoziationsvorgang

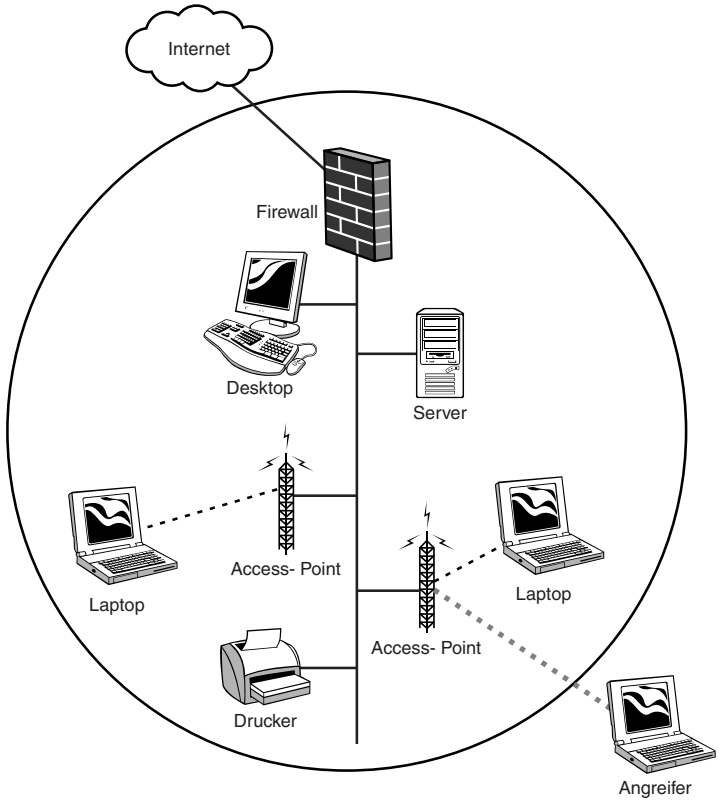


Abbildung 27.22: Typische Netzwerkkonfiguration mit Ethernet- und 802.11b-Geräten

Anspruchsvollere Access-Points bieten ACLs, mit denen ein Administrator die MAC-Adressen der Ethernetkarten aller Clients zur Assoziation und Authentifizierung vordefinieren kann. Wenn ein Client sich nun zu authentifizieren versucht und seine MAC-Adresse nicht in der ACL aufgeführt ist, dann wird ihm der Zugriff auf das Netzwerk verweigert. Es ist aber, wie wir bereits im Abschnitt »War-Driving« gesehen haben, mithilfe geeigneter Software möglich, eine gefälschte MAC-Adresse für unsere Funknetzwerkkarte zu konfigurieren. Mit dieser Funktionalität und einem Funknetz-Sniffer wie AiroPeek (`http://www.wildpackets.com`) können Sie eine Liste der MAC-Adressen abfangen, die im Netzwerk eingesetzt werden (siehe Abbildung 27.23). Wenn Sie die benötigten Informationen haben, können Sie die MAC-Adresse einer in der ACL aufgelisteten Ethernetkarte übernehmen, d. h., sich assoziieren und authentifizieren.

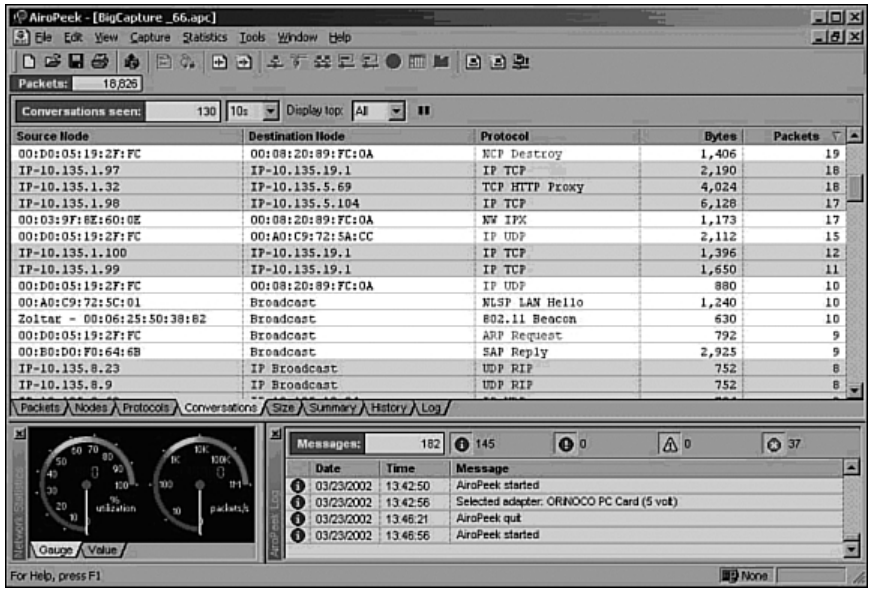


Abbildung 27.23: Ermittlung von MAC-Adressen mit AiroPeek

Hat ein Angreifer sich authentifizieren und assoziieren können, dann werden seine Möglichkeiten nur durch die von Ihnen implementierten Sicherheitsmaßnahmen für das interne Netzwerk beschränkt. Nehmen wir einmal an, Sie hätten ein Netzwerk ähnlich dem in Abbildung 27.22 gezeigten. Dies könnte sowohl ein Heimnetzwerk als auch ein Firmennetz mit oder ohne alle gezeigten Komponenten sein. Hat sich der Angreifer assoziiert, dann besteht sein nächster Schritt darin, im Netzwerk eine gültige IP-Adresse zu erhalten. Wenn er mit AiroPeek die Frames im WLAN abfängt, erhält er eine Liste gültiger IP-Adressen von derzeit im Netzwerk kommunizierenden Geräten und kann daraus seine Schlüsse bezüglich der IP-Adressvergabe im Netzwerk ziehen (siehe Abbildung 27.24).

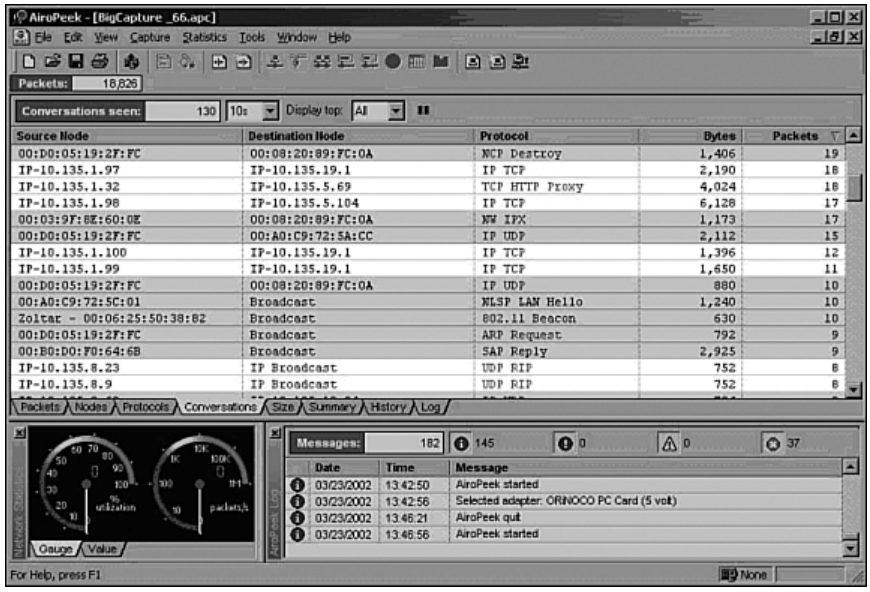


Abbildung 27.24: Mit AiroPeek abgefangene IP-Adressen

Nachdem der Cracker nun an eine gültige IP-Adresse in Ihrem Netzwerk gekommen ist, wird es für ihn Zeit, sein Opfer zu finden und mehr Informationen über Ihre Systemkonfiguration zu sammeln. Die verschiedenen Methoden zur Realisierung dieses Vorhabens unterscheiden sich nicht von denen, die man in einem normalen Ethernetnetzwerk einsetzen würde; es macht keinen Unterschied, ob eine Funknetzkarte sich mit einem Access-Point assoziiert oder ob der betreffende Computer direkt an Ihr Ethernet-LAN angeschlossen wird. Aus diesem Grund gelten alle in den anderen Kapiteln dieses Buches vermittelten Informationen zum Ausspähen eines Netzwerks entsprechend; all diese Methoden geben dem Angreifer letztendlich eine Liste der in Ihrem Netzwerk verfügbaren Ressourcen (z.B. Drucker) in die Hand.

In unserem Beispiel wollen wir einmal davon ausgehen, dass der Drucker mit dem integrierten TCP-Spooler arbeitet und über eine Weboberfläche konfiguriert werden kann (ein solches Szenario ist heutzutage in Firmennetzwerken nicht ungewöhnlich). Der Angreifer findet den Drucker und stellt bei der Überprüfung der Weboberfläche fest, dass er den Drucker in einen Modus versetzen kann, in dem dieser Testseite um Testseite ausdruckt. In der Zwischenzeit werden Sie auf Ihrem Drucker nicht drucken können, da die Warteschlange voller Testseiten ist, und der Druckertoner wird auch recht schnell verbraucht sein. Dies ist nur ein Beispiel für eine an sich harmlose, aber doch sehr unerfreuliche Attacke.

Druckerattacken sind ja noch vergleichsweise ungefährlich. Überlegen Sie einmal, wie anfällig in einer solchen Situation Ihre auf Computern und Servern im Netzwerk gespeicherten unternehmenskritischen Daten wären. Es ist schon paradox: Viele Unternehmen glauben, auf den Schutz ihrer Netzwerke vor

internen Angriffen verzichten zu können, verschließen aber des Nachts die Türen der Geschäftsgebäude, ohne allen Mitarbeitern einen Schlüssel auszuhändigen!

27.7.4 Nicht genehmigte Access-Points

Als nicht genehmigte Access-Points oder Rogue-Access-Points bezeichnet man solche, die an ein Netzwerk angeschlossen werden, ohne dass der Administrator dies geplant oder erlaubt hat. Ich kenne beispielsweise einen Administrator in Dallas, der gerade zum ersten Mal eine Überprüfung seines Funknetzes – eines über acht Stockwerke verteilten Campusnetzwerks – mithilfe des War-Drivings vorgenommen hat. Zu seiner Überraschung fand er insgesamt mehr als dreißig Access-Points – nicht schlecht angesichts der Tatsache, dass er nur vier davon für den Anschluss an das Netzwerk freigegeben hatte. Natürlich rollten Köpfe …

Nicht genehmigte Access-Points werden in der Sicherheitsbranche zunehmend zum Problem. Da der Preis erschwinglicher Access-Points mittlerweile auf etwas über 100 € gefallen ist, sind solche Geräte inzwischen allgegenwärtig. Außerdem finden sich bei vielen Access-Points Werkseinstellungen, die sie für das Netzwerk transparent machen, d. h., ihr Vorhandensein ist schwer zu entdecken.

Viele derartige Access-Points werden von Mitarbeitern aufgestellt, die sich bei der Arbeit mehr Bewegungsfreiheit verschaffen wollen. Sie bringen ihre eigenen Access-Points einfach von zu Hause mit und schließen sie ohne Erlaubnis der Administratoren direkt an das Firmen-LAN an. Diese Sorte nicht zulässiger Access-Points kann sehr gefährlich sein, da die meisten Benutzer sich nicht über die in Verbindung mit Netzwerken im Allgemeinen und Funknetzwerkgeräten im Besonderen auftretenden Sicherheitsprobleme im Klaren sind.

Überdies sind es auch nicht immer die wohlgesinntesten Angestellten, die Rogue-Access-Points in Betrieb nehmen. Verärgerte Mitarbeiter oder sogar externe Angreifer können einen solchen Access-Point innerhalb von Sekunden in Ihrem Netzwerk implementieren und später – etwa bei Nacht – eine Verbindung herstellen. Und wenn an diesem Access-Point DHCP aktiviert ist, dann befindet sich in Ihrem Netzwerk sogar noch ein unzulässiger DHCP-Server – zusätzlich zum Loch an der Peripherie Ihres Funknetzes.

Hier sind die sieben Schritte zum erfolgreichen Aufstellen eines Rogue-Access-Points:

- Bestimmen Sie die Vorteile, die Ihnen eine Aufstellung des Access-Points brächte.
- Planen Sie für die Zukunft. Wählen Sie einen Standort aus, der es Ihnen ermöglicht, ungesehen mit einem Laptop oder einem PDA zu arbeiten.
- Stellen Sie den Access-Point an einem diskreten Standort auf, der gleichzeitig größtmögliche Reichweite bietet.

- Deaktivieren Sie das SSID-Broadcasting (»stummer« Modus). Auf diese Weise wird die Entdeckung des Access-Points weiter erschwert, denn nun braucht man dafür einen Funknetz-Sniffer.
- Deaktivieren Sie Administrationsfunktionen. Viele Access-Points bieten die Möglichkeit, SNMP-Traps sowohl in leitungsgestützte als auch in Funknetze zu übertragen.
- Sofern es möglich ist, sollten Sie den Access-Point hinter einer Firewall platzieren. Auf diese Weise verbergen Sie Ihre MAC-Adresse vor dem LAN und den ARP-Tabellen der Router. Es gibt mehrere Programme auf dem Markt, die in leitungsgestützten Netzwerken nach den MAC-Adressen von Access-Points suchen.
- Seien Sie nicht zu gierig! Belassen Sie den Access-Point nur für kurze Zeit an seinem Standort. Je länger er in Betrieb bleibt, desto größer ist die Wahrscheinlichkeit, dass man Sie schnappt.

ACHTUNG

Die vorangegangenen Schritte sollten Sie selbstverständlich nur durchführen, wenn Sie in Ihrem eigenen Testnetzwerk experimentieren!

Wenn Sie bereits ein Funknetzwerk in Betrieb genommen haben und jemand unter Verwendung Ihrer vorhandenen SSID dort einen unzulässigen Access-Point aufstellt, dann haben Sie möglicherweise noch mehr Probleme. Ein solcher Access-Point kann Ihr Netzwerk über die Grenzen Ihres Büros hinaus vergrößern. In manchen Fällen kann der Rogue-Access-Point sogar so konfiguriert werden, dass er als Verbindungsglied fungiert, über das Ihre Netzwerkdaten in der ganzen Stadt verteilt werden. Schlimmer noch: Der Rogue-Access-Point kann so eingestellt werden, dass er als Teil Ihres Netzwerks erscheint, d. h., Ihre Clients verwenden ihn, um Verbindungen herzustellen. Wenn sich ein Client mit dem unzulässigen Access-Point verbindet und dann versucht, auf einen Server zuzugreifen, dann können Ihr Benutzername und Ihr Kennwort abgefangen und später für einen Angriff auf Ihr Netzwerk verwendet werden.

27.7.5 Jamming – DoS-Angriffe gegen das Funknetz

Wie Sie bereits in früheren Kapiteln gesehen haben, handelt es sich bei DoS-Angriffen um solche Angriffe, bei denen Funktionen oder Dienste nicht mehr ordnungsgemäß verwendet werden können. Solche Angriffe gibt es natürlich auch bei Funknetzen. Um dies nachvollziehen zu können, müssen Sie zunächst einmal verstehen, wie 802.11b-kompatible Funknetze operieren und auf welchen Frequenzen sie betrieben werden.

Der effiziente Angriff (bzw. die effiziente Absicherung) eines Funknetzes setzt ein gewisses Maß an Wissen darüber voraus, was Funksender, Frequenzen und Wellenlängen bedeuten und wie sie sich zueinander verhalten. Einrichtungen wie Polizeifunkgeräte, automatische Garagentüren, schnurlose Telefone, GPS-

Empfänger, Mikrowellenherde und Handys verwenden unterschiedliche Betriebsfrequenzen. Es gibt Millionen solcher Geräte, die im Funkspektrum betrieben werden können, ohne einander zu stören (siehe Tabelle 27.3).

Bandbereichsname	Frequenzbereich	Einsatzbereich
VLF (Very Low Frequency, Längstwelle)	10 kHz…30 kHz	
LF (Low Frequency, Langwelle)	30 kHz…300 kHz	Langwellenradio
MF (Medium Frequency, Mittelwelle)	300 kHz…3 MHz	Mittelwellenradio
HF (High Frequency, Kurzwelle)	3 MHz…30 MHz	Kurzwellenradio
VHF (Very High Frequency, Ultrakurzwelle)	30 MHz…328,6 MHz	UKW-Radio
UHF (Ultra High Frequency)	328,6 MHz…2,9 GHz	Mikrowellenherde, Mobiltelefonnetze (D-Netze: 890…960 MHz; DECT: 1,8…1,9 GHz; UMTS: 1,97…2,2 GHz), Bluetooth (2,402…2,480 GHz), WLAN (2,4GHz)
SHF (Super High Frequency)	2,9 GHz…30 GHz	WLAN (5,7GHz)
EHF (Extremely High Frequency)	>30 GHz	

Tabelle 27.3: Bezeichnungen der Funkfrequenzbereiche

Funkwellen sind sehr leicht zu erzeugen – das können Sie sogar selbst ausprobieren. Die folgende Beschreibung zeigt Ihnen, wie Sie Ihre eigenen Radiowellen generieren und hören können.

Benötigte Utensilien: 9-V-Blockbatterie, Münze, Mittelwellenradio

1. Stellen Sie am Radio eine Frequenz zwischen zwei Sendern ein, bei der Sie nur statisches Rauschen hören.
2. Platzieren Sie die Batterie in der Nähe der Radioantenne.
3. Tippen Sie mit der Münze auf die beiden Anschlüsse der Blockbatterie. Sorgen Sie dafür, dass die Münze mit beiden Anschlüssen gleichzeitig in Kontakt kommt.

Jedes Mal, wenn das Geldstück mit den Batterieanschlüssen in Kontakt kommt, wird eine kurze Funkwelle erzeugt, die sich im Radio als Knistern äußert. Dieser einfache Stromkreis produziert runde elektromagnetische Störwellen, die sich lotrecht zum Stromfluss ausbreiten.

Wenn ein 802.11b-kompatibles Gerät Daten sendet, dann tut es dies nicht auf einer einzelnen Frequenz. Eine Technologie namens DSSS (Direct Sequence Spread Spectrum) wird zur Verteilung der übertragenen Daten auf mehrere Frequenzen eingesetzt. DSSS wurde entwickelt, um die Effizienz der Funkübertragung zu optimieren und gleichzeitig das Störpotenzial zu minimieren. Tabelle 27.4 zeigt die Zuweisungen von Kanälen und Frequenzen.

Kanal	Frequenz	Kanal	Frequenz
1	2,412 GHz	8	2,447 GHz
2	2,417 GHz	9	2,452 GHz
3	2,422 GHz	10	2,457 GHz
4	2,427 GHz	11	2,462 GHz
5	2,432 GHz	12	2,467 GHz
6	2,437 GHz	13	2,472 GHz
7	2,442 GHz	14	2,484 GHz

Tabelle 27.4: Zuordnung von Kanälen und Frequenzen bei DSSS

Bei DSSS bezeichnet der Begriff *Kanal* eher einen Regelsatz als eine bestimmte Frequenz. Diese Regelsätze legen fest, wie der Funksender das Signal über mehrere Frequenzen verteilt, die eben Kanäle genannt werden. Das Prinzip lässt sich an folgendem Beispiel veranschaulichen:

Stellen Sie sich vor, Sie geben eine Party, bei der sich die Gäste im ganzen Haus verteilen – in insgesamt elf Räumen. In jedem dieser Räume reden die Leute über ein anderes Thema, und der Klang dieser Gespräche breitet sich von Raum zu Raum aus. Wenn Sie etwa in Raum 1 sind, dann hören Sie die Unterhaltungen in den Räumen 1 bis 5; Gäste im sechsten Raum hören hingegen die Diskussionen aus den Räumen, 2 bis 10, können jedoch aus Raum 1 nichts wahrnehmen, weil dort eine Mauer steht – dies ist der Regelsatz.

Tabelle 27.5 zeigt die Struktur der Kanäle und veranschaulicht, was bei jedem Kanalregelsatz zu hören ist. Unter den elf Regelsätzen befinden sich nur drei, die keine Überschneidungen miteinander aufweisen: die Kanäle 1, 6 und 11.

Kan. 1	Kan. 2	Kan. 3	Kan. 4	Kan. 5						
Kan. 1	Kan. 2	Kan. 3	Kan. 4	Kan. 5	Kan. 6					
Kan. 1	Kan. 2	Kan. 3	Kan. 4	Kan. 5	Kan. 6	Kan. 7				
Kan. 1	Kan. 2	Kan. 3	Kan. 4	Kan. 5	Kan. 6	Kan. 7	Kan. 8			
Kan. 1	Kan. 2	Kan. 3	Kan. 4	Kan. 5	Kan. 6	Kan. 7	Kan. 8	Kan. 9		
	Kan. 2	Kan. 3	Kan. 4	Kan. 5	Kan. 6	Kan. 7	Kan. 8	Kan. 9	Kan. 10	
		Kan. 3	Kan. 4	Kan. 5	Kan. 6	Kan. 7	Kan. 8	Kan. 9	Kan. 10	Kan. 11
			Kan. 4	Kan. 5	Kan. 6	Kan. 7	Kan. 8	Kan. 9	Kan. 10	Kan. 11
				Kan. 5	Kan. 6	Kan. 7	Kan. 8	Kan. 9	Kan. 10	Kan. 11
					Kan. 6	Kan. 7	Kan. 8	Kan. 9	Kan. 10	Kan. 11
						Kan. 7	Kan. 8	Kan. 9	Kan. 10	Kan. 11

Tabelle 27.5: Kanalüberschneidungen bei DSSS

Die Kommunikation, die über den Regelsatz 6 (Kanal 6) läuft, wird von einer Station, die mit einem der Regelsätze 1 oder 11 arbeitet, nicht erkannt. Aus diesem Grund stehen in großen Infrastrukturumgebungen letztendlich nur drei Regelsätze zur Verfügung. Ein Angreifer muss dies wissen, um ein Störgerät – einen so genannten Jammer – aufstellen zu können. Aus Tabelle 27.5 geht eindeutig hervor, dass ein Jammer, der auf die Kanäle 5, 6 und 7 zielt, den größtmöglichen Schaden anrichten kann.

Das Jamming (d.h. das Hervorrufen von Störungen in einem 802.11b-kompatiblen Netzwerk) ist eigentlich recht einfach. Es sind mehrere unterschiedliche Geräte erhältlich, die ein Funknetz in die Knie zwingen können). Ein einfaches Bluetooth-Gerät etwa kann dem Administrator eines 802.11b-kompatiblen Netzwerks bereits Kopfschmerzen verursachen. Ich habe festgestellt, dass ein Bluetooth-Gerät, das sich im Umkreis von zehn Metern zu einem Funknetzgerät befindet, einen DoS hervorrufen kann. Das Gleiche gilt für einige Schnurlostelefone mit der durchaus gängigen Sendefrequenz von 2,4 GHz; das 2,4-GHz-Band wird zunehmend genutzt und allgemein als frei verfügbar betrachtet, weswegen es von allen möglichen Geräten benutzt wird.

Die von solchen Geräten erzeugten Signale werden von 802.11b-kompatiblen Geräten als Signalübertragungen anderer Netzwerkstationen betrachtet. Das heißt, die Geräte stellen ihren Sendebetrieb vorübergehend ein, bis das Signal nicht mehr vorhanden ist (bzw. bis Sie aufgelegt haben). Eine andere Möglichkeit besteht darin, dass die Geräte eine Steigerung hochfrequenter Einstreuungen verursachen, was dazu führt, dass 802.11b-Geräte auf eine langsamere Datenübertragungsrate umschalten. Frames werden dann immer wieder und wieder gesendet, um die Wahrscheinlichkeit zu erhöhen, dass die Gegenstelle sie auch empfangen kann. Wird genau eine Kopie jedes Frames gesendet, dann werden die Daten mit einer Geschwindigkeit von 11 Mbit/s übertragen. Fällt die Effizienz auf 50 Prozent, dann beträgt die Übertragungsrate zwar nach wie vor 11 Mbit/s; da aber jeder Frame zweimal gesendet wird, fällt die effektive Rate auf 5,5 Mbit/s. Es ist also ein beträchtlicher Leistungsabfall festzustellen, weil alle Frames in zweifacher Ausfertigung übertragen werden. Gleichzeitig kann es bei einer Zunahme hochfrequenter Störungen zu einer drastischen Zunahme beschädigter Frames kommen; auch in diesem Fall muss das beschädigte Paket vollständig neu übertragen werden.

27.7.6 Praktisches WEP-Cracking

Leider ist die WEP-Verschlüsselung von Grund auf mängelbehaftet, und deswegen lässt sie sich auch knacken. Trotzdem möchte ich Ihnen ans Herz legen, sie in all Ihren Funknetzen zu verwenden, denn Gelegenheitshacker lassen sich dadurch abwehren. Zudem stellt die WEP-Verschlüsselung eine weitere Maßnahme zum Schutz gegen das Knacken verschlüsselter Übertragungssignale dar.

Nach dieser Anmerkung wenden wir uns nun der praktischen Vorgehensweise zum Knacken der WEP-Verschlüsselung zu. Das Wichtigste, was Sie zum Knacken eines WEP-verschlüsselten Signals benötigen, ist Zeit. Je länger Sie Daten abfangen können, desto größer ist die Wahrscheinlichkeit, dass Sie einen Frame

erwischen, der ein Schlüsselbyte enthält. Die Chancen, dass dies geschieht, liegen bei fünf Prozent (manchmal auch bei 13 Prozent). Sie müssen etwa 5.000.000 Frames abfangen, um ein WEP-verschlüsseltes Signal knacken zu können. Zu diesem Zweck benötigen Sie einen Funknetz-Sniffer wie etwa AirSnort (`http://airsnort.shmoo.com/`) sowie eine Anzahl von Perl-Scripts, die – passenderweise – WEPCRACK heißen. Diese Scripts finden Sie online unter `http://sourceforge.net/projects/wepcrack/`.

Wenn Sie alle benötigten Tools zusammen haben, gehen Sie wie folgt vor, um ein WEP-verschlüsseltes Signal zu knacken:

1. Sammeln Sie mit Ihrem Funknetz-Sniffer Frames aus dem WEP-Signal. Wie bereits erwähnt, benötigen Sie etwa 5.000.000 Frames.
2. Führen Sie das Script *prism-getIV.pl* an der Eingabeaufforderung mit folgender Syntax aus:

   ```
   prism-getIV.pl dateiname
   ```

   Hierbei ist `dateiname` der Name der in Schritt 1 erstellten Datei. Wenn ein schwacher IV entdeckt wird, wird für eine spätere Verwendung eine Datei namens *IVFile.log* erstellt.
3. Nach der Erstellung der Datei *IVFile.log* müssen Sie das Script *WEPcrack.pl* ausführen. Das Script versucht nun anhand der in der Datei gespeicherten IVs den WEP-Schlüssel zu ermitteln.
4. Die Ausgabe des Scripts erfolgt im Dezimalformat. Holen Sie also eine Umrechnungstabelle aus den Tiefen Ihrer Schreibtischschublade, und beginnen Sie mit der Konvertierung in das Hexadezimalformat. Hier eine Beispielausgabe:

   ```
   95 = 5F
   211 = D3
   124 = 7C
   211 = D3
   232 = E8
   27 = 1B
   211 = D3
   44 = 2C
   42 = 2A
   53 = 35
   47 = 2F
   185 = B9
   48 = 30
   95:211:211:53:185:211:232:44:47:48:124:27:42 (Decimal)
   5F:D3:D3:35:B9:D3:E8:2C:2F:30:7C:1B:2A (HEX)
   ```

5. Geben Sie die Hexadezimalversion des Schlüssels in den Client Manager ein.

27.8 Fazit

Die explosionsartige Zunahme 802.11b-kompatibler Funknetze, die wir in der letzten Zeit beobachten konnten, hat den Zustand der Netzwerksicherheit um mehr als zehn Jahre zurückgeworfen. In vielen Fällen besteht das Ziel des Angreifers nicht einfach darin, in ein Funknetz einzubrechen und dessen Dienste zu nutzen, sondern auch darin, sich einen kostenlosen Internetzugang zu verschaffen oder einen Fuß in das angeschlossene leitungsbasierte Netzwerk zu bekommen. Wenn Sie also die Nutzung eines Funknetzes planen, dann sollte Sicherheit an oberster Stelle stehen. Sicherheitsadministratoren müssen zudem Maßnahmen zur Erkennung und Bekämpfung von Rogue-Access-Points und nicht autorisierten Clients implementieren.

Viele Hersteller bieten bereits Software für 802.11b-kompatible Netzwerk an, und wenn die Beliebtheit solcher Netze steigt, werden es wohl noch mehr werden. Die in diesem Kapitel beschriebenen und empfohlenen Produkte stellen zwar nur einen winzigen Ausschnitt aus dem überwältigenden Marktangebot dar, aber sie haben unsere Erwartungen übertroffen, und Sie können sie deswegen als Empfehlung des Autors betrachten. Natürlich sind alle Benutzer und alle Netzwerke anders. Bei der Entscheidung für ein Produkt sollten Sie deswegen auch die Anforderungen *Ihrer* Umgebung und Anwendungen berücksichtigen.

Die WEP-Verschlüsselung sollte in allen 802.11b-Netzwerken eingesetzt werden. Obwohl sie mängelbehaftet ist, bietet diese Technologie doch einen gewissen Schutz vor der Einsichtnahme in Ihre Netzwerkdaten und verringert die Anzahl der Angriffe gegen Ihr Netzwerk. Zwar ist es möglich, WEP zu knacken, aber der zeitliche Aufwand und die schiere Anzahl von Access-Points, die wegen des Fehlens von WEP leichter anzuzapfen sind, werden die meisten potenziellen Angreifer dazu bewegen, nach anderen Zielen zu suchen. Allerdings sollten Sie nicht allein auf WEP bauen; auch hier ist der traditionelle Sicherheitsansatz mit seinen unterschiedlichen Ebenen die empfehlenswerteste Vorgehensweise.

Praktisch jeder kann praktisch überall einen Angriff gegen ein Funknetz ausführen. Ob es der ältere Herr neben Ihnen im Fahrstuhl ist, der Eingaben an seinem PDA macht, oder die vier Twens, die Sie gerade mit Tempo 160 auf der Autobahn überholt haben, sie alle sind vielleicht gerade dabei, Ihr Netzwerk zu knacken. Wenn Sie keine Maßnahmen ergreifen, um solche Angriffe abzuwehren, dann können Sie dem Angreifer auch gleich den Büroschlüssel in die Hand drücken.