

Berufsakademie Stuttgart

- Fachrichtung Wirtschaftsinformatik -

Praxisbericht

Die Sicherheit drahtloser Netzwerke

Ausbildungsbetrieb: Ernst & Young AG
Wirtschaftsprüfungsgesellschaft
Mergenthalerallee 10-12
65765 Eschborn/Frankfurt am Main

Fachabteilung: IT-Security
Student: Sebastian Wolfgarten
Studienjahrgang: WWIG2002
Matrikelnummer: 129066
Datum der Erstellung: 15.02.03

Inhaltsverzeichnis

EINLEITUNG	3
TECHNISCHE GRUNDLAGEN	4
AD-HOC-MODUS	5
INFRASTRUKTUR-MODUS	6
SICHERHEITSMECHANISMEN	7
NETZWERKNAME (SSID BZW. ESSID)	8
MAC-ADRESSE	8
WEP-VERSCHLÜSSELUNG, INTEGRITÄTSSCHUTZ UND AUTHENTISIERUNG	9
SICHERHEITSPROBLEME	9
SICHERHEITSKRITISCHE GRUNDKONFIGURATION	9
UNSICHERE NETZWERKNAMEN (SSID)	10
MAC-ADRESSEN MANIPULATION	10
SCHWACHSTELLEN DES WEP-PROTOKOLLS	10
SCHLÜSSELMANAGEMENT	12
BEDROHUNG LOKALER DATEN	12
UNKONTROLLIERTE AUSBREITUNG DER FUNKWELLEN	12
BEDROHUNG DER VERFÜGBARKEIT	12
ANGRIFFSSZENARIOEN	13
UNAUTORISIERTE HARDWARE	13
ABFANGEN UND MANIPULATION DES DRAHTLOSEN NETZWERKVERKEHRS	13
FEHLKONFIGURATIONEN UND BEKANNTE SICHERHEITSLÜCKEN DER ACCESS POINTS	13
BLOCKIERUNG	14
CLIENT-CLIENT ATTACKE	14
LÖSUNGSANSÄTZE	16
KONFIGURATION UND ADMINISTRATION DER FUNKKOMPONENTEN	16
ÜBER DEN 802.11B-STANDARD HINAUSGEHENDE MAßNAHMEN	16
ORGANISATORISCHE MAßNAHMEN	16
FAZIT	18
ANHANG A – WARDRIVING	18
ANHANG B - LITERATURANGABEN	20
ANHANG C - KENNTNISNAHME	20

Einleitung

Computer beherrschen unsere Zeit, die multimediale Vernetzung unserer Welt scheint unaufhaltbar. Die Verfügbarkeit von Informationen spielt eine immer wichtigere Rolle; Mitarbeiter benötigen rund um die Uhr und von überall auf der Welt Zugriff auf unternehmensinterne Informationen.

In den Unternehmen sowie in zunehmenden Maße auch in Privathaushalten verbinden traditionelle lokale Netzwerke (Local Area Network, LAN) mehrere Computer mittels Kabel und dienen als Übertragungsmedien für Daten aller Art. Da sie ortsgebunden sind und einer starren Struktur unterliegen, benötigt jeder Computer, der Teil dieses Netzwerkes werden will, einen eigenen Anschluss an das Netzwerk. Die Umstrukturierung oder Expansion des Netzwerkes erfordert den Ausbau bzw. die Neukonzeption der gesamten Netzwerk-Infrastruktur, durch die erhebliche Kosten und ein immens hoher Zeit- und Arbeitsaufwand entstehen.

Die immer populärer werdenden drahtlosen, funkbasierten Netzwerke (Wireless LAN, WLAN) scheinen hier die Lösung des Problems zu sein, da diese nicht ortsgebunden sind. Die Geräte lassen sich außerdem verhältnismäßig einfach in Betrieb nehmen und sind, im Vergleich zum Aufbau einer kabelbasierten Netzwerkinfrastruktur, nicht mit besonders hohen Kosten verbunden. Des Weiteren lassen sich funkbasierte Endgeräte sehr leicht in kabelbasierte Netzwerke einfügen und ermöglichen somit eine dynamische Expansion des lokalen Netzwerkes. Ein Mitarbeiter kann innerhalb eines Unternehmens problemlos seinen eigenen Standort wechseln, ohne dass er auf seine gewohnte EDV-technische Arbeitsumgebung sowie auf den Zugriff auf Intra- und Internetdienste verzichten muss. Auch die räumliche Expansion eines Unternehmens in nahe gelegene Gebäudekomplexe, die meist mit dem Umzug einer ganzen Abteilung verbunden ist, ist durch die Verwendung von drahtlosen Netzwerken möglich, ohne dass hierbei erneut in den Aufbau einer kabelbasierten Netzwerkstruktur investiert werden muss. Zusätzlich kommen drahtlose Netzwerke in solchen Umgebungen zum Einsatz, in denen der Aufbau einer kabelbasierten Infrastruktur aufgrund ihrer Beschaffenheit, ihrer besonderen Funktion (z.B. Messen, Bahnhöfe, Flughäfen, Hotels, Bars etc.) oder ihrer enormen Größe nicht bzw. nur eingeschränkt möglich ist.

Technisch gesehen basieren fast alle derzeit auf dem Markt verfügbaren WLAN-Systeme (WaveLAN) auf einer Erweiterung namens 802.11b des 1999 vom Institute of Electrical and Electronics Engineers (IEEE) verabschiedeten Standard IEEE 802.11. Die flächendeckende und preisgünstige Verfügbarkeit der Endgeräte sorgt laut einer Studie des amerikanischen Marktforschungsunternehmens Allied Business Intelligence (ABI) seit Anfang 2000 für einen Verkaufsboom von Funknetzen und deren Zubehör, der im Jahr 2000 eine Stückzahl von knapp acht Millionen erreicht hat. Durch die zunehmende Verbreitung von funkbasierten Netzwerken konnte der Verkauf von drahtlosen Endgeräten im Jahre 2001 weltweit sogar auf etwa 24 Millionen Stück gesteigert werden und das Marktforschungsunternehmen ABI rechnet bis 2007 mit einer jährlichen Zuwachsrate von 43 Prozent.

Seit Mitte 2001 ist jedoch bekannt, dass die Funklan-Technologie neben den genannten Vorteilen auch eine ganze Reihe von Nachteilen mit sich bringt, die zu massiven Sicherheitsproblemen führen. Obwohl die Sicherheitslücken veröffentlicht worden sind, konnten sich die Hersteller bisher nicht auf eine gemeinsame Lösung einigen, die die Sicherheitsrisiken der drahtlosen Vernetzung vollständig behebt. Die Identifizierung, Ausnutzung und Beseitigung der Sicherheitslücken funkbasierter Netzwerke sind Themen dieser Praxisarbeit. Schließlich werden genaue Hinweise und Verbesserungsvorschläge zur Erhöhung der eigenen Netzwerksicherheit gegeben und die bekanntesten Werkzeuge vorgestellt, die zum Eindringen in funkbasierte Netzwerke verwendet werden.

Technische Grundlagen

Die Abkürzung WLAN steht für Wireless Local Area Network und bezeichnet ein funkbasiertes lokales Netzwerk. Dabei basieren fast alle derzeit auf dem Markt verfügbaren und gängigen Systeme auf einer 1999 erschienenen Erweiterung namens 802.11b (auch WiFi genannt) des 1997 vom Institute of Electrical and Electronics Engineers (IEEE) verabschiedeten Standard IEEE 802.11. Die drahtlosen Netzwerke benutzen den lizenzfreien Frequenzbereich von 2,4 bis 2,48 Ghz und bieten, je nach Umgebung und Betriebsart, eine Reichweite von 30 Metern in geschlossenen Gebäuden und bis zu 300 Metern in freien Umgebungen. In Deutschland stehen insgesamt 13 Frequenzkanäle mit je einer maximalen Übertragungsgeschwindigkeit von 11 Mbit/Sekunde zur Verfügung, wobei in der Praxis Geschwindigkeiten von 1 bis 5,5 Mbit/Sekunde realistisch sind. Die folgende Tabelle zeigt, welche genauen Frequenzen innerhalb des Frequenzbandes für drahtlose Kommunikation verwendet werden können. Beachtenswert ist, dass eigentlich 14 Funkkanäle vorgesehen sind, aber durch länderspezifische Gegebenheiten diese nicht global verwendet werden können. So sind beispielsweise Kanal 12 und 13 in den USA schon belegt und Kanal 14 ist nur in Japan verfügbar. Daher beschränken sich einige Hersteller auf den Frequenzbereich, der den Funkkanälen 1-11 entspricht. Dies ist gegebenenfalls beim Aufbau eines drahtlosen Netzwerkes zu berücksichtigen:

Kanal	Frequenzbereich (in Ghz)	Länder
1	2,412	Europa (außer Frankreich und Spanien), USA
2	2,417	Europa (außer Frankreich und Spanien), USA
3	2,422	Europa (außer Frankreich und Spanien), USA
4	2,427	Europa (außer Frankreich und Spanien), USA
5	2,432	Europa (außer Frankreich und Spanien), USA
6	2,437	Europa (außer Frankreich und Spanien), USA
7	2,442	Europa (außer Frankreich und Spanien), USA
8	2,447	Europa (außer Frankreich und Spanien), USA
9	2,452	Europa (außer Frankreich und Spanien), USA
10	2,457	Europa, USA
11	2,462	Europa, USA
12	2,467	Europa (außer Spanien)
13	2,472	Europa (außer Spanien)
14	2,477	Japan

Tabelle 1: Funkkanäle, Frequenz- und Geltungsbereiche des 802.11b-Standards

In Deutschland stehen im 2,4 Ghz-Frequenzbereich 13 Frequenzkanäle mit einem Frequenzabstand von 5 Mhz (siehe Tabelle) zur Verfügung. Bei einer Kanalbandbreite von ca. 22 Mhz können jedoch nur drei Kanäle gleichzeitig überlappungsfrei genutzt werden, wie die folgende Darstellung veranschaulicht:

Die Sicherheit drahtloser Netzwerke

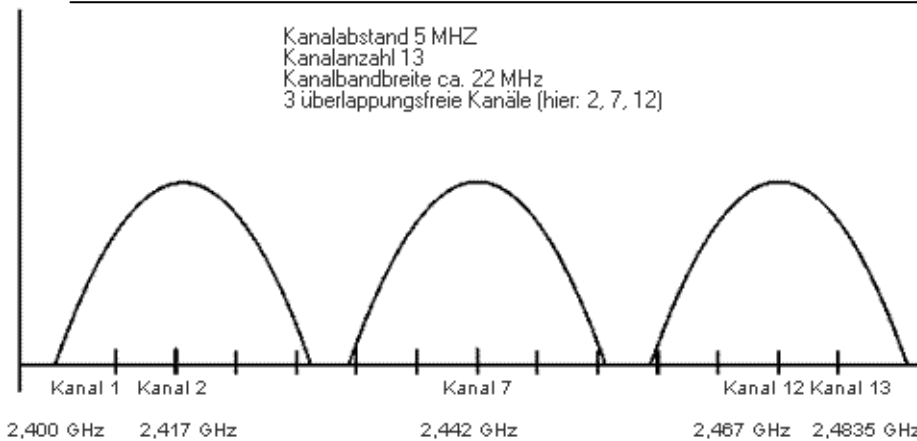


Abbildung 1: Kanalaraster und überlappungsfreie Kanäle
(Bildmaterial: Bundesamt für Sicherheit in der Informationstechnik, <http://www.bsi.bund.de>)

In diesem Beispiel können die Kanäle zwei, sieben und zwölf überlappungsfrei genutzt werden. Sollten sich Kanäle überlappen, kann es zu erheblichen Störungen des Funknetzwerkes (siehe Abschnitt „Bedrohung der Verfügbarkeit“) kommen. Beim Betrieb von WLANs unterscheidet man prinzipiell zwei verschiedene Betriebsmodi, die ich kurz erläutern möchte:

Ad-hoc-Modus

Der so genannte Ad-hoc-Modus bezeichnet einen Betriebsmodus, in dem die Kommunikation zwischen den einzelnen Teilnehmern (Clients) untereinander ohne zentrale Verbindungsstelle (Access Point) erfolgt. Ein Datenaustausch findet direkt statt, weshalb diese Betriebsart auch Peer-to-Peer-Modus (Kommunikation zwischen Endgerät und Endgerät) oder Independent Basic Service Set (IBSS) genannt wird. In der Praxis findet man im Ad-hoc-Modus betriebene Funknetzwerke relativ selten, da diese oft nur temporär installiert werden, um kurzzeitig einen Datenaustausch (z.B. während eines Meetings) zu realisieren und danach wieder abgeschaltet oder fortan im Infrastruktur-Modus betrieben werden. Des Weiteren kann es bei der direkten Verbindung zwischen zwei Endgeräten zu Problemen kommen, da der Ad-hoc-Modus weniger stark standardisiert ist als der Infrastruktur-Modus und die einzelnen Hersteller teilweise unterschiedliche, zueinander nicht kompatible Systeme verwenden. Die folgende Darstellung veranschaulicht die Funktionsweise eines drahtlosen Netzwerkes im Ad-hoc-Modus:

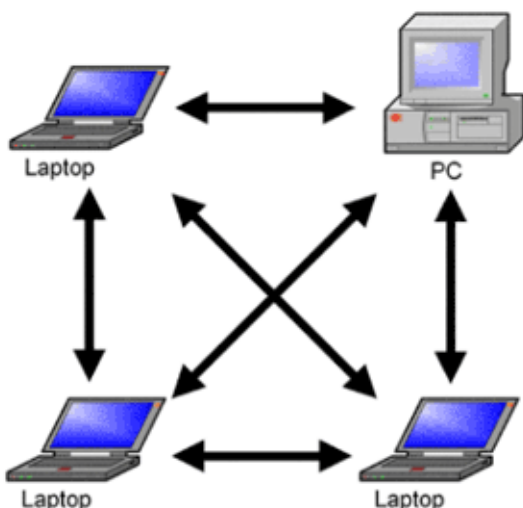


Abbildung 2: Funktionsweise eines im Ad-hoc-Modus betriebenen Funknetzwerkes
(Bildmaterial: Networkers Aktiengesellschaft, <http://www.networkers.de>)

Die Kommunikation der einzelnen Endgeräte (z.B. PCMCIA-Karte für Notebook und PCI-Karte mit Adapter für PC) erfolgt direkt und ohne eine zentrale Vermittlungsstelle (Access Point). In der Praxis findet man jedoch häufiger eine andere Betriebsart:

Infrastruktur-Modus

Im so genannten Infrastruktur-Modus findet die Kommunikation zwischen zwei drahtlosen Endgeräten nur über eine zentrale Vermittlungsstelle, einem so genannten Access Point (AP), statt. Zwischen den einzelnen Endgeräten findet, im Gegensatz zum Ad-hoc-Modus zu keinem Zeitpunkt eine direkte Datenübertragung statt. Ähnlich wie bei einem Mobiltelefon bildet dabei jeder Access Point eine Funkzelle und die Endgeräte (Clients) sind nur solange Teilnehmer dieses Netzwerkes, wie sie sich innerhalb der Reichweite der Funkzelle befinden. Der Infrastruktur-Modus, der mindestens zwei drahtlose Endgeräte über einen Access Point verbindet, wird auch als Basic Service Set (BSS) bezeichnet und findet insbesondere in Firmennetzwerken sowie professionellen Heimnetzwerken Verwendung. Das folgende Schaubild zeigt die Funktionsweise eines drahtlosen Netzwerkes im Infrastruktur-Modus:

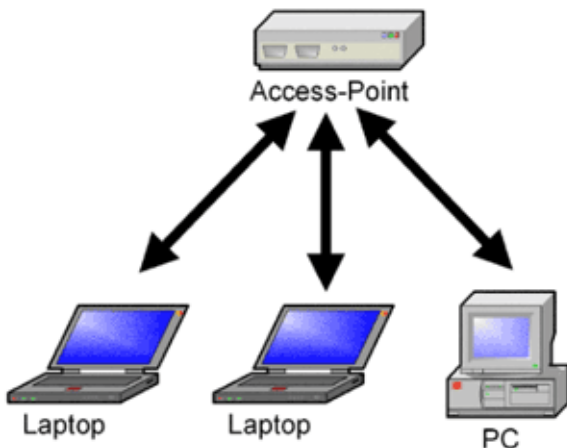


Abbildung 3: Funktionsweise eines im Infrastruktur-Modus betriebenen Funknetzwerkes (Bildmaterial: Networkers Aktiengesellschaft, <http://www.networkers.de>)

Die Kommunikation der einzelnen Endgeräte (z.B. PCMCIA-Karte für Notebook und PCI-Karte mit Adapter für PC) erfolgt über den Access Point, der als zentrale Funkbrücke fungiert und die Daten der angeschlossenen Geräte entgegennimmt und verteilt. Ebenso ist über einen Access Point eine Verbindung von einem funkbasierten Endgerät in ein kabelgebundenes Segment des lokalen Netzwerkes (LAN) möglich, wie das folgende Schaubild darstellt:

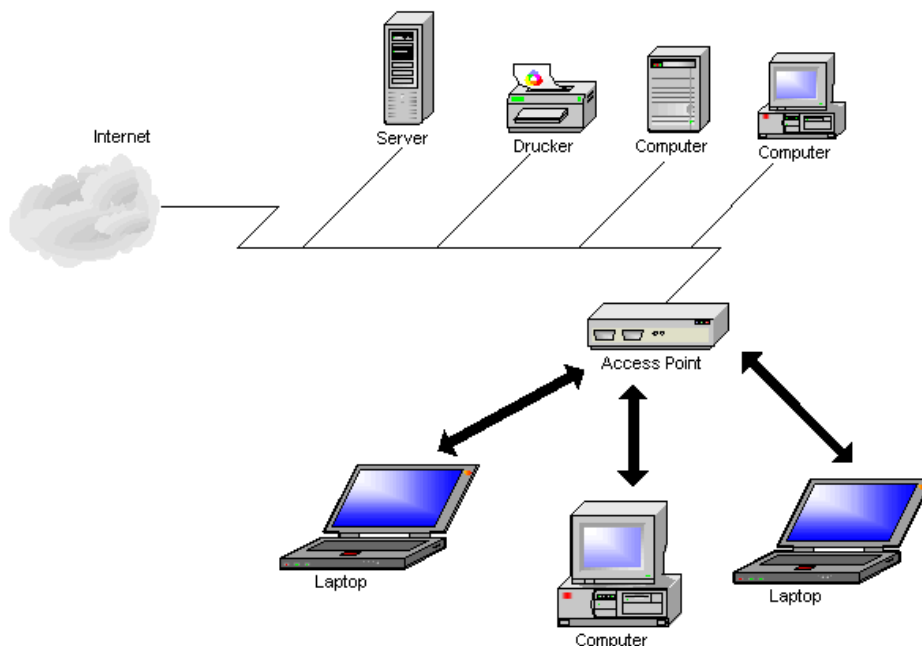


Abbildung 4: Schematische Darstellung eines funkbasierten Netzwerkes (WLAN) mit Anschluss an ein lokales Netz (LAN)

Diese Konstellation findet man gerade in Firmennetzwerken sehr häufig, da viele Firmen bereits über eine bestehende, kabelgebundene Netzwerkinfrastruktur verfügen und durch funkbasierte Geräte ihr eigenes Netzwerk dynamisch an unternehmensinterne Ereignisse (z.B. Umzug in ein anderes Gebäude, Mitarbeiterzuwachs etc.) anpassen. Häufig werden drahtlose Netzwerke auch aus Kostengründen, zur Anbindung von Benutzern mit tragbaren Computern (Notebooks) oder zu Testzwecken angeschafft. Eine Verbindung in das kabelgebundene Netzwerk und den dort verfügbaren Informationen und Anwendungen ist oftmals unerlässlich und erfordert deshalb den Einsatz einer zentralen Vermittlungsstelle (Access Point) zwischen dem funkbasierten sowie dem drahtgebundenen Netzwerk, die nur im Infrastruktur-Modus möglich ist. Des Weiteren ermöglicht der Infrastruktur-Modus durch die Installation mehrerer Access Points eine flächendeckende Versorgung von großen Bereichen, da durch die sich überlappenden Funkzellen die Funkverbindung auch beim Übergang eines Clients in die nächste Funkzelle aufrecht erhalten werden kann. Dieser Vorgang heisst Roaming und wird in sehr ähnlicher Form auch im Mobilfunk eingesetzt. Weiterhin können zwei Access Points auch als Brücke (Bridge) zwischen zwei leitungsgebundenen lokalen Netzwerken eingesetzt werden. Ebenso kann ein Access Point auch als Relaisstation (Repeater) fungieren, um die Reichweite eines drahtlosen Netzwerkes zu erhöhen. Schließlich kann bei Verwendung entsprechender Komponenten (z.B. Richtantennen) an den Access Points ein funkbasiertes Netzwerk auch zur Vernetzung von Liegenschaften (z.B. entfernten Niederlassungen) eingesetzt werden. In diesem Fall ist eine Reichweite von mehreren Kilometern möglich, die Access Points können dabei als Relaisstation (Repeater) oder Brücke eingesetzt werden.

Sicherheitsmechanismen

Um in ein kabelgebundenes lokales Netzwerk physikalisch einzudringen, muss ein Angreifer in der Regel Zutritt zu einem Gebäude und entsprechenden Zugriff auf zentrale Verbindungsstellen (z.B. Hubs, Switches oder Netzwerkdozen) haben. Erst wenn es ihm gelingt, einen lokalen Netzwerkanschluss zu erhalten, ist er in der Lage, Teil des Netzwerkes zu werden und dieses gezielt zu attackieren.

Aufgrund der Beschaffenheit (Funkwellen) eines drahtlosen Netzwerkes sind die Sicherheitsprobleme, denen ein solches Netzwerk ausgesetzt ist, in keinster Weise mit denen eines leitungsgebundenen Netzwerkes zu vergleichen. Während der Datenfluss in einem kabelgebundenen Netzwerk durch die fest installierte Infrastruktur unveränderbar vorgegeben ist, lässt sich die Ausbreitung der elektromagnetischen Wellen und der damit verbundene Datenfluss in einem funkbasierten Netzwerk kaum begrenzen. Ein Angreifer muss sich also nur in die Nähe einer Funkzelle begeben und nicht zwingend innerhalb eines Gebäudes aufhalten, um potenziellen Zugriff auf das drahtlose Netzwerk und ein eventuell dahinterliegendes, kabelgebundenes, lokales Netzwerk zu erhalten. Die folgende Abbildung zeigt ein kabelgebundenes, lokales Netzwerk mit einem drahtlosen Netzwerksegment, dessen Reichweite über die Gebäudebegrenzung hinweg reicht und somit Angreifern einen guten Angriffspunkt auf das gesamte Netzwerk zur Verfügung stellt:

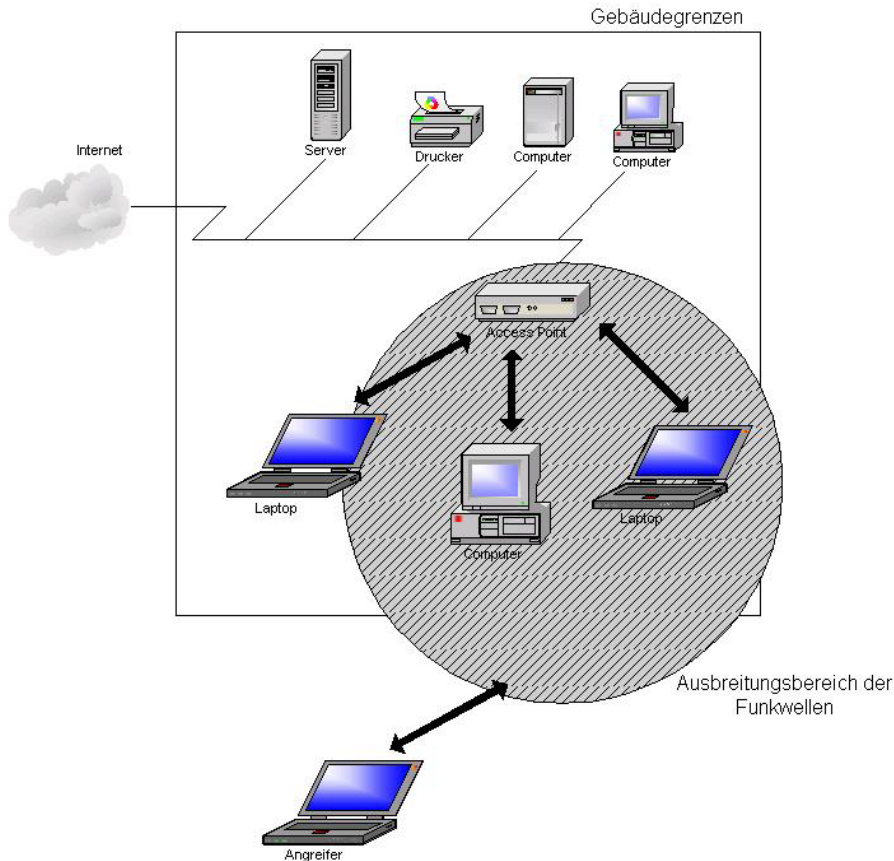


Abbildung 5: Darstellung eines lokalen Netzwerkes mit einem funkbasierten Netzwerkbereich, dessen Reichweite die Gebäudemauern überschreitet

Die besonderen Eigenschaften von Funknetzen und die daraus resultierenden, potenziellen Schwachstellen sind bei der Entwicklung der drahtlosen Netzwerktechnik in besonderem Maße berücksichtigt worden. Der Standard 802.11b sieht die folgenden Sicherheitsmechanismen vor:

1. Netzwerkname (SSID bzw. ESSID)

Jedem Funknetz kann ein eigener Netzwerkname, die so genannte SSID (Service Set Identity) bzw. ESSID (Extended Service Set Identity), zugewiesen werden. Der Sinn dieser Maßnahme besteht darin, dass nur solche Clients am Netzwerk teilnehmen können, die den Namen des Netzwerkes (SSID) kennen. Wenn jeder Client sich mit einem Access Point verbinden können soll (z.B. öffentlicher Hotspot am Flughafen), wird als Netzwerkennung der Begriff „Any“ verwendet. Da der Netzwerkname im Klartext über das Netz gesendet wird, kann ein Angreifer den Namen schnell herausfinden (Stichwort: WarDriving, siehe Anhang) und somit unerwünschterweise Teilnehmer des Netzwerkes werden, sofern keine zusätzlichen Sicherheitsvorkehrungen vorhanden sind. Der durch die SSID erzielte Schutz ist also faktisch unwirksam.

2. MAC-Adresse

Jede Netzwerkkarte verfügt über eine vom Hersteller vergebene, eindeutige Hardwareadresse. Die so genannte MAC-Adresse (Media Access Control) identifiziert die Netzwerkkarte eindeutig und unverwechselbar. Einige Access Points unterstützen deshalb die Erstellung einer Positiv-Liste von MAC-Adressen, die sich mit dem Access Point verbinden und somit Teilnehmer des Funknetzwerkes werden dürfen. Da die Liste der erlaubten MAC-Adressen manuell gepflegt werden muss, ist ein nicht unerheblicher Aufwand erforderlich, der die Verwendung von Positiv-Listen auf Basis der MAC-Adressen in vielen Einsatzszenarien unmöglich macht. Außerdem lassen sich die MAC-Adressen (z.B. 00:40:CA:BE:82:30) durch den Einsatz spezieller Software (z.B. ifconfig unter Unix/Linux und smac unter Microsoft Windows) bewusst fälschen und bieten somit keinen ausreichenden Schutz.

3. WEP-Verschlüsselung, Integritätsschutz und Authentisierung

Der wichtigste, obgleich optionale Sicherheitsmechanismus in drahtlosen Netzwerken heißt „Wired Equivalent Privacy“ (WEP). Das Protokoll verwendet ein symmetrisches Verschlüsselungsverfahren, d.h. Sender und Empfänger einer verschlüsselten Nachricht nutzen denselben Schlüssel zur Kodierung bzw. Dekodierung der Nachricht, und es soll die Vertraulichkeit, Integrität und die Authentizität der drahtlos übertragenen Daten und Informationen sicherstellen. Das WEP-Verfahren arbeitet mit zwei Verschlüsselungslängen (64 und 128 Bit), und der Schlüssel setzt sich aus einem statisch berechneten, 24-Bit umfassenden Initialisierungsvektor (IV) sowie dem eigentlichen geheimen Schlüssel von 40 bzw. 104-Bit zusammen. Um ein Datenpaket zu übertragen, wird zunächst eine Prüfsumme (Integritätscheck, IC) nach dem CRC 32-Verfahren (Cyclic Redudancy Check) gebildet, um zu verhindern, dass ein Angreifer die Daten während des Versands manipuliert. Danach wird aus dem geheimen WEP-Schlüssel und dem Initialisierungsvektor nach dem so genannten RC4-Verfahren ein Schlüsselstrom gebildet, der mittels der logischen XOR-Funktion (exklusives ODER) mit der Prüfsumme verknüpft wird. Die Daten werden übertragen, in dem zuerst der Initialisierungsvektor im Klartext übertragen wird, gefolgt von den verschlüsselten Daten. Der Empfänger der Daten muss aus dem Initialisierungsvektor und dem ihm bekannten WEP-Schlüssel den RC4-Schlüsselstrom erzeugen, um schließlich durch eine logische XOR-Funktion die Daten zu entschlüsseln. Die folgende Abbildung zeigt die Funktionsweise einer Datenübertragung nach dem WEP-Verfahren:

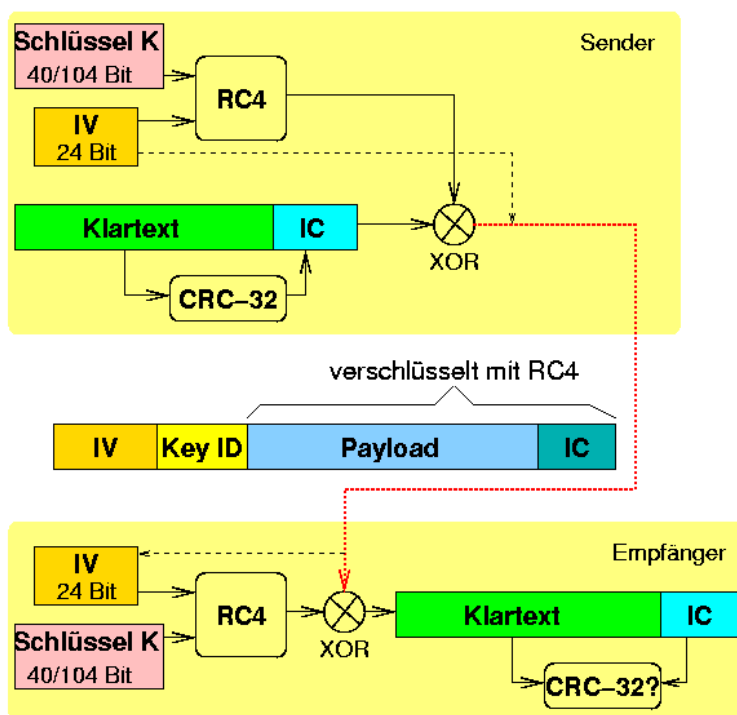


Abbildung 6: Funktionsweise des WEP-Verfahrens
 (Bildmaterial: Technische Universität Chemnitz, <http://www.tu-chemnitz.de>)

Sicherheitsprobleme

Die vorgestellten Sicherheitsmechanismen sind überwindbar und stellen heute keinen ausreichenden Schutz dar. Die Schwachstellen drahtloser Funknetzwerke sind im einzelnen:

1. Sicherheitskritische Grundkonfiguration

Viele Hersteller liefern ihre drahtlosen Endgeräte in einer bedenklichen Grundkonfiguration aus und deaktivieren eventuell vorhandene Sicherheitsmechanismen (z.B. WEP), ohne auf

mögliche Gefahren und eventuell vorhandene Lösungsansätze hinzuweisen. Die Endanwender wissen oft nicht über die Gefahren einer ungesicherten Kommunikation Bescheid und vertrauen in Puncto Sicherheit auf die Vorgaben des jeweiligen Herstellers, so dass die Sicherheit und Integrität der übertragenen Daten nicht sichergestellt sind.

2. Unsichere Netzwerknamen (SSID)

Der Netzwerkname (SSID) dient eigentlich der Beschreibung und Identifizierung eines drahtlosen Netzwerkes. Aus Unwissenheit wählen viele Anwender jedoch einen ungünstigen Netzwerknamen (z.B. Arztpraxis, Anwalt, Büro oder Internet), der pikante Details (z.B. Firmennamen, Funktion oder Standort eines Netzwerkes etc.) verrät und somit Angreifer zusätzlich anlockt. Außerdem weisen viele Hersteller ihre Kunden nicht darauf hin, dass die werksseitig vorgegebenen Netzwerknamen (z.B. default, tsunami) vor Inbetriebnahme geändert werden sollten, damit Angreifern der Zugriff auf das Funknetz erschwert wird.

3. MAC-Adressen Manipulation

Die in einigen Access Points eingebauten MAC Adressen-Filter, die verhindern sollen, dass sich unbekannte Endgeräte unerlaubterweise Zugang zu einem funkbasierten Netzwerk verschaffen, sind überwindbar. Durch eine spezielle Software (Sniffer, z.B. ethereal), die den Netzwerkverkehr aufzeichnet und mitschneidet, können die MAC-Adressen der Endgeräte identifiziert werden, denen es erlaubt ist, eine Verbindung mit dem Access Point aufzubauen. Indem ein Angreifer sich manuell eine erlaubte MAC-Adresse zuweist und das ursprünglich mit dieser MAC-Adresse versehene Endgerät gezielt attackiert, kann dieser den MAC Adressen-Filter umgehen. Generell sind die MAC Adressen-Filter in den meisten Access Points nicht vorhanden bzw. in der Grundkonfiguration deaktiviert.

4. Schwachstellen des WEP-Protokolls

Um die Vertraulichkeit der übertragenen Daten zu gewährleisten, verwendet das WEP-Protokoll den Verschlüsselungs-Algorithmus RC4. Dieser Algorithmus ist ein so genannter Stromchiffre, d.h. jedes Zeichen wird einzeln verschlüsselt, und er wurde 1987 von Ron Rivest der RSA Data Security entwickelt. 1994 wurde der bis dato geheim gehaltene Algorithmus im Internet veröffentlicht und wird seitdem in vielen kommerziellen (z.B. Lotus Notes, Oracle Secure SQL) sowie freien Softwareprodukten (z.B. OpenSSL) verwendet. Er verwendet Schlüssel mit variabler Länge zwischen 1 und 2048 Bit und gilt, wie jeder Stromchiffre, als unsicher, wenn ein Schlüssel mehrfach zur Verschlüsselung eingesetzt wird. Wie bereits vorgestellt, werden im WEP-Verfahren die Daten paketweise und in Abhängigkeit von einem Schlüssel und einem Initialisierungsvektor (IV) in Chiffpratdaten umgewandelt. Der Schlüssel ist dabei eine Zeichenkette von wahlweise 40 oder 104 Bit und muss den am Funknetz beteiligten Clients sowie dem Access Point vorab zur Verfügung gestellt werden, wobei für das gesamte Netzwerk ein gemeinsamer Schlüssel verwendet wird. Aufgrund der Tatsache, dass innerhalb des gesamten Netzwerkes nur ein gemeinsamer Schlüssel verwendet wird und aufgrund des allgemeinen Aufbaus des WEP-Verfahrens ergeben sich deshalb konkret die folgenden Schwachstellen:

- Eine Schlüssellänge von 40 Bit ist viel zu kurz. Mit nur einem mitgeschnittenen Teil des Chiffrats kann das gesamte Chiffrat mit einem handelsüblichen Computer innerhalb weniger Tage mit sämtlichen infrage kommenden Schlüsseln verglichen werden, um den korrekten Schlüssel zu errechnen (Brute Force-Attacke). Sobald ein Angreifer den korrekten Schlüssel gefunden hat, ist dieser in der Lage, den gesamten Netzwerkverkehr des drahtlosen Netzwerkes mitzulesen, bis der Schlüssel durch den Betreiber des Funknetzes gewechselt wird, sofern dies überhaupt geschieht. Bei einer Schlüssellänge von 104 Bit ist jedoch aus heutiger Sicht ein ausreichender Schutz gegen solche Brute Force-Attacken gewährleistet.
- Die Gesamtlänge des im Klartext übertragenen Initialisierungsvektors (IV) ist mit 24 Bit zu kurz. Da im WEP-Verfahren mit RC4 ein Stromchiffrier-Algorithmus zum Einsatz kommt, kann die Datenübertragung nur dann sicher sein, wenn der generierte Bitstrom für je zwei Datenpakete unterschiedlich ist. Sobald zwei Mal mit demselben Bitstrom

Die Sicherheit drahtloser Netzwerke

verschlüsselt wurde, lassen sich sowohl die beiden Datenpakete als auch der Bitstrom in vielen Fällen rekonstruieren. Da sich der Bitstrom aus dem Schlüssel und dem Initialisierungsvektor berechnet und der Schlüssel für längere Zeit als konstant angenommen werden kann, kann es ausreichend sein, zwei verschlüsselte Datenpakete mit demselben Initialisierungsvektor abzufangen, um diese zu entziffern. Aufgrund der Tatsache, dass der Initialisierungsvektor nach einem fest stehenden Algorithmus nach jedem neuen Paket verändert wird, bedeutet dies, dass spätestens nach 2^{24} , d.h. nach ca. 16,7 Millionen Datenpaketen wieder mit der gleichen Abfolge von Initialisierungsvektoren begonnen wird und der Verschlüsselung der folgenden Pakete die gleichen Zeichenfolgen zugrundeliegen. Ein Angreifer kann also ab diesem Zeitpunkt mit einer hohen Wahrscheinlichkeit den gesamten Netzwerkverkehr mitlesen. Die Problematik der zu kurzen Initialisierungsvektoren betrifft Schlüssellängen von 40 und 104 Bit gleichermaßen.

- Bereits im Jahr 2001 brachte ein Team von Wissenschaftlern der University of California, Berkeley, eine Untersuchung heraus, die eine Reihe von Schwachstellen des WEP-Protokolls aufdeckte. Die Wissenschaftler Fluhrer, Mantin und Shamir fanden heraus, dass es so genannte schwache Initialisierungsvektoren gibt, die mit einer fünfprozentigen Trefferwahrscheinlichkeit Hinweise auf ein Byte des Schlüssels geben und somit die komplette Entschlüsselung des WEP-Schlüssels ermöglichen. Um einen Angriff erfolgreich durchzuführen, muss ein Angreifer etwa vier bis sechs Millionen Datenpakete des Funknetzes passiv abhören. Dabei ist die für den Angriff benötigte Zeit nicht nur von der Anzahl der abzuhörenden Pakete abhängig, sondern im Wesentlichen auch von der durchschnittlichen Paketgröße und Auslastung des Access Points. Die folgenden Tabellen zeigen eine Abschätzung der Dauer eines passiven Angriffs in Abhängigkeit der benötigten Datenmenge, der Anzahl der Pakete und der durchschnittlichen Paketgröße:

Anzahl Datenpakete	Paketgröße:		
	512 Byte	1024 Byte	2048 Byte
2.000.000	0,95 GB	1,91 GB	3,81 GB
4.000.000	1,91 GB	3,81 GB	7,63 GB
6.000.000	2,86 GB	5,72 GB	11,44 GB
8.000.000	3,81 GB	7,63 GB	15,26 GB

Tabelle 2: Benötigte Datenmenge in Abhängigkeit von der durchschnittlichen Paketgröße und der Anzahl der Pakete
(Quelle: Bundesamt für Sicherheit in der Informationstechnik, <http://www.bsi.bund.de>)

Abgehörte Datenmenge	Auslastung:		
	5 Mbit/s	1 Mbit/s	0,1 Mbit/s
0,95 GB	3 Minuten	16 Minuten	2,70 h
1,91 GB	7 Minuten	33 Minuten	5,43 h
2,86 GB	10 Minuten	49 Minuten	8,14 h
3,81 GB	13 Minuten	65 Minuten	10,84 h
5,72 GB	20 Minuten	98 Minuten	16,27 h
7,63 GB	26 Minuten	130 Minuten	21,70 h
11,44 GB	39 Minuten	195 Minuten	32,54 h
15,26 GB	52 Minuten	260 Minuten	43,41 h

Tabelle 3: Benötigte Zeit in Abhängigkeit von der Datenmenge und der durchschnittlichen Auslastung des Access-Points
(Quelle: Bundesamt für Sicherheit in der Informationstechnik, <http://www.bsi.bund.de>)

Die Tabellen zeigen, dass es einem Angreifer möglich ist, den kompletten WEP-Schlüssel zu ermitteln, wenn er ausreichend schwache Initialisierungsvektoren (ca. 1500) gefunden hat. Bei einer durchschnittlichen Paketgröße von 1024 Byte und einer Gesamtmenge von ca. vier Millionen Datenpaketen sind demnach etwa 3,81 GB an abgehörten Daten notwendig, um einen erfolgversprechenden Angriff auf den RC4-Algorithmus durchführen zu können. Bei einem Access Point mit einer mittleren Auslastung von 5 Mbit/s benötigt der Angriff etwa 65

Minuten.

- Prinzipiell ist ein Angreifer in der Lage, Datenpakete zu fälschen. Der von der Stromchiffre generierte Bitstrom ist abhängig von dem verwendeten Schlüssel und dem Initialisierungsvektor. Gelangt ein Angreifer in den Besitz eines einzigen dieser generierten Bitströme, so kann er bis zum nächsten Schlüsselwechsel beliebige Datenpakete fälschen, d. h. korrekte Chiffre erzeugen. Weiterhin ist es ihm möglich, die verschlüsselten Daten durch eine XOR-Funktion zu berechnen, falls ihm zu einem abgehörten Chiffre die Klardaten bekannt sind („Known Plaintext Attack“).
- Die bei der Verschlüsselung erzeugte Prüfsumme ist wirkungslos, da ein Angreifer durch gezielte Manipulation der Chiffre die verschlüsselte CRC-Prüfsumme so ändern kann, dass es dem Empfänger nicht möglich ist, die Manipulation zu erkennen. Der Grund für diese Schwachstelle ist die Verwendung einer einfachen XOR-Funktion im Stromchiffrier-Algorithmus des WEP-Protokolls und die Linearität der CRC-Summe.

5. Schlüsselmanagement

Eine weitere Schwachstelle des WEP-Verfahrens ist das nicht vorhandene Schlüsselmanagement. Die WEP-Schlüssel müssen manuell im Netz verteilt werden, d.h. in jedem Access Point und drahtlosen Endgerät (Client) muss der gleiche Schlüssel per Hand eingetragen werden, da ein automatisiertes Verfahren zur Verteilung der Schlüssel im gesamten Netzwerk nicht existiert. Die manuelle Vorgehensweise ist sehr zeitaufwändig und erfordert physikalisch Zugriff auf die einzelnen Komponenten, so dass in der Praxis der geheime WEP-Schlüssel selten oder überhaupt nicht gewechselt wird. Sobald ein Angreifer den Schlüssel geknackt hat, weil er beispielsweise in den Besitz eines Clients des Netzwerkes gelangt ist oder den Schlüssel mittels frei erhältlicher Werkzeuge herausgefunden hat, kompromittiert er das gesamte Funknetz und die Sicherheit der übertragenen Daten sowie aller an den jeweiligen Access Point angeschlossenen, drahtlosen und kabelgebundenen Teilnehmer ist nicht mehr gewährleistet.

6. Bedrohung lokaler Daten

Die lokalen Daten der Teilnehmer eines drahtlosen Netzwerkes sind, gerade in öffentlich zugänglichen Bereichen (z.B. Flughäfen, Bahnhöfe, Bars) und in solchen Netzwerken, die im Ad hoc-Modus betrieben werden, besonderen Risiken ausgesetzt, da lokale Datei- und Druckerfreigaben in der Grundeinstellung vieler Betriebssysteme (z.B. Microsoft Windows 2000) auch über funkbasierte Verbindungen angesprochen werden können. Ein unerlaubter Zugriff auf lokale Dateien und Verzeichnisse sowie eine gezielte Ausnutzung bekannter Sicherheitslücken des durch einen Teilnehmer des Funknetzes verwendeten Betriebssystems sind möglich.

7. Unkontrollierte Ausbreitung der Funkwellen

Die Funkwellen drahtloser Geräte breiten sich fast unkontrolliert aus und reichen meist weit außerhalb der gewollten Nutzreichweite. Physikalische Grenzen (z.B. Gebäudemauern) werden oft ohne Kenntnisse der Betreiber überschritten, wodurch eine akute Abhörgefahr entsteht.

8. Bedrohung der Verfügbarkeit

Wenn sich andere elektromagnetische Quellen (z.B. Mikrowellen) in der Reichweite eines drahtlosen Netzwerkes befinden, kann die Kommunikation der einzelnen drahtlosen Geräte stark gestört und im Extremfall sogar vollständig verhindert werden. Dies kann auch unbeabsichtigt durch andere technische Systeme (z.B. Bluetooth-Geräte, andere Funk-LANs, medizinische Geräte, etc.) oder durch absichtliches Betreiben einer Störquelle (Jammer) als so genannter Denial-Of-Service-Angriff erfolgen.

Angriffsszenarien

Die möglichen Angriffe auf drahtlose Funknetzwerke lassen sich prinzipiell in fünf Hauptkategorien einteilen:

- **Unautorisierte Hardware (engl.: insertion attack)**

Die Gefahr durch unautorisierte Hardware besteht in dem Anschluss von drahtlosen Geräten (z.B. Access Points) an das Firmennetz, die zuvor keinen firmeninternen Sicherheitsprozess durchlaufen haben, beziehungsweise keiner Sicherheitsüberprüfung durch den Systemadministrator unterzogen worden sind. Dabei kann die unautorisierte Hardware entweder durch den Angreifer selbst oder einen unbedachten Firmenmitarbeiter installiert werden, der beispielsweise die Reichweite eines drahtlosen Netzwerkes nach seinen Wünschen vergrößern oder überhaupt ein drahtloses Netzwerk in Betrieb nehmen möchte. Ein unerlaubt installierter Access Point wird Rogue Access Point (verbrecherischer Zugangspunkt) genannt, weil ein Angreifer dadurch die gesamten Sicherheitsvorkehrungen einer Firma unterwandern kann. Sobald ein Angreifer einen solchen Zugangspunkt zum Netzwerk gefunden hat, wird dieser durch den unautorisierten Einsatz von Clients versuchen, mit seinem drahtlosen Endgerät eine Verbindung zu einem Access Point des Firmennetzes aufzubauen und von dort in das gesamte (Firmen-) Netzwerk einzudringen.

- **Abfangen und Manipulation des drahtlosen Netzwerkverkehrs (engl.: interception and monitoring wireless traffic)**

Das Abhören und die Manipulation von Daten ist eine beliebte Attacke in drahtgebundenen und drahtlosen Netzwerken. Durch so genannte Snifferprogramme (z.B. ethereal, AiropEEK) bzw. Netzwerk-Analyseprogramme kann ein Angreifer, sofern sich seine Funknetzwerkkarte im so genannten „Promiscuous Mode“ betreiben lässt, den gesamten Datenverkehr in der Abstrahlungsfläche eines drahtlosen Netzwerkes abhören. Eventuell vorhandene WEP-Schlüssel, die den unerlaubten Zugang zu einem drahtlosen Netzwerk verhindern sollen, können mit frei verfügbaren Werkzeugen (z.B. AirSnort) überwunden werden. Sobald ein Angreifer in der Lage ist, die drahtlose Kommunikation abzufangen und die notwendigen Autorisierungsdaten zu ermitteln (z.B. durch Entschlüsseln des WEP-Schlüssels), kann dieser manipulierend in eine bestehende Netzwerkverbindung (z.B. ARP-Spoofing) eingreifen und eine aktuell laufende Kommunikationssitzung eines Nutzers übernehmen (Hijacking). Die Übernahme einer bestehenden TCP- oder UDP-Verbindung ist selbst dann möglich, wenn diese verschlüsselt (z.B. SSL oder SSH-Verbindung) erfolgt (Man in the middle-Attacke). Des Weiteren kann sich das Mitschneiden des Netzwerkverkehrs nicht nur auf das drahtlose Funknetz beschränken, da ein Angreifer mittels „Broadcast Monitoring“ auch den Netzwerkverkehr des drahtgebundenen Netzwerkes mitlesen kann, wenn vom Access Point eine Verbindung (z.B. via Hub/Switch) in das drahtgebundene Netzwerksegment existiert.

- **Fehlkonfigurationen (engl.: misconfiguration) und bekannte Sicherheitslücken der Access Points**

Viele drahtlose Endgeräte sind im Auslieferungszustand für eine schnelle, einfache und reibungslose Inbetriebnahme konfiguriert, d.h. eventuell vorhandene Sicherheitsmechanismen (z.B. WEP) sind weitestgehend deaktiviert. Da die Hersteller auf die aus Kompatibilitätsgründen deaktivierten Schutzmaßnahmen nicht bzw. nur unzureichend hinweisen, wissen viele Anwender nicht um die Gefahren, die durch die Ausschaltung der Sicherheitstechniken entstehen. Außerdem ist, falls ein Access Point diese Funktionalität überhaupt bietet, die automatische IP-Adressvergabe via DHCP (Dynamic Host Configuration Protocol) in vielen Fällen eingeschaltet, damit ein Anwender im lokalen Netzwerk nicht manuell die IP-Adressen zuweisen muss und eine möglichst problemlose Datenkommunikation zwischen den einzelnen Teilnehmern des drahtlosen Netzwerkes möglich ist. Diese Funktion, die eigentlich unerfahrenen Anwendern den Betrieb eines drahtlosen Netzwerkes erleichtern soll, kann von einem Angreifer missbraucht werden, um selbst unerlaubterweise Teilnehmer eines Funknetzes zu werden. Des Weiteren verwenden viele Firmen und Privatleute anstatt einer alphanumerischen

Zeichenkette, einen Begriff aus dem Wörterbuch bzw. aus ihrem Firmen- oder Privatumfeld als WEP-Schlüssel und werden somit bewusst oder unbewusst anfällig für eine „Brute Force“- oder Dictionary-Attacke. Bei einer Brute Force bzw. Dictionary-Attacke versucht ein Angreifer, Zugang zu einem passwortgeschützten System zu erlangen, indem er automatisiert eine große Anzahl Passwörter durchprobiert, bis er das richtige Passwort gefunden hat. Ein Angreifer hat es noch leichter, wenn der Betreiber eines Funknetzwerkes das durch den Hersteller eines Access Points vorgegebene Passwort überhaupt nicht ändert, da im Internet Listen mit den entsprechenden Standardpasswörtern kursieren. Zusätzlich besitzen manche Programmteile der auf einigen Access Points verwendeten Betriebssysteme zum Teil erhebliche Sicherheitslücken, die auf unsaubere Programmierung zurückzuführen sind. Ein Angreifer kann beispielsweise durch speziell präparierte Anfragen sensible Administrationsdaten (z.B. Passwörter) abfragen oder ganze Konfigurationsdaten aus dem Access Point auslesen.

- **Blockierung (engl.: jamming)**

Das gezielte Blockieren (engl.: jamming) eines Access Points bzw. der übertragenen Funkwellen stellt ein großes Problem dar. Ein Angreifer kann einen Access Point mit einer so genannten „Denial of service“-Attacke lahmlegen, indem er den Access Point über einen längeren Zeitraum mit einer großen Anzahl Paketen bombardiert, bis dieser unter der Last zusammenbricht und damit das gesamte, funkbasierte Netzwerk lahmlegt. Derartige Störungen können, gewollt oder ungewollt, auch durch andere Quellen (z.B. schnurlose Telefone etc.) entstehen, die den gleichen Frequenzbereich verwenden.

- **Client-Client Attacke (engl.: client to client attacks)**

Alle Teilnehmer eines funkbasierten Netzwerkes speichern die sensiblen Zugangsdaten (z.B. WEP-Schlüssel), die zur Authentifizierung und Kommunikation mit einem Access Point verwendet werden, lokal zwischen. Da viele Hersteller die Zugangsdaten auf den Festplatten der Teilnehmer komplett ohne oder nur mit einer sehr schwachen Verschlüsselung versehen, kann ein Angreifer durch das gezielte Ausnutzen einer Schwachstelle des Betriebssystems eines Teilnehmers in den Besitz der Zugangsdaten gelangen. Des Weiteren sind alle lokalen Daten auf den Festplatten der einzelnen Teilnehmer des Funknetzes prinzipiell bedroht, sofern diese nicht mit besonderen Maßnahmen geschützt sind (z.B. Dateisystemverschlüsselung).

Der Einbruch in ein funkbasiertes Netzwerk erfolgt entweder durch Ausnutzung einer bekannten Schwachstelle der vorgestellten Sicherheitsmechanismen (z.B. schwache Initialisierungsvektoren im WEP-Protokoll) oder durch einen gezielten Angriff gemäß der fünf identifizierten Angriffsvarianten. Den schematischen Ablauf eines typischen Angriffs auf ein drahtloses Netzwerk veranschaulicht die folgende Grafik:

Die Sicherheit drahtloser Netzwerke

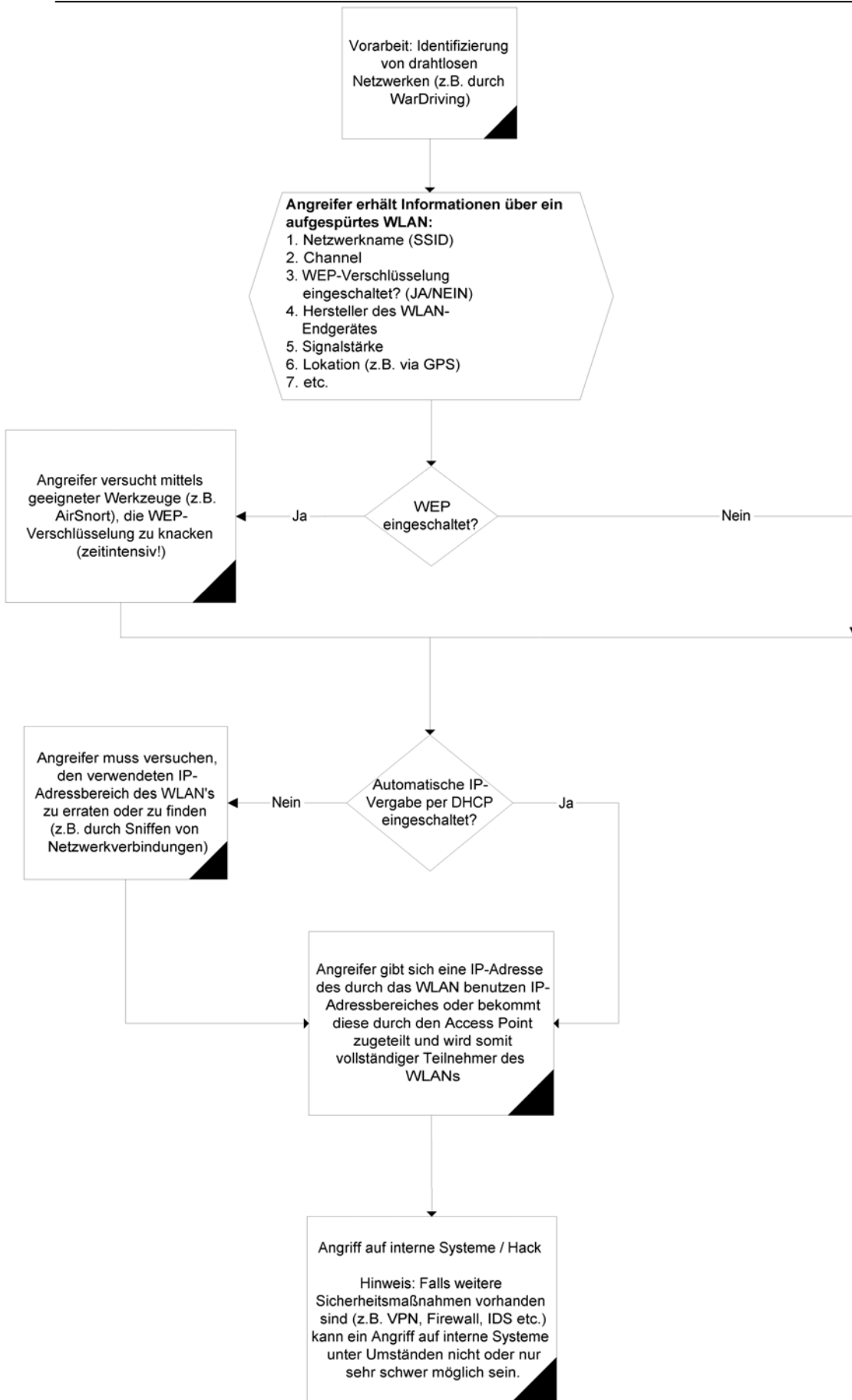


Abbildung 7: Schematischer Ablauf eines Angriffes auf ein funkbasiertes Netzwerk

Ein Angreifer muss zunächst ein funkbasiertes Netzwerk aufspüren (z.B. durch WarDriving, siehe Anhang) und identifizieren. Geeignete Werkzeuge (z.B. Netstumbler) liefern ihm wichtige Daten über das gefundene Funknetz und helfen ihm einen Angriff vorzubereiten. Falls der gefundene Access Point das WEP-Protokoll aktiviert hat, muss ein Angreifer zunächst den geheimen WEP-Schlüssel herausfinden (z.B. mit AirSnort), um eine Verbindung mit dem Access Point aufbauen zu können. Sofern der Betreiber eines Access Points das WEP-Protokoll nicht eingeschaltet hat, kann der Angreifer direkt versuchen, von einem eventuell vorhandenen DHCP-Server eine IP-Adresse zu beziehen. Sollte kein DHCP-Server vorhanden sein, muss ein Angreifer den IP-Adressbereich der im lokalen Funknetz verwendet wird, erraten oder mittels eines Sniffers feststellen, um sich selbst eine gültige IP-Adresse aus dem benutzten IP-Adressbereich zu geben. Danach ist ein Angreifer bereits vollständiger Teilnehmer eines funkbasierten Netzwerkes und kann, sofern keine weiteren Sicherheitsmechanismen vorhanden sind (z.B. Virtual Private Networks, SSH-Tunneling) und eine Verbindung vom drahtlosen in das drahtgebundene Segment eines Netzwerkes besteht, das gesamte Netzwerk angreifen.

Lösungsansätze

Zur Erhöhung der Sicherheit von drahtlosen Funknetzen sind, abhängig vom Einsatzszenario und dem Schutzbedarf der Informationen, mehrere Maßnahmen erforderlich. Die einzuleitenden Maßnahmen sind in drei Kategorien einteilbar:

- **Konfiguration und Administration der Funkkomponenten**
Einfache Basisschutzmaßnahmen (z.B. Aktivierung von WEP) an den Komponenten des drahtlosen Netzwerkes (z.B. Access Points) sollten trotz bekannter Unzulänglichkeiten aktiviert werden.
- **Über den 802.11b-Standard hinausgehende technische Maßnahmen**
Zusätzliche technische Maßnahmen (z.B. Verwendung von starker Verschlüsselung), die über die durch den 802.11b-Standard definierten Sicherheitsmechanismen hinausgehen, erhöhen die Sicherheit enorm.
- **Organisatorische Maßnahmen**
Auch organisatorische Maßnahmen, können in Verbindung mit den beiden vorhergehenden Maßnahmen, das allgemeine Sicherheitsniveau anheben.

Die folgenden Basisschutzmaßnahmen sollten an den einzelnen Komponenten des drahtlosen Netzwerkes vorgenommen werden:

1. Durch den Hersteller vorgegebene Passwörter ändern und durch eigene, nicht in Wörterbüchern vorkommende, alphanumerische Zeichenketten ersetzen. Diese sollten neben Groß- und Kleinbuchstaben auch Zahlen und Sonderzeichen enthalten (z.B. „A@!x7~sJ3/“) und über eine Mindestlänge von acht Zeichen verfügen.
2. Vorgegebenen Netzwerknamen (SSID) ändern. Der neue Netzwerkname darf keinerlei Rückschlüsse auf die Funktion (z.B. Internetgateway), den Standort (z.B. Rotebühlplatz 11) oder den Betreiber (z.B. Firma XY) eines Access Points zulassen. Deaktivieren Sie außerdem das Broadcasten der SSID am Access Point, sofern möglich.
3. Wenn möglich, sollte die Konfiguration des Access Point mit einem zusätzlichen Passwort versehen werden. Dieses Passwort sollte auf keinen Fall mit dem WEP-Kennwort übereinstimmen und sollte Groß- und Kleinbuchstaben, Zahlen sowie Sonderzeichen enthalten. Auch hier ist eine Länge von mindestens acht Zeichen ratsam.
4. Sofern der Zugang zu einem Access Point durch einen MAC Adressen-Filter beschränkt werden kann, sollte diese Schutzmaßnahme aktiviert werden.
5. Ebenso sollte auf jeden Fall die WEP-Verschlüsselung eingeschaltet werden, auch wenn diese als unsicher einzustufen ist. WEP bietet einen geringen Grundschutz und sollte nur

Die Sicherheit drahtloser Netzwerke

mit einer 128 Bit langen Verschlüsselung verwendet werden.

6. Die geheimen WEP-Schlüssel müssen periodisch gewechselt werden. Je sensibler die per Funknetz übertragenen Daten sind, desto öfter muss der WEP-Schlüssel gewechselt werden.
7. Aufstellort und Antennencharakteristik des Access Points sind so wählen, dass möglichst nur das gewünschte Gebiet funktechnisch versorgt wird. Dabei ist zu beachten, dass sich die Funkwellen sowohl horizontal als auch vertikal ausbreiten. Des weiteren sollte die Sendeleistung des Access Points reduziert werden, damit nach Möglichkeit nur das gewünschte Gebiet funktechnisch versorgt wird.
8. Wenn der Access Point die automatische Vergabe von IP-Adressen via DHCP (Dynamic Host Configuration Protocol) unterstützt, sollte diese abgeschaltet werden. Die lokalen IP-Adressen sollten statisch vergeben und ein möglichst kleiner IP-Adressbereich gewählt werden. Falls möglich, sollten statische ARP-Speichertabellen sowie Intrusion Detection Systeme eingesetzt werden, die Angriffe auf ein lokales Netzwerk erkennen und melden können. Ein DHCP Server wird einem Eindringling andernfalls automatisch eine gültige IP-Adresse zuweisen.
9. Manche Hersteller haben auf die aufgedeckten Schwachstellen des WEP-Protokolls reagiert und eigene, proprietäre Erweiterungen (z.B. WEPplus, Fast Packet Keying) auf den Markt gebracht, die die Sicherheit der drahtlosen Datenübertragung erhöhen sollen. Man sollte deshalb die einzelnen Endgeräte softwaremäßig auf den neuesten Stand bringen. Da die neuen Sicherheitsverfahren jedoch nicht standardisiert sind, können nur die Komponenten mit der gleichen Erweiterung zusammen verwendet werden, andernfalls wird die Aktivierung der proprietären Sicherheitsmechanismen unterbunden.
10. Bei Nichtbenutzung einer drahtlosen Komponente sollte diese abgeschaltet werden. Dies gilt insbesondere für funkbasierte Endgeräte in Firmennetzwerken, um in Zeiten, in denen die Funktionalität der Komponenten nicht benötigt wird (z.B. am Wochenende) einem Angreifer keine Angriffsfläche zu bieten.

Da die durch den Standard 802.11b bereitgestellten Sicherheitsmechanismen bei weitem nicht ausreichend sind, sollten die nachfolgend beschriebenen technischen Maßnahmen eingeleitet werden:

1. Als zusätzliche Sicherheitsmaßnahme wird bei Verwendung eines Funknetzes die Benutzung eines VPN-Tunnels empfohlen. Hierzu wird hinter dem Access Point jeder Liegenschaft ein VPN-Gateway installiert. Beim Verbindungsaufbau wird ein kryptographischer Tunnel (z.B. basierend auf dem Standard IPSEC) aufgebaut. Durch diese Maßnahme wird ein Mithören der Datenpakete entsprechend der Stärke und Wirksamkeit dieses zusätzlichen Verschlüsselungsverfahrens erschwert und fast unmöglich gemacht. Da es sich bei IPSEC um einen weltweiten Standard handelt, können alle marktgängigen Produkte, die diesen Standard erfüllen, verwendet werden. Sollte die Verwendung eines VPN-Tunnels aus technischen Gründen nicht möglich sein, sollten alternative Verschlüsselungsverfahren (z.B. SSH-Tunnel, SSL etc.) angewendet werden, um ein Mithören der übertragenen Datenpakete zu verhindern.
2. Ein drahtloses Netzwerk sollte immer als feindliches („untrusted“) Netzwerk, ähnlich dem Internet, angesehen werden und ist deshalb durch eine Firewall vom Unternehmensnetz zu trennen. Ebenfalls sollte das drahtgebundene Netzwerk mit Intrusion Detection System ausgestattet werden, um Angriffe auf das Netzwerk frühzeitig zu erkennen und entsprechende Gegenmaßnahmen einleiten zu können.
3. Auf jedem Client, der an einem funkbasierten Netzwerk teilnimmt, sollten neben der allgemeinen Betriebssystemsicherheit weitere lokale Schutzmaßnahmen implementiert werden (z.B. Zugriffsschutz, Benutzerauthentisierung, Virenschutz, Personal Firewall,

Die Sicherheit drahtloser Netzwerke

restriktive Datei- und Ressourcenfreigabe auf Betriebssystemebene, lokale Verschlüsselung, etc.), um einen Einbruch in das System und das Stehlen lokaler Daten zu verhindern.

Aus organisatorischer Sicht sollte beim Betrieb eines funkbasierten Netzwerkes folgende Maßnahmen eingeleitet werden:

1. Die Administratoren eines drahtlosen Netzwerkes sollten die Vorgänge innerhalb des Netzwerkes restriktiv untersuchen (z.B. durch Kontrolle der Access Points und Clients mittels Snifferprogramme und Netzwerk-Analysewerkzeuge, regelmäßige Überprüfung der an einem Access-Point angemeldeten Clients, etc.) und kritisch beurteilen. Insbesondere die Anbindung mobiler Clients sowie der Datenaustausch zwischen dem drahtgebundenen und dem drahtlosen Segment eines Netzwerkes ist ein kritischer Bereich, der genauestens beobachtet werden muss.

Fazit

Drahtlose Netzwerke sind zweifelsohne eine bequeme und flexible Möglichkeit, ein eigenes Netzwerk aufzubauen oder ein bereits bestehendes Netzwerk zu vergrößern. Leider hat sich herausgestellt, dass bei der Entwicklung der funkbasierten Netzwerktechnik die Sicherheit der übertragenen Daten nicht in ausreichendem Maße berücksichtigt worden ist. Das WEP-Protokoll erreicht keines der drei geforderten Schutzziele Vertraulichkeit, Authentizität und Integrität, da die Schwachstellen sowohl im Verschlüsselungsalgorithmus selber (XOR von Klartext und Chiffretext ergibt Schlüsselstrom, Known Plaintext-Angriffe), als auch bei der Definition des Standards (zu kleiner Raum von Initialisierungsvektoren, statische Berechnung der Initialisierungsvektoren, Manipulation der Prüfsumme möglich) so gravierend sind, dass WEP praktisch nur unzureichenden Schutz vor Angreifern bietet. Dennoch sollten die vorhandenen Sicherheitsverfahren (z.B. 128-Bit WEP) als eine Art Grundschutz eingeschaltet werden, und durch die Verwendung von zusätzlichen Schutzmaßnahmen (z.B. VPNs, Firewalls, Intrusion Detection System) kann eine sichere Kommunikation auch über ein drahtloses Netzwerk abgebildet werden.

Anhang A – WarDriving

WarDriving bezeichnet das Suchen und Aufspüren von drahtlosen Netzwerken nach dem 802.11b-Standard mit einem PKW und wird als eine Art Sport oder im Vorfeld eines Angriffes auf ein drahtloses Netzwerk durchgeführt. Ein WarDriver fährt mit seinem PKW meist ziellos durch die Stadt und versucht, oft unterstützt durch eine zusätzlich am Wagen angebrachte Antenne, mit Hilfe einer speziellen Software (z.B. Netstumbler, Kismet) Funknetzwerke aufzuspüren. Das Vorwort „War“ stammt ursprünglich vom Begriff WarDialing, der in den 80er Jahren u.a. durch den Film „WarGames“ (1983) geprägt worden ist, in dem ein Jugendlicher durch automatisiertes Anrufen von Telefonnummern in einen Zentralcomputer des Verteidigungsministeriums der USA eindringt und somit eine internationale Atomkrise auslöst. Der zweite Teil des Wortes („Driving“) bezeichnet das Fortbewegungsmittel, welches ein WarDriver benutzt. Gerade in den USA, aber auch vermehrt in Europa, werden Funknetzwerke auch mit anderen Fortbewegungsarten aufgespürt (z.B. per Boot, Helicopter, zu Fuß), wodurch der Begriff WarXing entstanden ist. Der sprachliche Platzhalter Xing steht dabei für das Fortbewegungsmittel, das zum Aufspüren eines drahtlosen Netzwerkes verwendet wird, wobei der PKW („WarDriving“) die gebräuchlichste Art der Fortbewegung ist. Als Ausstattung dient einem WarDriver ein handelsüblicher Laptop sowie eine PCMCIA-Funknetzwerkkarte (z.B. Compaq WL 311). Gefundene Funknetzwerke werden durch die Bemalung von Hauswänden („Warchalking“) mit Kreide für andere Wardriver kenntlich gemacht. Unter Microsoft Windows wird vielfach eine Software namens Netstumbler verwendet, die zur leichten Aufspürung und Identifizierung von funkbasierten Netzwerken dient. Die Software liefert dem Benutzer verschiedene Informationen über das gefundene Netzwerk (z.B. SSID, Channel, WEP-Optionen und Signalstärke) und kann im Zusammenspiel mit einem GPS-System die genaue Position der Access Points protokollieren, so dass diese später sehr leicht wiedergefunden werden können. Durch Verwendung der Software Stumbverter (<http://www.sonar-security.com>) hat der

Die Sicherheit drahtloser Netzwerke

Anwender außerdem die Möglichkeit, die durch Netstumbler gesammelten Daten in das Programm MapPoint 2002 von Microsoft zu importieren und dort geographisch in einer Landkarte auszuwerten. Des weiteren gibt es mit Ministumbler eine Variante für kleine und tragbare Computer (sog. Handhelds), auf denen das PocketPC-Betriebssystem läuft (z.B. Compaq IPAQ) sowie eine freie Variante für Macintosh (MacStumbler). Die folgende Abbildung zeigt ein Bildschirmfoto von Netstumbler:

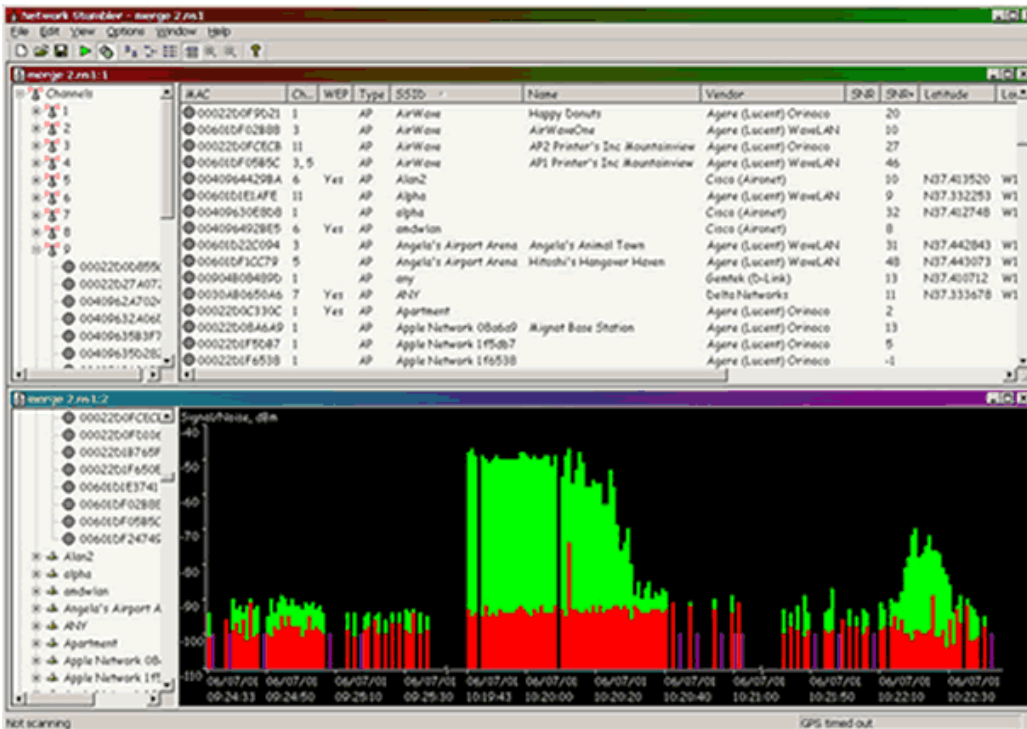


Abbildung 8: Die Software Netstumbler zeigt umfangreiche Informationen über gefundene Funknetzwerke an (Bildmaterial: SANS Institute, <http://www.sans.org>)

Um mir persönlich ein Bild von der Verbreitung von Funknetzwerken zu machen und mögliche Sicherheitslücken aufzudecken, habe ich werktags in Düsseldorf, Frankfurt und Stuttgart jeweils für ca. 120 Minuten Wardriving betrieben. Ich habe die folgenden Ergebnisse erhalten:

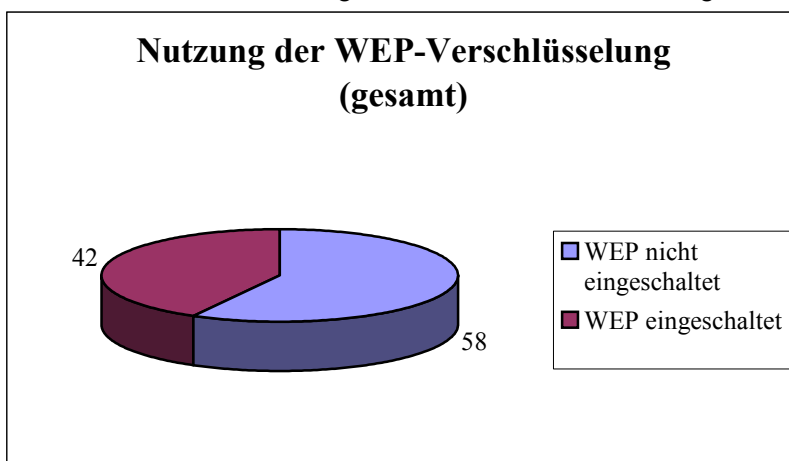


Abbildung 9: Prozentuale Verbreitung der WEP-Verschlüsselung

Bei den 137 von mir gefundenen Funknetzwerken hatten 57 % die WEP-Verschlüsselung nicht eingeschaltet, nur in 43 % aller Fälle war dieser Basisschutz aktiv.

Die nachfolgende Tabelle zeigt die gefilterten Gesamtergebnisse, jeweils aufgliedert nach

Städten, Betriebsmodus und Nutzung der WEP-Verschlüsselung:

Stadt	Anzahl gefundene Geräte	Anteil in %	Infrastruktur-Modus	Ad hoc-Modus	WEP aktiviert	WEP nicht aktiviert
Düsseldorf	49	36 %	46	3	20	29
Frankfurt	63	46 %	62	1	32	31
Stuttgart	25	18 %	24	1	6	19
Gesamt	137	100 %	132	5	58	79

Tabelle 4: Kurzübersicht der Ergebnisse des WarDrivings in Düsseldorf, Frankfurt und Stuttgart

Anhang B - Literaturangaben

Für die Erstellung dieser Praxisarbeit habe ich, neben eigenen Kenntnissen, die folgenden, im Internet verfügbaren Literaturquellen verwendet:

- Bundesamt für Sicherheit in der Informationstechnik: „Sicherheit im Funk-LAN“, http://www.bsi.bund.de/fachthem/funk_lan/index.htm
- Zeitschrift Computer und Technik (c't): „WLAN-Wegweiser“, <http://www.heise.de/ct/01/18/122/>
- Networkers Aktiengesellschaft, <http://www.networkers.de/services/netsecurity/sicherheit/wlan/>
- Fujitsu-Siemens: „Wireless LAN“, http://www.fujitsu-siemens.de/rl/mobility/download/Broch_freeBusiness.pdf
- tecchannel.de: „Sicherheit im WLAN“, <http://www.tecchannel.de/hardware/928/index.html>
- Technische Universität Chemnitz: „Wireless Local Area Networks“, <http://rnvs.informatik.tu-chemnitz.de/wlan/index.htm>
- tomshardware.de: „Sicherheit im WLAN offen wie ein Scheuentor“, <http://www.de.tomshardware.com/network/20020606/index.html>
- Zeitform OHG: „Verschlüsselung“, http://fiatlux.zeitform.info/technische_infos/encryption.html
- Internet Security Systems Incorporation: „Wireless LAN Security FAQ“, http://www.iss.net/wireless/WLAN_FAQ.php

Des weiteren habe ich die durch Ernst & Young erstellte Studie „Wireless Lan – Analyse zum Stand der Sicherheit in drahtlosen Netzwerken basierend auf IEEE 802.11b“ vom 01.02.2003 zur Erstellung dieser Praxisarbeit verwendet.

Anhang C - Kenntnisnahme

Mir bestätige ich, dass ich die vorliegende Praxisarbeit von Herrn Sebastian Wolfgarten gelesen und zur Kenntnis genommen habe.

Marcus Rubenschuh
Mitglied der Geschäftsleitung
Ernst & Young IT Security GmbH
Mergenthalerallee 10 – 12
65728 Eschborn / Frankfurt am Main