Sicherheit in Wireless Lan Netzwerken

Schule: Elsa-Brändström-Gymnasiums Oberhausen

Schuljahr: 12 Fach: Informatik Kurs: 1

Name des Schülers: Alexander Gratza

Thema der Arbeit: „Sicherheit in Wireless Lan Netzwerken“

Die Arbeit wurde am 11.02.2005 abgegeben.

Unterschrift des Schülers:

Unterschrift des Fachlehrers:

Beurteilung der Arbeit:

Note: Punktzahl:

Datum: Unterschrift des Fachlehrers:

Inhaltsverzeichnis

Vorwort

Durch mein großes Interesse an Computern und der Technik, war es für mich nicht schwer ein geeignetes Thema für meine Facharbeit in der Informatik zu finden. Wireless Lan wird sicher in Zukunft von großer Bedeutung sein, und da ich selber über ein Funknetzwerk verfüge und besorgt über die Sicherheit bin, kam ich zu dem Entschluss meine Facharbeit über die Sicherheit in Wireless Lan Netzwerken zu schreiben, um tiefer „in die Materie einzusteigen“ und diese besser zu verstehen. Dazu wird mir diese Facharbeit auch in Zukunft behilflich sein, wenn ich wieder einmal bei Bekannten oder Verwandten ein Firmennetzwerk einrichten soll oder im Internet Kollegen mit Rat und Tat zur Seite stehe. Unter anderem könnte man mit den gewonnenen Informationen eventuell selber Assistenten programmieren oder eine kleine Broschüre erstellen, die anderen PC-Benutzern helfen ihre Netzwerke einzurichten und geeignete Einstellungen in Bezug auf die Sicherheit vor zu nehmen. Bei meiner Facharbeit ist mir wichtig, dass andere Leute die Sicherheitsprobleme und deren Risiken ernster als zuvor nehmen, so dass man in Zukunft keine unverschlüsselten Funkverbindungen mehr vorfindet.

An das Experiment die Sicherheit der Funknetzwerke in Oberhausen zu untersuchen, bin ich durch zahlreiche Berichte in Computerfachzeitschriften gekommen und fand diese für mein Projekt sehr sinnvoll.

An dieser Stelle will ich mich bei einem Experten Roelof Berg (http://www.berg-solutions.de) bedanken, der mir bei Verständnisfragen geholfen und Quellenhinweise und Erklärungen geliefert hat, damit ich meine Facharbeit fortführen und die Richtigkeit der beschriebenen Sicherheitsverfahren korrekt darstellen konnte.

Was ist Wireless Lan?

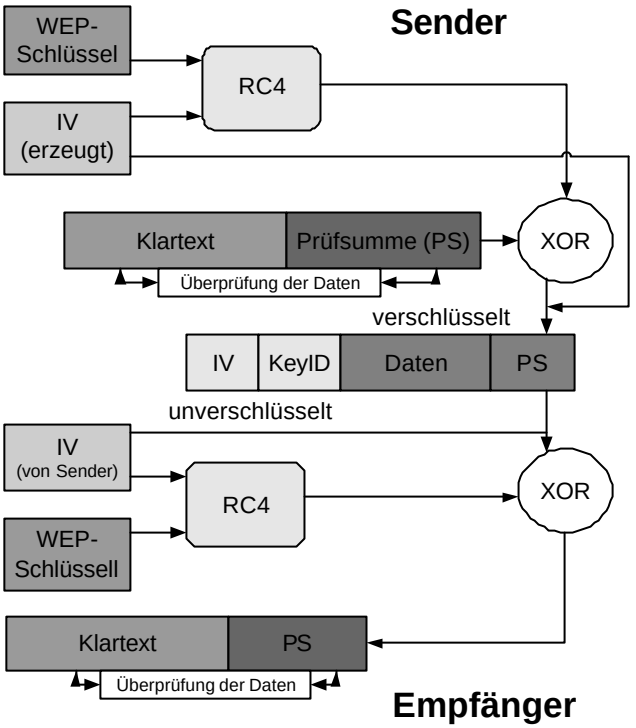
Wireless Lan ist die neuste Technik zur Verbindung von Computern zu einem kabellosen Netzwerk. Diese Netzwerke funktionieren fast genau so wie herkömmliche Netzwerke, nur das diese anfälliger in Hinblick auf die Sicherheit sind.
So kann jeder, der sich in der Reichweite eines Funknetzwerkes befindet, sich mit den notwendigen Einstellungen in ein Netzwerk einloggen oder dieses abhören.
Die Funknetzwerke arbeiten alle mit dem IEEE 802.11x (x steht für a, b, b+, g) Standard.
Es gibt zwei verschiedene Strukturen von Funknetzwerken.
Einmal das Ad-hoc Netzwerk (ad-hoc = sofort), wobei jeder Rechner mit anderen Endgeräten (Clients) kommunizieren und Daten austauschen kann, ohne über einen Access Point zu verfügen. Dazu müssen alle WLan Adapter auf den gleichen Funkkanälen arbeiten und in Reichweite der Funkwellen sein. Zurzeit gibt es bis zu 13 Funkkanäle, die man mit Hilfe von Software beliebig einstellen kann. Die Funkwellen arbeiten im 2,4 und 5 Ghz Bereich und haben eine Übertragungsrate von 11 – 100 Mbit/s.
Als zweite Struktur ist das Infrastruktur-Netzwerk bekannt, das mindestens einen Zugangspunkt (Access Point) besitzt. Über diesen Access Point, auch als WLan-Router bekannt, lassen sich noch zahlreiche Computer, sowohl über Wireless Lan als auch Kabelgebundene Rechner anschließen, da der Access Point in den meisten Fällen auch einen Switch / Hub eingebaut hat. (Beispiele für versch. Funknetzwerke im Anhang 1.1)
Die am meisten verwendete Netzwerk-Architektur ist das Prinzip der Infrastruktur-Netzwerke, die oft direkt über den Access Point an das Internet angeschlossen sind, sodass auch alle Computer, egal wo sie sich im Haus befinden, ohne Kabel ins Internet kommen. Dies spart nicht nur Kosten sondern auch viel Zeit, die man ansonsten für das Verlegen von Netzwerkkabeln (z.B. RJ45) brauchen würde.
Wireless Lan steht für Mobilität und Informationszugang an öffentlichen Plätzen insbesondere durch Hot Spots. Hot Spots findet man an Flughafen, Bahnhöfen, Cafes und zahlreichen anderen öffentlichen Plätzen.
Wireless Lan ist bei vielen Leuten beliebt und in vielen Fällen gar nicht mehr wegzudenken, doch nicht jeder weiß, dass jeder Kontakt durch den privaten Rechner mit einem Funknetzwerk ein großes Risiko mit sich bringt. Daher werde ich in meiner

Facharbeit auf die gröbsten Risiken eines WLan-Netzes aufmerksam machen, und erklären wie es zu Sicherheitslücken kommt und wie man vorbeugen kann.

Sicherheitsverfahren

Wired Equivalent Privacy (WEP)

Die WEP-Verschlüsselung setzt sich aus dem so genannten RC4 zusammen, der den WEP-Schlüssel und den erzeugten 24 Bit langen Intialization Vector (IV) enthält. Der RC4 codiert mit Hilfe des XOR-Verfahrens den Klartext bzw. die Klardaten mit einer Checksumme CRC [1] genannt. Nun existiert ein Datenpaket mit unverschlüsseltem IV, der errechneten KeyID und den verschlüsselten Daten mit der Prüfsumme. Mit Hilfe des IVs kann der Empfänger mit dem bekannten WEP-Schlüssel die gesendeten Daten mit dem RC4 wieder über das XOR- Verfahren decodieren und richtig auslesen.



„Die WEP-Verschlüsselung im schematischen Aufbau“, Quelle: Buch, Wireless Lan – Das kabellose Netzwerk von Thomas Köhre, Markt+Technik Verlag (2003)

Doch da die Vektoren des IV automatisch erstellt werden „fallen auch Werte an, die das Datenpaket nur unzureichend verschlüsseln“ (Wireles Lan / Das kabelose Netzwerk von Thomas Köhre 2003, Markt + Technik Verlag, S.41). Als Folge ist es möglich, die schlecht verschlüsselten Daten Mitzulesen und das Zurückrechnen des WEP-Schlüssels mit Hilfe des unverschlüsselten IV.

Die meist verbreiteten WEP-Schlüssel sind die 64 (ASCII Zeichenlänge: 5) und 128 Bit (ASCII Zeichenlänge: 13). Diese WEP-Schlüssel unterscheiden sich nur durch die verschiedenen Längen der Schlüssel (Keys). Je länger die Schlüssel sind, desto weniger besteht die Gefahr eines aktiven Angriffes auf ein Funknetzwerk, da das Ausprobieren eines WEP-Schlüssels bei einer 128 Bit WEP-Verschlüsselung lange dauern kann. Auf solche Tests werde ich im dritten Kapitel der Facharbeit noch genauer eingehen.

[1] Mehr zu CRC : http://de.wikipedia.org/wiki/1Cyclic_Redundancy_Check (08.02.2005)

Vorteil der WEP-Verschlüsselung ist eigentlich nur, die weit verbreitete Benutzung des Sicherheitsverfahrens, doch dies bringt große Probleme mit sich.
Zu den Nachteilen der WEP-Verschlüsselung gehört das Auslesen der MAC Adressen des Clients, der die Daten sendet, die wie der IV unverschlüsselt verschickt werden. So kann ein Hacker die MAC Adresse eines Rechners auslesen und manuell bei seinem System einstellen. Dadurch kann der Angreifer den MAC Adressen Filter des Access Points umgehen. Dazu kann man durch eine Challenge and Response Anfrage beim Access Point Schlüssel ausprobieren oder mitlesen. Die Änderung des Schlüssels ist bei größeren Netzwerken sehr aufwendig, da an jedem Client der Schlüssel manuell gewechselt werden muss. Durch die unverschlüsselte Authentifizierung des Netzwerknamens ist es nicht schwer den Netzwerknamen (SSID / ESSID) heraus zu finden.

Wi-Fi Protected Access (WPA)

WPA hat im Gegensatz zu WEP einen dynamischen Schlüssel der in regelmäßigen Abständen geändert wird. Das Sicherheitsverfahren basiert auf dem Temporal Key Integrity Protocol (TKIP), das zur Authentifizierung verwendet wird und sich um den WEP-Schlüssel legt und so die Sicherheitslücke schließt. Dazu bietet WPA zwei Arten der Anmeldung an ein Netzwerk. Entweder wird das Managed Key Verfahren verwendet, bei dem die Anmeldung zum Netzwerk über einen Server gesteuert wird und jeder Benutzer seine eigenen Zugangsdaten bekommt, oder man verwendet das „Pre-Shared Keys“ Verfahren, wobei alle Benutzer das gleiche Passwort zur Anmeldung verwenden.
Die zweite Variante ist die Unsicherere, da hier durch zufällig generierte Zeichenfolgen das Passwort nach längerer Zeit herausgefunden werden kann, wenn man sich nicht an das Grundschutzhandbuch[2] des Bundesamtes für Sicherheit in der Informationstechnik (BSI) hält. Durch die Session Keys, die regelmäßig geändert werden, wird das Funknetzwerk sicherer für den allgemeinen Datenverkehr. Im Gegensatz zum WEP kann hier ein Angreifer alleine durch das Abhören des Traffics nicht viel erreichen, da sich der Schlüssel nicht vor einem Schlüsselwechsel entschlüsseln bzw. zurückrechnen lässt, weil dafür in der kurzen Zeit viel zu wenige Datenpakete verschickt werden. Auch reicht der Schlüssel alleine nicht aus, da man zur Authentifizierung an das Netzwerk

[2] siehe http://www.bsi.bund.de/gshb/deutsch/m/m02011.html 08.02.2005

noch das Zugangspasswort benötigt. WPA bietet durch das automatische Schlüssel wechseln einen höheren Komfort für den Benutzer und Administrator eines Netzwerkes und in unserem Fall eine viel höhere Datensicherheit als WEP. Mit dem neuen Verschlüsselungsverfahren WPA2 wird der RC4 ausgewechselt, auch der Advanced Encryption Standard (AES). Diese Verschlüsselung ist ein symmetrisches Kryptosystem, dessen Schlüssel eine Länge von 128, 192 oder 256 Bit haben. Dieses Verschlüsselungsverfahren gilt als nicht zurückrechenbar, da es zu aufwendig konzipiert ist und sich durch die langen Schlüssellängen in der Sicherheit bewährt.

Hohe Sicherheit durch IPsec in Firmennetzwerken

In Firmennetzwerken wird bei Verwendung eines Funk-Lans auf das Tunnelprotokoll IPsec zugegriffen, das bis jetzt die höchste Sicherheit bietet. Dieses Protokoll arbeitet sowohl mit symmetrischen und asymmetrischen Schlüsseln, die zwischen den beiden Clients oder Access Point und Client automatisch vereinbart werden können, um mit Hilfe der jeweiligen IP die Daten zu entschlüsseln. So wird gewährleistet, dass auch nur der jeweilige Empfänger die Daten entschlüsseln kann. IPsec bietet zwar große Sicherheit, hat aber den Nachteil, dass man durch die mehrfache Verschlüsselung der Daten Bandbreitenprobleme in Kauf nehmen muss, um die höchste Sicherheit zu erreichen. Dazu kommt der hohe Kostenfaktor zum Verwalten des Systems. Weitere Probleme tauchen bei der Beschaffung der nötigen Hardware auf, so dass z.B. sehr wenige WLan-Router IPsec zurzeit unterstützen. Bei meinen Ausflügen ins Internet konnte ich gerade mal einen WLAN-Router[3] finden, der IPsec unterstützt.

Zukunft von Sicherheitsverfahren

Da Wireless Lan noch am Anfang seiner Möglichkeiten steht, werden sicher in den nächsten Jahren immer wieder gängige Sicherheitsverfahren von Hackern geknackt und es werden immer wieder neue Standards hinzukommen, die die Sicherheit der Funknetzwerke erhöhen sollen. Durch die steigenden Übertragungsraten bei Funknetzwerken und immer höheren Rechenleistungen werden auch bald noch aufwändigere Verfahren eingesetzt werden können, bei denen man mit längeren Schlüsseln arbeiten und mehr Verschlüsselungsverfahren kombinieren wird. WPA2 ist derzeit das neuste, abwärtskompatible Verschlüsselungsverfahren zu WEP und WPA.

[3] WLAN-Router mit IPsec: http://www.lancom-systems.de/produkte/lc_1811_wireless_dsl.php 08.02.05

Trotz der Sicherheitsverfahren, die manchmal mehr und manchmal weniger schützen werden Firmen dieses Verfahren der Datenübertragung nur verwenden, wenn sie das Risiko in Kauf nehmen, dass Fremde bei großem Aufwand die Daten des Unternehmens mit aufzeichnen und abhören können.

Wie sicher sind die Funknetzwerke in Oberhausen?

Ich habe am 1. und 2. Februar 2005 einige Netzwerke in Oberhausen unter die Lupe genommen und festgestellt, dass etwas mehr als die Hälfte der gefundenen Funknetzwerke noch nicht einmal die Standard Sicherheitseinstellungen aktiviert hatten. So wurden innerhalb von 70 Minuten 202 Funknetzwerke mit Access Points vom Programm Network Stumbler aufgespürt. Unter diesen 202 Funknetzwerken waren nur 99 verschlüsselt und bei 22 Netzwerken war die SSID (der Netzwerkname) versteckt, so dass sich kein Unbefugter schnell in das ungesicherte Netzwerk einloggen konnte. Durch die 103 unverschlüsselten Netzwerken bin ich recht stutzig geworden, da man sowohl theoretisch als auch praktisch in jedes der Netzwerke ohne Zusatzprogramme eindringen könnte, solang die Benutzer beim Access Point keine MAC Filterung eingestellt haben. Ebenso ist mir aufgefallen, dass einige Access Points noch die Firmeneinstellungen besaßen, die ab Werk nicht mehr verändert worden sind und somit auch dem Angreifer eines unverschlüsselten Netzwerkes keine Schwierigkeiten bereiten würden. Die am meisten benutzten Netzwerknamen (SSIDs) waren in meinem Testgebiet (siehe Anhang 3.1) WLAN (63 mal), default (25 mal) und NETGEAR (12 mal).

Da sehr viele Netzwerke keine Verschlüsselung eingestellt hatten, hätte ich in fast jedes dieser Netzwerke eindringen können, indem ich die SSID des zu erreichbaren Netzwerkes und den Kanal (Channel) in ein mitgeliefertes Funklan-Programm eines beliebigen Herstellers eingegeben hätte.

Das Ergebnis dieser kleinen Statistik lässt darauf schließen, dass noch viel Aufklärungsbedarf in Hinsicht der Sicherheit von Funknetzwerken nachzuholen ist. Dazu sollte man auch in den Medien noch mehr auf die Folgen schlampiger Sicherheitseinstellungen aufmerksam machen. Ansonsten werden neugierige Hacker oder Nachbarn bald mehr über die nachlässigen Benutzer erfahren, da jene ihren Rechner eventuell auf private Bilder und ähnliches durchsuchen. Die Hersteller sollten versuchen die Einstellungen der Access Points noch übersichtlicher zu gestalten und gegebenenfalls Software Assistenten anbieten, die den Benutzer in wenigen Schritten zu

einem einigermaßen sicheren Funknetzwerk verhelfen, so dass auch Leute, die nicht über das nötige Know-how verfügen ihr Funknetzwerk sicherer gestalten können.

Hacken des eigenen W-Lans

Ich habe den Versuch unternommen mein eigenes Wireless Lan Netz, das verschlüsselt ist, zu hacken. Doch dabei bin ich auf einige Probleme gestoßen. Einerseits laufen dafür die meisten kostenlosen und legal erhältlichen Tools, wie z.B. WebCrack, WebAttack und Airsnort zum größten Teil nur unter Unix/Linux basierten Systemen. Bei der Installation der W-Lan Komponente waren keine entsprechenden Treiber vorhanden und daher konnte der W-Lan Adapter nicht installiert werden. Darauf habe ich eine Airsnort Version für das Windows Betriebssystem im Internet gefunden. Es stellte sich nach kurzer Zeit aber heraus, dass meine älteren W-Lan Adapter den Monitor Mode nicht unterstützen, den man zum Aufzeichnen des Traffics benötigt.
Daher werde ich in diesem Teil meiner Facharbeit die Vorgehensweisen der Tools erklären und auf weitere Sicherheitslücken eingehen.

Passiver Angriff auf ein Funknetzwerk

Den Schlüssel eines Netzwerkes kann man alleine durch passives Abhören des Funknetzwerkes zurückrechnen. Als erstes muss ein Angreifer verschlüsselte Datenpakete mit den zugehörigen IVs sammeln, die immer den gleichen WEP-Schlüssel enthalten, aber mit einem anderen IV verschlüsselt wurden. Danach lässt sich durch statistische Methoden der Schlüssel berechnen.
„Interessant sind für den Angreifer dabei nur solche Pakete, die im ersten Byte des IVs einen Wert zwischen i=3 und i=15 und im zweiten Byte den Wert 255 haben; hiervon werden für jeden Wert i zwischen 3 und 15 ca. 60 IVs benötigt. Außerdem ist von den zugehörigen Chiffratdaten nur das erste Byte erforderlich. Da ein unverschlüsseltes Funk-LAN-Paket stets mit demselben Byte (nämlich hexadezimal AA) beginnt, kann aus dem ersten Chiffratbyte das erste Byte des RC4-Bitstroms ermittelt werden.“ (Sicherheit im Funk-LAN WLAN, IEEE 802.11, BSI , Seite 11, 2003)

In der folgenden Tabelle (Tabelle1) wird die Dauer eines Angriffes auf den RC4 mit der durchschnittlichen Übertragungsrate in Verbindung gebracht. Da die Entschlüsselung der Daten frühestens nach einer Paketmenge von 0,95 GB durchzuführen ist, dauert das Sammeln der entsprechenden Daten nach der jeweiligen Auslastung des Funknetzes länger. So kann es vorkommen, dass man den Schlüssel bei großem Datenaustausch schon nach 25 Minuten erhält (siehe Tabelle 1) und bei einem anderen Funknetzwerk erst nach über 21 Stunden den Schlüssel erhalten kann, da die Übertragungsrate so gering ist das eine größere Menge an Datenpaketen gesammelt werden muss.

Datenmenge	Auslastung		
	5 Mbit/s	1 Mbit/s	0,1 Mbit/s
0,95 GB	25 min	2,11 h	21,11 h
1,91 GB	50 min	4,24 h	42,44 h
2,86 GB	1,27 h	6,36 h	2,65 Tage
3,81 GB	1,70 h	8,47 h	3,53 Tage
5,72 GB	2,54 h	12,71 h	5,30 Tage
7,63 GB	3,39 h	16,96 h	7,06 Tage
11,44 GB	5,08 h	25,42 h	10,59 Tage
15,26 GB	6,78 h	33,91 h	14,13 Tage

Tabelle1 - Quelle: Sicherheit im Funk-LAN (WLAN, IEEE 802.11), Bundesamt für Sicherheit in der Informationstechnik, 2003

Dazu ist die Rechnerleistung von der Schnelligkeit der Entschlüsselung abhängig.
Gegen solche passiven Angriffe kann man sich teilweise nur durch die schon erwähnte MAC Filterung und automatisch ändernden Schlüsseln, wie bei WPA und WPA2 schützen.

Aktiver Angriff auf ein Funknetzwerk

Aktive Angriffe werden bei einem Funknetzwerk sehr selten benutzt, da diese meistens langwieriger sind, da es zum Ausprobieren verschiedener Schlüssel gerade im WEP 128 Bit Bereich viel zu viele Möglichkeiten gibt, einen 13 zeichenlangen Schlüssel mit Groß- und Kleinbuchstaben, Nummern und Sonderzeichen zu füllen.
Doch bei 64 Bit Schlüssel sind diese Attacken schnell ein Erfolg, da diese Schlüssel nur aus 5 Zeichen bestehen. Ich habe dazu kleine Tests gemacht die sich zwar nur auf einen Schlüssel beziehen, der sich aus Kleinbuchstaben zusammensetzt, aber zur Veranschaulichung beiträgt.
Bei dem 64 Bit Schlüssel müsste der aktive Angreifer bei dem folgenden Schlüssel „zyhix“ 11851188 Mal Kontakt mit dem Access Point aufnehmen, um sich in das verschlüsselte Funknetzwerk ein zu wählen. Bei einer Verschlüsselung mit dem

Schlüssel „abdce“ sind nur noch 19661 Kontaktaufnahmen zu bewältigen (siehe weitere Beispiele im Anhang 4.1). Dies lässt nochmals auf die Wichtigkeit eines qualitativen Passwortes schließen, dass sowohl aus Groß- und Kleinbuchstaben, als auch Nummern und Sonderzeichen bestehen sollte. Umso mehr die Zeichen miteinander kombiniert werden, desto sicherer wird das Netzwerk gegenüber aktiven Angriffen von Hackern.

Fazit

Bei meiner Testreihe kam ich zu dem Entschluss, dass die Sicherheit von Netzwerken auf zahlreichen Einstellungen und Optionen beruhen. Daher kann man nicht allzu schnell in fremde Netzwerke eindringen. Und dass die vorgestellten Theorien auch in der Praxis mit den neusten W-Lan Adaptern funktionieren. Dies ist von den Fachhochschulabsolventen Jan Flink, Jörn Göbbels, Sandra Köhler, Olaf Köster von der Fachhochschule Bonn–Rhein–Sieg im Fachbereich Angewandte Informatik belegt, die sich mit dem Thema „WLAN-Sicherheitsfunktion WEP „aushebeln““ im Jahr 2003 beschäftigt haben und dass durch kostenlose Tools theoretisch jeder ein WEP Netzwerk hacken könnte, wenn er wollte und das WEP auf keinen Fall eine eindeutige Sicherheit bietet. Daher rate ich Klein- und Großunternehmen nur mit erweiterten Standards, wie mit WPA2 oder IPsec ein Funknetzwerk zu betreiben, wenn diese keine Daten übertragen, die andere Personen missbrauchen oder anderen damit schädigen könnten. Firmen mit vertrauensvollen Daten sollten daher kein Funknetzwerk betreiben.

Folgen eines unsicheren Wireless Lan Netzes

Gelingt es einem Fremden in ein Funknetzwerk einzudringen oder sich anzumelden, muss man mit Datenklau und Datenvernichtung rechnen. Die Schäden dadurch sind für private Netzwerke meistens sehr gering, doch für kleinere Firmen Existenz gefährdend. Mit den privaten Daten kann man auch ein Bewegungs- und Benutzerprofil über die Leute, denen das Funknetzwerk gehört, erstellen. Man kann sogar mit den persönlichen Daten, wie Bankverbindungen und PIN-Codes, falls die Benutzer des Netzwerkes diese auf ihren Rechner gespeichert haben, sein Unwesen treiben.
Dies wären schon fatale Folgen, wobei die Personen mit einem hohen finanziellen Schaden rechnen müssen. Dazu würde in diesem Fall auch das schnelle Online-Banking beitragen. Doch dies ist nur ein Beispiel und es handelt sich noch nicht um die schlimmsten Folgen, denn wenn das Netzwerk über einen W-Lan Router mit dem Internet verbunden ist, können Unbefugte über ihre Leitung z.B. Viren verbreiten oder

sich bei diversen Portalen anmelden, Abbos auf ihren Namen bestellen, illegales Unwesen in ihrem Namen im „Weltweiten Datennetz“ (World Wide Web) treiben, wie z.B. illegal MP3s oder Videofilme herunterladen. Falls sie einen Volumentarif für den Internetzugang besitzen, können durch die Fremdnutzung weitere Kosten bei der Überschreitung des Trafficvolumen anfallen. Für Straftaten, die über ihr Netzwerk von Fremden begangen wurden, müssen sie in erster Linie aufkommen, da man grob fahrlässig handelt, wenn man ein Funknetzwerk ungeschützt betreibt.
Hacker könnten zusätzlich Programme auf ihren Computern installieren, die weitere Sicherheitslücken öffnen und so Hackern aus dem Internet Eintritt gewähren.
Das Problem bei der Sache ist, dass sie bei allen oben genannten Folgen glaubhaft nachweisen müssen, dass sie z.B. das Angebot nicht bei eBay abgegeben haben oder das Abonnement der Zeitung „Der Spiegel“ nicht bestellt haben. Doch das kann sehr viel schwerer sein, als man denkt, da die IP Adresse hinterlegt wird und später bei der Zurückverfolgung der Verbindung nur auf ihren Anschluss schließen lässt und es nicht genau zu erkennen ist, von welchem Computer die Bestellung, Anmeldung oder der Virus losgeschickt wurde und dazu sind sie für die Sicherheit in ihrem Funknetzwerk selber verantwortlich.
Insbesondere bei der Nutzung von Hot Spots sollten sie vorsichtig sein, da in diesen Funknetzwerken mit keiner Verschlüsselung die Sicherheit der Datenübertragung gewährleistet ist, damit jeder schnell die Hot Spots benutzen kann ohne Einstellungen am eigenen Rechner vornehmen zu müssen. Wie sie ihren Rechner schützen, erfahren sie im nächsten Abschnitt.

Wie kann man sein Wireless - Lan Netz besser schützen

Jeder der ein Funknetzwerk betreibt kann sich prinzipiell vor Eindringlingen schützen, indem er bestimmte Grundeinstellungen in der mitgelieferten Software oder beim Access Point / WLAN-Router einstellt.
Dazu gehören die folgenden Begriffe und Einstellungen, wie MAC Adresse, SSID, WEP, WPA, WPA2 und weitere Einstellungen, die man beachten sollte.
Jede Verbindung zum Access Point sollte nach Möglichkeit nur über das Kabelnetzwerk erfolgen unter Verwendung sicherer Protokolle wie SSL, TLS oder SNMPv3.
Man sollte die Basisschutzmaßnahmen einstellen, indem man die Passwortvorgaben der Hersteller am Access-Point so schnell wie möglich ändert und das alte Passwort durch ein längeres ersetzt. Regelmäßiges Ändern der Passwörter, WEP-Schlüssel und der

SSID tragen zur Sicherheit bei. Die SSID sollte keine Rückschlüsse auf Firma oder Standort des Funknetzwerkes hinweisen. Dazu sollte die Funktion des SSID Broadcast am Access Point abgeschaltet werden, so dass verhindert wird, dass die SSID immer zur Authentifizierung mit gesendet wird.
Falls der Access Point über eine MAC Adress-Filterung verfügt, sollte diese mit einer Liste der MAC Adressen aus dem eigenen Netzwerk gefüttert werden.
Auf jeden Fall sollte man ein Verschlüsselungsverfahren einstellen. Wenn der Access Point über das neuste Verfahren WPA2 verfügt sollte dieses auch aktiviert werden, ansonsten sollte man mindestens die 128 Bit WEP-Verschlüsselung wählen und dabei darauf achten, dass man die Schlüssel aus einem Gemisch von Buchstaben (Groß- u. Kleinschreibung), Sonderzeichen und Zahlen wählt. Die Schlüssel sollte man bei der WEP-Verschlüsselung öfters wechseln, vor allem wenn ein anderes Funknetzwerk in der Nähe ist.
Bei der Authentifizierungsmethode sollte man „Open“ wählen, da die Einstellung „Shared Key“ zusätzliche Sicherheitsprobleme mit sich führt.
Dazu sollte man das Dynamic Host Configuration Protocol (DHCP) auf dem Access Point abschalten und statt dessen ein IP Spektrum so eng wie möglich wählen, dass dann nur so viele Rechner in das Netzwerk gelassen werden, die eine IP in dem vorgegebenen IP Spektrum besitzen.
Firmupdates sind immer sehr wichtig, da diese Fehler in den Systemen ausbessern oder neue und erweiterte Verschlüsselungsverfahren mit sich bringen. Dabei ist aber darauf zu achten, dass alle anderen Komponenten des Funknetzes auch die neuen Funktionen unterstützten, da es sonst zu Komplikationen kommen kann. Daher gilt immer bei Updates; nur die Firmupdates der jeweiligen Hersteller zu nehmen und sich vorher darüber zu informieren, ob die anderen Netzwerkkomponenten die neuen Standards unterstützen.
Man sollte auch auf den Clients gängige Sicherheitsprogramme wie Virenscanner, Personal Firewall, Datei und Ressourcenfreigabe auf Betriebssystemebene installieren und einstellen, um insbesondere bei der Nutzung von Hot Spots seinen Rechner ausreichend zu schützen.
Wenn man das Funknetzwerk nicht benutzt, sollte man dieses abschalten, sowohl den Access point als auch die Adapter an den Clients. Eine Eingrenzung des Funkbereiches dürfte zusätzlich verhindern, dass sich die Funkwellen unaufhaltsam verbreiten, Man sollte den Access Point so ausrichten, dass dieser zu allen Clients die geringste

Entfernung hat und darauf dann die Funkintensität, falls technisch möglich, so herabsenkt, dass zum größten Teil nur die Clients des eigenen Funknetzwerkes mit den Funkwellen versorgt werden können. Dabei ist zu beachten, dass sich die Funkwellen sowohl horizontal wie auch vertikal ausbreiten.

Fazit

Während ich mich mit meiner Facharbeit beschäftigt habe, habe ich entdeckt, dass zahlreiche Netzwerke noch nicht einmal eine Standardverschlüsselung, wie WEP verwendeten und somit ein großes Risiko für die betroffenen Personen in diesen Funknetzwerken zur Folge haben.

Auf der anderen Seite zeigten meine Tests, dass nur die 64 Bit WEP-Verschlüsselung bei einem aktiven Angriff erfolgreich geknackt werden und ein passiver Angriff nur erfolgreich sein kann, wenn man über die neue Hardware und auch über mehr Fachwissen in Sachen Unix / Linux verfügt, aber dass auch durch immer neuere so genannte Hacking-Tools die WEP-Verschlüsselung wegen der zahlreichen Sicherheitslücken bald ausgedient haben wird und neuere Verschlüsselungsverfahren wie WPA2 die WEP-Verschlüsselung ersetzen werden.

Ich hoffe, dass in der Öffentlichkeit weiter über die Folgen eines ungeschützten Funknetzwerkes informiert wird und die Betroffenen mehr über die Sicherheit beim Datenverkehr nachdenken werden und die Probleme erkennen. (siehe dazu Zeitungsartikel im Anhang 5.1)

Durch die Reflektion meiner Arbeit bin ich auf Ideen gestoßen, die dass Wireless Lan sicherer machen würden, bevor ich weitere Informationen vorliegen hatte. So kam ich zu dem Schluss, dass bei der Verschlüsselung der Daten ein ständiger Wechsel der Schlüssel ein sehr wichtiger Teil der Sicherheitsverfahren sein muss.

Ziel meiner Arbeit war die Sicherheitsverfahren und deren Funktionen, sowie die Folgen und Lösungen für die Sicherheitsprobleme der Wireless Lan Netze zu veranschaulichen. Leider mussten wegen der festgelegten Seitenzahlen einige Themen aus der Arbeit herausfallen. Darunter fiel ein Konzept zur Sicherung von größeren Funknetzwerken auf Firmenbasis und die technischen Grundlagen für die entsprechende Verwendung.

Persönlicher Eindruck

Mein persönlicher Eindruck ist, dass ich trotz eines umfangreichen Themas, dennoch die wichtigsten Aspekte für die Sicherheit in Funknetzwerken darstellen konnte und bei einigen Lesern, durch die beschriebenen Folgen eines schlecht geschützten Funknetzwerkes, ein neues Sicherheitsbewusstsein geschaffen habe.
Dazu war meine Arbeit durch sehr viele Exkurse an einigen Punkten schwierig und sehr zeitintensiv. Doch ohne diese Exkurse hätte ich diese Facharbeit nicht sinngemäß beenden können, da ansonsten z.B. die Sicherheitsverfahren falsch und daher nicht korrekt hätten dargestellt werden können.
Aber dennoch bin ich zum Ende meiner Facharbeit gekommen und habe viele neue Erfahrungen in der Materialbeschaffung sowie der Auswertung gewonnen.
Ich habe mit der Facharbeit natürlich auch mein Fachwissen erweitern können und werde dieses auch in sinnvoller Form weiter verwenden und benutzen, um zum Beispiel eine Anleitung für die Schritte, die nötig sind um ein sicheres Funknetzwerk aufzubauen, zu schreiben oder später ein Tool zu erstellen, das für die Einrichtung von Funknetzwerken benutzt werden kann.
Ich hoffe, dass viele Leute meine Facharbeit mit Interesse lesen werden und auch durch die gewonnen Informationen behutsamer mit ihrem Funknetzwerken daheim umgehen werden.

Glossar

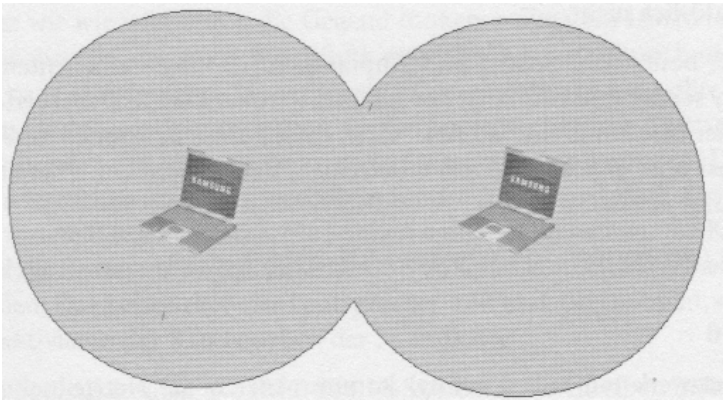
SSID	Service Set Identity; „Netzwerkname“ des Funk-LANs
SSL	Secure Socket Layer
TKIP	Temporal Key Integrity Protocol
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WiFi	Wireless Fidelity; Marketing Begriff generiert durch WECA
WiFi-Alliance	Vereinigung von Herstellern von Funk-LAN-Komponenten nach IEEE 802.11; früher WECA
WPA	WiFi Protected Access; Bezeichnung für über IEEE 802.11 hinaus gehende Sicherheitsmechanismen; generiert durch die WiFi-Alliance
XOR	logische Verknüpfung "exklusiv oder"
CRC	Cyclic Redundancy Check; Bitfehler Erkennungsverfahren
DHCP	Dynamic Host Configuration Protocol
DSSS	Direct Sequence Spread Spectrum; Codemultiplex – Bandspreizverfahren
ESSID	Extended Service Set Identity; „Netzwerkname“ des Funk-LANs
IEEE	Institute of Electrical and Electronics Engineers, New York, www.ieee.org
IP	Internet Protocol
IPSEC	Internet Protocol Security
LAN	Local Area Network; Lokales Netz
MAC.	Media Access Control; Funkzugriffsprotokoll auf ISO Layer 2 Data Link; Es definiert Paket-Format, Paket-Adressierung und Fehlerdetektion
MAC-Adresse	Seriennummer einer Netzkomponente, die durch den Hersteller vergeben wird
RADIUS	Remote Authentication Dial-In User Service;

	Authentisierungs- und Über-wachungsprotokoll auf Anwendungsebene für Authentisierung, Integritätsschutz und Accounting im Bereich Netzzugang
RC4	Stromchiffrierverfahren von Ron Rivest, "Rons Code"
SNMPv3	Simple Network Management Protocol Version 3
802.11	Funk-LAN Spezifikation des IEEE; Datenrate bis 2 Mbit/s; im 2,4 GHz ISM Band; FHSS und DSSS; auch Infrarot Spektrum Kommunikation vorgesehen
802.11a	802.11 Erweiterung; Datenrate bis 54 Mbit/s; im 5 GHz Band; OFDM;
802.11b	802.11 Erweiterung; Datenrate bis 11 Mbit/s; im 2,4 GHz Band; hohe Markt-durchdringung,
802.1X	Spezifikation eines portbasierenden Authentisierungsmechanismus durch IEEE
AES	Advanced Encryption Standard
Client	Jeder mit einem Funk-LAN-Adapter (Funk-LAN-Karte) ausgestattete Rechner, der von anderen Teilnehmern des Funk-Netzwerkes Dienste in Anspruch nimmt

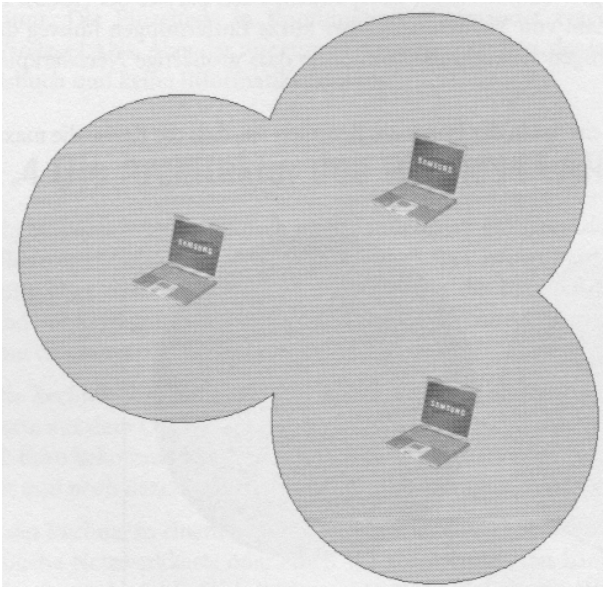
Anhang

Anhang 1.1

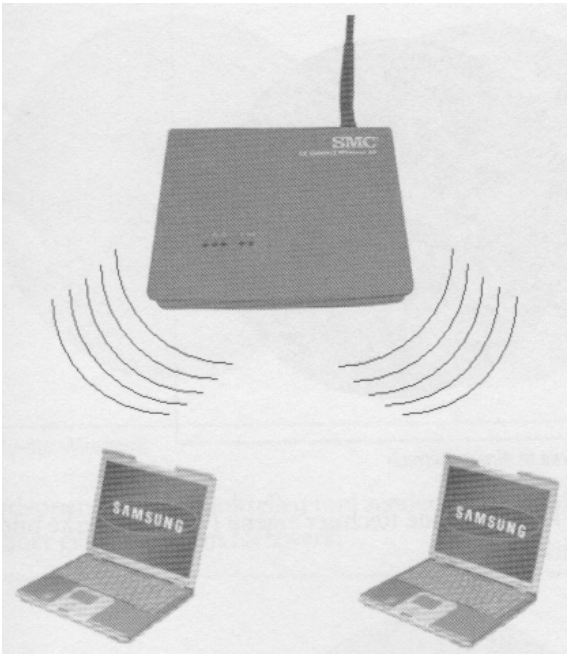
Netzwerkstruktur



Ein Ad-hoc-Netzwerk



Erweitertes Ad-hoc-Netzwerk

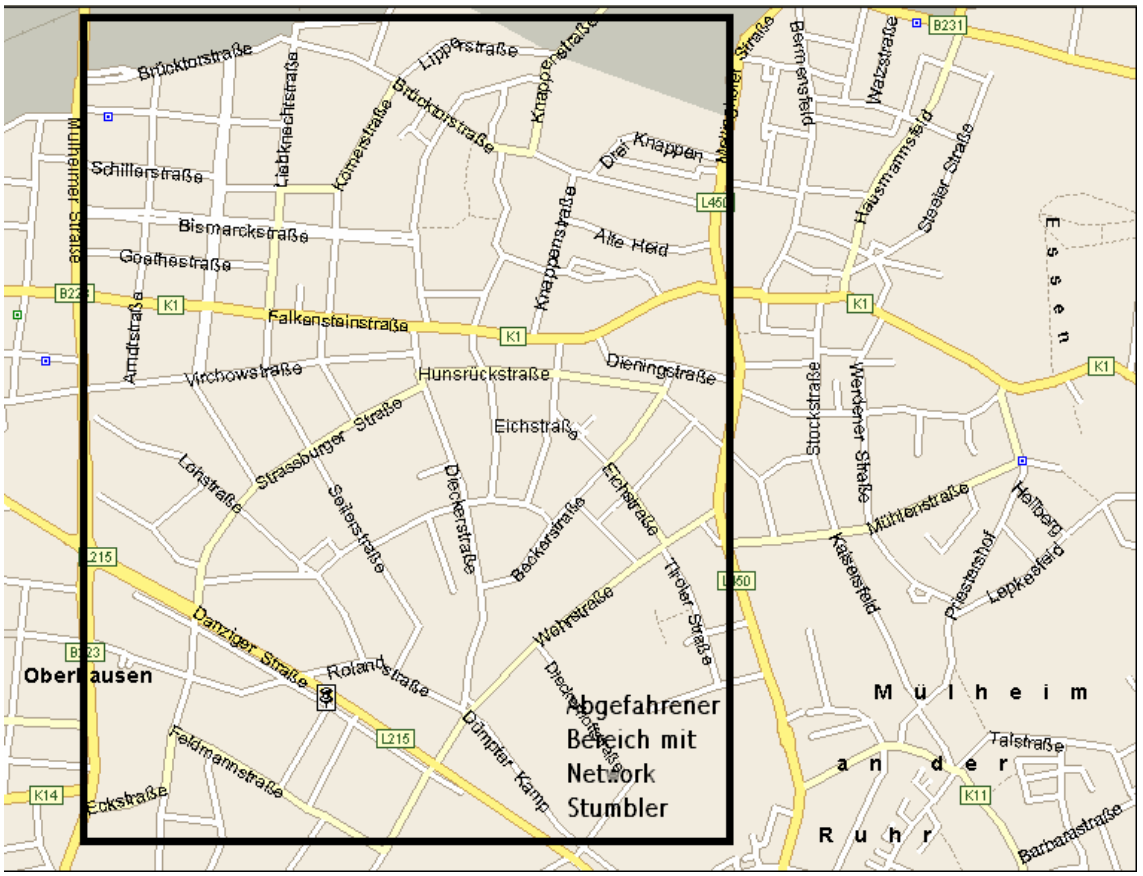


Infrastruktur-Netzwerk mit Access Point

Dazu gibt es noch zahlreiche andere Kombinationen

Quelle: Bilder , aus „Wireless Lan – Das kabellose Netzwerk“ von Thomas Köhre, Markt+Tech Verlag (2003)

Anhang 3.1



Dies ist ungefähr der abgefahrene Bereich des Testgebietes

Ausgewertete Daten des WarDriving in Oberhausen vom 1. und 2. Februar 2005

MAC	SSID	Chan	Speed	Vendor	T...	En...	S...	N...	S...	First S...	Last S...	Fla...	B...
00904B170EBC		6	11 Mbps	Gemtek	AP	WEP	-47	-100	53	16:12:40	16:16:01	0011	100
0030F1CC1A74	154XR	11	11 Mbps	Accton	AP		-81	-100	19	16:11:13	16:12:16	0001	100
0030F1C35429	WLAN	11	11 Mbps	Accton	AP	WEP	-90	-100	10	16:09:59	16:10:26	0011	100
000CF6082CFB	default	11	54 Mbps		AP		-90	-100	10	16:09:31	16:09:33	0001	100
00095B9C8318	NETGEAR	10	11 Mbps	Netgear	AP		-90	-100	10	16:09:18	16:09:20	0001	100
00032F185C9F	Triangle02	11		GST (...	AP	WEP	-89	-100	11	16:09:13	16:09:21	0011	100
00904B2ED982	default	10	11 Mbps	Gemtek	AP		-86	-100	14	16:09:10	16:09:12	0001	100
0060B37998BF	default	6	11 Mbps	Z-Com	AP	WEP	-81	-100	19	16:09:06	16:09:12	0011	100
0080C8AFEE72		6	22 Mbps	D-Link	AP	WEP	-90	-100	10	16:08:59	16:09:06	0011	100
0030F1BD0E9D	vizquel	11	11 Mbps	Accton	AP	WEP	-90	-100	10	16:08:46	16:08:58	0011	100
00A0C566F376	kaisicher	6	11 Mbps	Zyxel	AP		-74	-100	26	16:08:45	16:08:53	0001	100
00095B9A182C	NETGEAR	11	11 Mbps	Netgear	AP	WEP	-79	-100	21	16:08:34	16:08:50	0011	100
0030F1BD05C8	WLAN	11	11 Mbps	Accton	AP		-81	-100	19	16:08:26	16:08:33	0001	100
0030F1E5F6AF	WLAN	11	22 Mbps	Accton	AP		-67	-100	33	16:08:20	16:08:30	0001	100
0030F1D67BC0	WLAN	11	22 Mbps	Accton	AP		-67	-100	33	16:08:19	16:08:42	0001	100
00904B152973	default	6	11 Mbps	Gemtek	AP		-84	-100	16	16:08:09	16:08:12	0001	100
00095B2DA3AC	NETGEAR	11	11 Mbps	Netgear	AP		-73	-100	27	16:08:06	16:08:09	0001	100
00095BA0B985	ZwoKa	11	11 Mbps	Netgear	AP	WEP	-69	-100	31	16:07:59	16:08:09	0011	100
000F3D97C592	uEvoli.Net	6	22 Mbps		AP		-84	-100	16	16:07:43	16:07:45	0001	200
0001E30DAB4D	car1505car0904	11	54 Mbps		AP		-90	-100	10	16:07:27	16:07:27	0001	100
00032F1F498B	default	6		GST (...	AP		-90	-100	10	16:07:22	16:07:22	0001	100
0030F1BCA50B	AP-Ocki	11	11 Mbps	Accton	AP		-89	-100	11	16:07:21	16:07:24	0001	100
000FB50DF3A5	NETGEAR	13	11 Mbps		AP	WEP	-89	-100	11	16:07:16	16:07:18	0011	100
0030F174D5F1	WLAN	7	11 Mbps	Accton	AP		-90	-100	10	16:07:05	16:07:05	0001	100
0001E308806A	ConnectionPoint	11	54 Mbps		AP		-90	-100	10	16:07:01	16:07:02	0001	100
0011500DEE75	belkin54g	11	54 Mbps	(Fake)	AP		-78	-100	22	16:06:36	16:06:39	0001	100
00027203F0F8	Acer	11	11 Mbps	CC&C	AP		-71	-100	29	16:06:33	16:06:38	0001	100

MAC	SSID	C...	Speed	Vendor	Ty...	En...	S...	N...	S...	First S...	Last S...	Fla...	B...
00A0C58102A4	FuWlan	6	22 Mbps	Zyxel	AP	WEP	-66	-100	34	16:02:03	16:02:18	0011	200
0060B379F484	default	6	11 Mbps	Z-Com	AP		-87	-100	13	16:01:35	16:01:36	0001	100
0001E308A55B	ConnectionPoint	11	54 Mbps		AP	WEP	-89	-100	11	16:01:34	16:01:39	0011	100
0030F1C09FEC	WLAN	11	11 Mbps	Accton	AP		-88	-100	12	16:01:30	16:01:36	0001	100
0030F1A8D1ED	WLAN	11	11 Mbps	Accton	AP		-90	-100	10	16:01:27	16:01:35	0001	100
0030F1E5B086	WLAN	11	22 Mbps	Accton	AP	WEP	-90	-100	10	16:01:03	16:01:08	0011	100
000124F45910	WLAN	11	11 Mbps	Acer	AP		-90	-100	10	16:00:57	16:00:59	0001	100
00032F207063	MANNY	6	22 Mbps	GST (...	AP		-88	-100	12	16:00:44	16:00:49	0001	100
0030F1DF6569		11	22 Mbps	Accton	AP	WEP	-90	-100	10	16:00:28	16:00:29	0011	100
00040E2E6FAC	FRITZ!Box SL WLAN	6	22 Mbps		AP	WEP	-71	-100	29	16:00:24	16:00:33	0011	100
0001E3089F26		11	54 Mbps		AP	WEP	-73	-100	27	16:00:22	16:00:25	0011	100
0030F1EC382D	WLAN	11	22 Mbps	Accton	AP	WEP	-74	-100	26	16:00:06	16:00:19	0011	100
0030F1BAE69B	WLAN	11	11 Mbps	Accton	AP	WEP	-67	-100	33	15:59:36	16:00:00	0011	100
00027243DDF1	Acer	11	11 Mbps	CC&C	AP	WEP	-78	-100	22	15:59:23	15:59:31	0011	100
00040E36D791	FRITZ!Box Fon WLAN	6	22 Mbps		AP	WEP	-90	-100	10	15:59:10	15:59:14	0011	100
0003C9447F27	WLAN	11	54 Mbps		AP		-90	-100	10	15:58:52	15:58:57	0001	100
0011090862A2	RG54G2	7	11 Mbps	(Fake)	AP		-90	-100	10	15:58:50	15:58:51	0001	100
000FB517BE24	Petra	11	11 Mbps		AP	WEP	-90	-100	10	15:58:32	15:58:32	0011	100
0030F1E6C306	WLAN	11	22 Mbps	Accton	AP	WEP	-73	-100	27	15:58:12	15:58:17	0011	100
00A0C5FA9767	kaisicher	6	22 Mbps	Zyxel	AP		-84	-100	16	15:58:07	15:58:07	0001	200
0030F197A29F		4	11 Mbps	Accton	AP		-90	-100	10	15:58:06	15:58:07	0001	100
00027203DE2C	dukommsthiernetrein!	8	11 Mbps	CC&C	AP	WEP	-88	-100	12	15:58:04	15:58:06	0011	100
0030F1F65BC3	WLAN	11	22 Mbps	Accton	AP	WEP	-90	-100	10	15:57:52	15:57:56	0011	100
00095BFFBF50		11	11 Mbps	Netg...	AP	WEP	-90	-100	10	15:57:20	15:57:25	0011	100
0003C943A3EA	WLAN	11	54 Mbps		AP	WEP	-69	-100	31	15:57:05	15:57:11	0011	100
00040E3BB1D9	INTERNA-WLAN	6	22 Mbps		AP	WEP	-71	-100	29	15:56:59	15:57:05	0011	100
00095BA886C0	NETGEAR	11	11 Mbps	Netg...	AP	WEP	-75	-100	25	15:56:55	15:57:02	0011	100
000D88F35C02	default	6	22 Mbps	D-Link	AP		-89	-100	11	15:56:11	15:56:49	0001	100
0030F1F5D7CF		11	22 Mbps	Accton	AP	WEP	-77	-100	23	15:55:47	15:55:53	0011	100
0030F1EC06DA	Netzwerk	8	22 Mbps	Accton	AP	WEP	-87	-100	13	15:55:43	15:55:53	0011	100
0080C823F225	Blade	6	22 Mbps	D-Link	AP	WEP	-90	-100	10	15:54:41	15:55:53	0011	100
0030F1D25C21	WLAN	11	11 Mbps	Accton	AP		-80	-100	20	15:54:40	15:55:53	0001	100
0001E30C8D84	KlodoNetz	11	54 Mbps		AP	WEP	-77	-100	23	15:54:35	15:54:40	0011	100
00904B6A098F	default	6	11 Mbps	Gemtek	AP		-73	-100	27	15:54:24	15:54:29	0001	100
000D882B98D7	default	6	11 Mbps	D-Link	AP	WEP	-90	-100	10	15:53:45	15:53:51	0011	100
0030F1F2D803	WLAN	11	22 Mbps	Accton	AP	WEP	-90	-100	10	15:53:34	15:53:34	0011	100
000D8895E83D	haus	6	22 Mbps	D-Link	AP	WEP	-89	-100	11	15:53:30	15:53:37	0011	100
00040E29C969	FRITZ!Box SL WLAN	6	22 Mbps		AP	WEP	-86	-100	14	15:53:27	15:53:30	0011	100
00A0C5640C9A	Weirich	6	11 Mbps	Zyxel	AP	WEP	-90	-100	10	15:53:22	15:53:23	0011	100

MAC	SSID	C...	Speed	Vendor	Ty...	En...	S...	N...	S...	First S...	Last S...	Fla...	B...
0030F1BEA4A4	mary	5	11 Mbps	Accton	AP	WEP	-90	-100	10	15:53:21	15:53:23	0011	100
0030F191EDAF	WLAN	6	11 Mbps	Accton	AP		-86	-100	14	15:52:40	15:52:50	0001	100
0030F1CA9507	WLAN	11	11 Mbps	Accton	AP	WEP	-90	-100	10	15:52:37	15:52:42	0011	100
0030F1E5F58C	WLAN	11	22 Mbps	Accton	AP	WEP	-90	-100	10	15:52:36	15:52:41	0011	100
00400528E56E	LANMARTIN	6	22 Mbps	D-Link	AP	WEP	-90	-100	10	15:52:35	15:52:38	0011	100
00A0C5EC7173	ArcorWirelessLANE2jp	6	22 Mbps	Zyxel	AP	WEP	-72	-100	28	15:52:20	15:52:35	0011	200
0030F1B1E86F		11	11 Mbps	Accton	AP	WEP	-90	-100	10	15:52:18	15:52:35	0011	100
0030F1B1390A		11	11 Mbps	Accton	AP	WEP	-68	-100	32	15:52:17	15:52:27	0011	100
0030AB1E58BD	WirelessStoeck	1	11 Mbps	Delta ...	AP	WEP	-76	-100	24	15:52:10	15:52:10	0011	100
00095B6F2406		11	11 Mbps	Netg...	AP		-63	-100	37	15:51:59	15:52:16	0001	100
001195361759	geheim	6	22 Mbps	(Fake)	AP	WEP	-90	-100	10	15:51:59	15:51:59	0011	100
000D9381B886	onAir	10	11 Mbps	Apple	AP	WEP	-90	-100	10	15:51:53	15:51:53	0011	100
0080C8B09548	default	6	22 Mbps	D-Link	AP		-76	-100	24	15:51:25	15:51:43	0001	100
0030F1DF417E	WLAN	3	22 Mbps	Accton	AP	WEP	-73	-100	27	15:51:11	15:51:18	0011	100
0080C8136715	default	6	22 Mbps	D-Link	AP		-90	-100	10	15:50:41	15:50:58	0001	100
000FB51A2A08	NETGEAR	11	11 Mbps		AP		-74	-100	26	15:50:37	15:50:58	0001	100
000F3D9DC9C6	STIV	6	22 Mbps		AP	WEP	-81	-100	19	15:50:23	15:50:27	0011	200
0030F1E60B8B	WLAN	11	22 Mbps	Accton	AP		-88	-100	12	15:49:49	15:50:08	0001	100
000F3D983096	G664T_WIRELESS	6	22 Mbps		AP		-79	-100	21	15:49:46	15:49:49	0001	200
00119503B4EA	default	6	22 Mbps	(Fake)	AP		-83	-100	17	15:49:45	15:49:48	0001	100
00095B73FBB6	SCHAUFELCHEN	11	11 Mbps	Netg...	AP		-90	-100	10	15:49:41	15:49:48	0001	100
0030F19F2626	WLAN	8	11 Mbps	Accton	AP		-88	-100	12	15:49:39	15:49:48	0001	100
0030F18EB5D4	WLAN	9	11 Mbps	Accton	AP		-80	-100	20	15:49:30	15:49:48	0001	100
0030F1C8CA79	WLAN	11	11 Mbps	Accton	AP		-85	-100	15	15:49:29	15:49:48	0001	100
0030F1E78AC8	WLAN	11	22 Mbps	Accton	AP		-75	-100	25	15:49:28	15:49:48	0001	100
00119509BD4C	Hayabusa	10	22 Mbps	(Fake)	AP	WEP	-90	-100	10	15:49:26	15:49:28	0011	100
0050FCBA6378	default	3	11 Mbps	Edimax	AP		-88	-100	12	15:49:07	15:49:07	0001	100
0040965C430E		7	11 Mbps	Cisco	AP	WEP	-90	-100	10	15:48:55	15:48:56	0011	100
0001E30A8399		10	11 Mbps		AP		-90	-100	10	15:48:45	15:48:45	0001	100
00040E3BB460	FRITZ!Box SL WLAN	6	22 Mbps		AP	WEP	-90	-100	10	15:48:33	15:48:45	0011	100
000FB522646C		6			AP	WEP	-90	-100	10	15:48:23	15:48:26	0011	100
000FB51526C2	TheConstruct	12	11 Mbps		AP		-66	-100	34	15:48:23	15:48:40	0001	100
0050FCFC92E5	default	11	11 Mbps	Edimax	AP		-72	-100	28	15:48:16	15:48:26	0001	100
000C41E38269	linksys	11	54 Mbps	Linksys	AP	WEP	-72	-100	28	15:47:53	15:47:58	0011	100
00095BFB50AE	NETGEAR	11	22 Mbps	Netg...	AP	WEP	-90	-100	10	15:47:41	15:47:41	0011	200
00119535BE4F	DI-624+	6	22 Mbps	(Fake)	AP	WEP	-90	-100	10	15:47:31	15:47:33	0011	100
0030F1ABEC88	WLAN	11	11 Mbps	Accton	AP		-90	-100	10	15:47:25	15:47:32	0001	100
000FB5639CDA		11	54 Mbps		AP	WEP	-90	-100	10	15:47:02	15:47:02	0011	100
0030F1BAD1C3	WLAN	11	11 Mbps	Accton	AP		-72	-100	28	15:47:01	15:53:16	0001	100

MAC	SSID	C...	Speed	Vendor	Ty...	En...	S...	N...	S...	First S...	Last S...	Fla...	B...
0030F1AE6A9B	belkin54g	10	11 Mbps	Accton	AP	WEP	-79	-100	21	15:46:51	15:53:08	0011	100
0030F1FC4288	WLAN	11	22 Mbps	Accton	AP	WEP	-77	-100	23	15:46:35	15:46:42	0011	100
0030F1FC1DBC	WLAN	11	22 Mbps	Accton	AP		-88	-100	12	15:46:25	15:46:29	0001	100
0030F1B611CC	WLAN	11	11 Mbps	Accton	AP		-88	-100	12	15:46:24	15:46:29	0001	100
0030F1E5F697	WLAN	11	22 Mbps	Accton	AP	WEP	-82	-100	18	15:46:23	15:46:30	0011	100
00904B15360A	default	6	11 Mbps	Gemtek	AP		-90	-100	10	15:45:41	15:45:41	0001	100
0030F1EB6A4D	WLAN	11	22 Mbps	Accton	AP		-90	-100	10	15:45:39	15:45:39	0001	100
0030F1CE2E2E	WLAN	11	11 Mbps	Accton	AP		-90	-100	10	15:45:36	15:45:41	0001	100
0030F1927EB2	WLAN	1	11 Mbps	Accton	AP		-65	-100	35	15:45:34	15:45:46	0001	100
0030F1B14A73	KAWA	11	11 Mbps	Accton	AP		-83	-100	17	15:45:14	15:45:21	0001	100
0030F1DEC7DA	WLAN	1	22 Mbps	Accton	AP		-85	-100	15	15:45:13	15:45:21	0001	100
0001E3083BBC	SKKConPoint	11	54 Mbps		AP		-90	-100	10	15:44:52	15:44:55	0001	100
00095BCA78EE	NETGEAR	11	22 Mbps	Netg...	AP	WEP	-90	-100	10	15:44:46	15:44:51	0011	200
0030F1F244B8	WLAN	11	22 Mbps	Accton	AP	WEP	-88	-100	12	15:44:45	15:44:51	0011	100
0030F1B60DE1	WLAN	11	11 Mbps	Accton	AP		-90	-100	10	15:44:45	15:44:51	0001	100
00C002FFD584	default	11	11 Mbps	Serco...	AP	WEP	-65	-100	35	15:44:16	15:44:29	0011	100
0030F1F28DC0	WLAN	11	22 Mbps	Accton	AP		-74	-100	26	15:44:08	15:54:05	0001	100
0030F1E22F4A	Test	11	22 Mbps	Accton	AP		-68	-100	32	15:44:05	15:54:05	0001	100
0030F18EAE1E	WLAN	5	11 Mbps	Accton	AP		-89	-100	11	15:43:51	15:43:59	0001	100
00095BE78BC6	JAMDOWN	6		Netg...	AP	WEP	-73	-100	27	15:43:51	15:54:05	0011	100
00C002EB5D54	Sitecom	11	11 Mbps	Serco...	AP	WEP	-68	-100	32	15:43:42	15:43:48	0011	100
00040E1E8A86		6	22 Mbps		AP	WEP	-90	-100	10	15:43:28	15:43:29	0011	200
000F3D97BE14	G664T_WIRELESS	6	22 Mbps		AP		-90	-100	10	15:43:14	15:43:17	0001	200
0030F1F5B825	WLAN	11	22 Mbps	Accton	AP	WEP	-68	-100	32	15:43:08	15:43:17	0011	100
00095B95951A	NETGEAR	11	22 Mbps	Netg...	AP		-71	-100	29	15:43:08	15:43:17	0001	100
0030F1FC42D0	WLAN	11	22 Mbps	Accton	AP	WEP	-90	-100	10	15:42:56	15:42:57	0011	100
0030F1D6A167	WLAN	11	22 Mbps	Accton	AP		-90	-100	10	15:42:28	15:42:57	0001	100
525D3E5772CB	Fingerweg	6	11 Mbps	(User-...	Peer		-70	-100	30	15:42:24	15:42:32	0002	100
0030F1E1F5EA	WLAN	11	22 Mbps	Accton	AP	WEP	-77	-100	23	15:42:20	15:42:57	0011	100
0030F1BAD838	WLAN	11	11 Mbps	Accton	AP	WEP	-90	-100	10	15:42:14	15:42:17	0011	100
000FB51A29CC	NETGEAR	11	11 Mbps		AP	WEP	-73	-100	27	15:42:14	15:42:26	0011	100
0030F1A2C5DE	WLAN	11	11 Mbps	Accton	AP		-90	-100	10	15:42:13	15:42:25	0001	100
000D88298383	default	6	11 Mbps	D-Link	AP	WEP	-86	-100	14	15:41:54	15:41:56	0011	100
00095BAD2440	NETGEAR	11	11 Mbps	Netg...	AP	WEP	-60	-100	40	15:41:51	15:42:06	0011	100
0080C8136AE7	default	1	22 Mbps	D-Link	AP	WEP	-66	-100	34	15:39:10	15:41:47	0011	100
0030F1B6065D	Nicos-Web	11	11 Mbps	Accton	AP	WEP	-69	-100	31	15:39:06	15:41:51	0011	100
0080C8AFEE72		6	22 Mbps	D-Link	AP	WEP	-83	-100	17	15:38:22	15:38:37	0011	100
00095B9A182C	NETGEAR	11	11 Mbps	Netg...	AP	WEP	-90	-100	10	15:38:15	15:38:16	0011	100
0001E30A80F3	ConnectionPoint	10	11 Mbps		AP		-90	-100	10	15:37:55	15:38:08	0001	100

MAC	SSID	C...	Speed	Vendor	Ty...	En...	S...	N...	S...	First S...	Last S...	Fla...	B...
0030F1CC1A74	154XR	11	11 Mbps	Accton	AP		-90	-100	10	15:37:26	16:04:24	0001	100
000D88866F6B	default	6	22 Mbps	D-Link	AP	WEP	-90	-100	10	15:36:03	15:36:07	0011	100
00119509E52C	wrouter	8	22 Mbps	(Fake)	AP	WEP	-75	-100	25	15:35:59	15:36:03	0011	100
0030F1E5F6AF	WLAN	11	22 Mbps	Accton	AP		-90	-100	10	15:35:49	15:35:52	0001	100
0030F1D67BC0	WLAN	11	22 Mbps	Accton	AP		-90	-100	10	15:35:49	15:35:51	0001	100
000F66903A8C	linksys	11	54 Mbps	Linksys	AP		-70	-100	30	15:35:21	15:35:33	0001	100
00055DEBDF5E	123	6	11 Mbps	D-Link	AP		-83	-100	17	15:35:05	15:35:18	0001	90
0030F1D2ABE7	WLAN	11	11 Mbps	Accton	AP		-81	-100	19	15:34:53	15:35:01	0001	100
00A0C563224B	kaisicher	6	11 Mbps	Zyxel	AP		-74	-100	26	15:34:48	15:35:03	0001	100
0030AB1EE47F	hau_ab	11	11 Mbps	Delta ...	AP		-90	-100	10	15:34:46	15:34:46	0001	100
00A0C573838E	kaisicher	6	22 Mbps	Zyxel	AP		-90	-100	10	15:34:38	15:34:38	0001	200
0030F1AAC739	WLAN	11	11 Mbps	Accton	AP	WEP	-71	-100	29	15:34:37	15:35:05	0011	100
0030F19D419C	WLAN	5	11 Mbps	Accton	AP		-86	-100	14	15:34:34	15:34:35	0001	100
0004E2AD9B00		9	11 Mbps	SMC	AP	WEP	-90	-100	10	15:34:33	15:34:35	0011	100
0001E3033E5C	ConnectionPoint	10	11 Mbps		AP	WEP	-78	-100	22	15:34:19	15:34:27	0011	100
00055DEBE688	CONCEPTLAN	6	11 Mbps	D-Link	AP	WEP	-90	-100	10	15:34:14	15:34:14	0011	90
000CF6082545	default	11	54 Mbps		AP		-90	-100	10	15:34:00	15:34:00	0001	100
0001E30A764F		10	11 Mbps		AP	WEP	-90	-100	10	15:33:43	15:33:52	0011	100
000F3D48CF30	default	6	22 Mbps		AP		-72	-100	28	15:33:37	15:34:04	0001	100
000F3D61B822	default	6	22 Mbps		AP		-74	-100	26	15:33:30	15:33:50	0001	100
0030F1EF1450	WLAN	11	22 Mbps	Accton	AP		-68	-100	32	15:33:07	15:33:18	0001	100
0003C9441F43	WLAN	11	54 Mbps		AP		-90	-100	10	15:33:02	15:33:06	0001	100
0030F1AA5F3A	WLAN	1	11 Mbps	Accton	AP		-90	-100	10	15:32:36	15:32:36	0001	100
0030F1E573CC	WLAN	11	22 Mbps	Accton	AP	WEP	-81	-100	19	15:32:27	15:32:36	0011	100
0030F1DF30B0	WLAN	11	22 Mbps	Accton	AP	WEP	-78	-100	22	15:32:27	15:32:36	0011	100
0030F17E6878	WLAN	13	11 Mbps	Accton	AP		-90	-100	10	15:31:47	15:31:49	0001	100
00A0C5C05728	kima	6	22 Mbps	Zyxel	AP	WEP	-70	-100	30	15:31:19	15:31:30	0011	200
0030F1E7B5A6	WLAN	11	22 Mbps	Accton	AP		-71	-100	29	15:29:12	15:29:16	0001	100
0030F1E5FB02		11	22 Mbps	Accton	AP	WEP	-90	-100	10	15:28:41	15:28:46	0011	100
0030F1BAE6ED	WLAN	11	11 Mbps	Accton	AP		-90	-100	10	15:28:27	15:28:29	0001	100
00040E1E2567	FRITZ!Box Fon WLAN	6	22 Mbps		AP	WEP	-89	-100	11	15:28:19	15:28:28	0011	100
00040E3629EC	FRITZ!Box Fon WLAN	6	22 Mbps		AP	WEP	-89	-100	11	15:28:18	15:28:28	0011	100
000FB5151B1A	FUENGERLINGS	4	11 Mbps		AP	WEP	-90	-100	10	15:27:49	15:27:52	0011	100
02003606582D	gpsoft	10	11 Mbps	(User-...	Peer	WEP	-74	-100	26	15:27:31	15:27:39	0012	100
0030F1D51725		11	11 Mbps	Accton	AP		-90	-100	10	15:27:31	15:27:32	0001	100
000F3D97C592	uEvoli.Net	6	22 Mbps		AP		-88	-100	12	15:27:16	15:27:18	0001	200
001150099474	belkin54g	11	54 Mbps	(Fake)	AP		-70	-100	30	15:26:44	15:26:47	0001	100
00027245221F	Acer	11	11 Mbps	CC&C	AP	WEP	-90	-100	10	15:26:42	15:26:42	0011	100
000124F45616	WLAN	1	11 Mbps	Acer	AP	WEP	-87	-100	13	15:26:27	15:26:34	0011	100
0001E30A7967		10	11 Mbps		AP		-90	-100	10	15:26:26	15:26:27	0001	100
00904B172131	default	6	11 Mbps	Gemtek	AP	WEP	-90	-100	10	15:26:16	15:26:22	0011	100
004005CAD5BA	homeoffice	6	22 Mbps	D-Link	AP	WEP	-78	-100	22	15:26:13	15:26:22	0011	100
00095B2DF7AA	Speedynet	10	11 Mbps	Netg...	AP		-79	-100	21	15:26:09	15:26:22	0001	100
000C417ED50A	Home	11	11 Mbps	Linksys	AP	WEP	-83	-100	17	15:26:01	15:26:12	0011	100
000D88F38BA8	default	6	22 Mbps	D-Link	AP		-75	-100	25	15:25:40	15:25:43	0001	100
0001E30B63E2		11	54 Mbps		AP	WEP	-90	-100	10	15:24:08	15:24:18	0011	100
0011500982BF	orlando	11	54 Mbps	(Fake)	AP	WEP	-73	-100	27	15:24:05	15:24:18	0011	100
0030F1BEA582	belkin54g	11	11 Mbps	Accton	AP		-83	-100	17	15:23:56	15:24:18	0001	100
0030F1A4CD76	WLAN	10	11 Mbps	Accton	AP		-90	-100	10	15:21:29	15:21:32	0001	100
0001E30FC439	ConnectionPoint	11	54 Mbps		AP		-73	-100	27	15:21:13	15:21:20	0001	100
000D8835F707	default	6	11 Mbps	D-Link	AP		-79	-100	21	15:20:54	15:21:00	0001	100
00A0C5FA94A7	rene	6	22 Mbps	Zyxel	AP		-72	-100	28	15:20:46	15:20:50	0001	200
0001E308806A	ConnectionPoint	11	54 Mbps		AP		-90	-100	10	15:20:37	15:20:37	0001	100
0030F174D5F1	WLAN	7	11 Mbps	Accton	AP		-72	-100	28	15:20:33	15:20:46	0001	100
0011500DEE75	belkin54g	11	54 Mbps	(Fake)	AP		-90	-100	10	15:20:09	15:21:24	0001	100
0030F197A242	WLAN	8	11 Mbps	Accton	AP		-90	-100	10	15:20:03	15:20:03	0001	100
00027203F0F8	Acer	11	11 Mbps	CC&C	AP		-74	-100	26	15:19:59	15:20:09	0001	100
00904B170EBC	Gratza	6	11 Mbps	Gemtek	AP	WEP	-87	-100	13	15:19:47	16:04:44	0011	100

Anhang 4.1

Aktiver Angriff

64 Bit Verschlüsselung wurde mit aktivem Angriff versucht zu knacken.

	Schlüssel	***Zeit***	***Versuche***
1	zyhix	5 sek.	11851188
2	abdce	1 sek.	19661
3	cxkli	2 sek.	1325255
4	rpsad	3 sek.	8044404
5	gzdaw	3 sek.	3183307

Bei der aktiven Attacke auf einen 13 zeichenlangen Schlüssel ist der Rechner abgestürzt und darauf hin wurden die Test für diese Schlüssel eingestellt. Als Auslöser vermute ich einen Buffer Overrun.

Quelltext des selbst geschriebenen Testprogramms

```
procedure TForm1.Button1Click(Sender: TObject);
var a1, a2, a3, a4, a5 : char;
    b, c : string[5];
    d : longint;
begin
 b:= edit1.text ;
 {hier könnte noch eine Formatprüfung erfolgen,
  ob b wirklich 5-stellig ist und nur aus Kleinbuchstaben besteht}
 d:= 0;
 for a1 := 'a' to 'z' do
  begin
   for a2 := 'a' to 'z' do
    begin
     for a3 := 'a' to 'z' do
      begin
       for a4 := 'a' to 'z' do
        begin
         for a5 := 'a' to 'z' do
            begin
```

```
            inc(d);
            c := concat(a1, a2, a3, a4, a5);
            if c = b then break;
           end;
          if c = b then break;
         end;
        if c = b then break;
       end;
      if c = b then break;
     end;
    if c = b then break;
    end;
     if c = b then break;
end;
     Label1.caption :=inttostr(d);
     label2.caption:= c    ;
     Label3.Caption:= inttostr(zeit)   ;
end    ;
```

Anhang 5.1

Abgeschlossen und durchnummeriert

Wie man Funk-Netzwerke besser sichert

Von Rafael Heiling

Wenn Informationen durch die Luft schwirren, haben es Eindringlinge leicht: Drahtlose Heimnetzwerke sind recht leicht zu knacken - mit Software aus dem Internet. Eine Verschlüsselung macht die Daten zumindest sicherer.

Die Gefahr bei drahtlosen Netzwerken (Wireless Local Area Networks, kurs WLAN) ist: Möglicherweise können sich Fremde heimlich ins Netzwerk einklinken, beispielsweise von draußen mit dem Laptop, und dann auf Kosten des WLAN-Besitzers surfen oder in seinem Namen Spam versenden.

Dagegen ist theoretisch ein Kraut gewachsen: Man kann die Datenpakete verschlüsselt im Netzwerk umherschicken, indem man WEP (Wired Equivalent Privacy) aktiviert. Dann müssen sich auch alle Geräte, die ins Netzwerk wollen, ausweisen („authentifizieren"). Bei WEP zählt vor allem die Länge der Codes („Schlüssel"), 128 Bit sollten es schon sein.

Das ist dann besser als nichts, aber ein Angreifer kann mit ein paar Stunden Zeit die verschlüsselung knacken. Software schneidet die Datenpakete mit und reimt sich auf der Grundlage den Schlüssel zusammen. Programmpakete wie „Aircrack" sollen sogar nur Sekunden brauchen.

Dagegen ist WPA (Wi-Fi Protected Access) die bessere Lösung - wer ein Gerät hat, das es unterstützt, sollte WPA aktivieren. Dann nämlich werden die Schlüssel in Abständen automatisch geändert, damit Angreifer weniger Zeit haben, sie herauszubekommen.

Eine weitere Methode, um sein drahtloses Netzwerk sicherer zu machen, ist der MAC-Filter, eine Art digitale Gästeliste: Darauf stehen die Nummern der Geräte, die ins Netzwerk dürfen, also am besten nur die eigenen. Die MAC-Nummern muss man an der WLAN-Basisstation eingeben - sie werden als „physikalische Adresse" aufgelistet, wenn man im MS-DOS-Fenster „ipconfig/all" eingibt.

Quelle: Tageszeitung WAZ vom 10.02.05

Literaturverzeichnis

Primärliteratur:

Thomas Köhre, Wireless Lan – Das kabellose Netzwerk, Markt+Technik Verlag, 2003

Bundesamt für Sicherheit in der Informationstechnik, Projektgruppe "Local Wireless Communication", 2003, (http://www.bsi.bund.de/literat/doc/wlan/wlan.pdf, 05.02.2005)

Rafael Heiling, WAZ vom 10. Februar 2005

Sekundärliteratur:

http://de.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol , 08.02.05

http://de.wikipedia.org/wiki/WPA , 08.02.05

http://de.wikipedia.org/wiki/WEP ,

http://de.wikipedia.org/wiki/Advanced_Encryption_Standard , 08.02.05

http://www.lancom-systems.de/produkte/lc_1811_wireless_dsl.php , 08.02.05

Bildverzeichnis

Titelblatt:

Laptop -
http://images.google.de/imgres?imgurl=http://www.futurecomputers.co.uk/images/PC/easyonesilver/refurbished-laptop-laptops.jpg&imgrefurl=http://www.futurecomputers.co.uk/acorn/refurbished-laptop-laptops.html&h=222&w=248&sz=9&tbnid=L8jxXECt49YJ:&tbnh=94&tbnw=105&start=2&prev=/images%3Fq%3DLaptop%26hl%3Dde%26lr%3D (10.02.2005)

Kabelsalat -
http://images.google.de/imgres?imgurl=http://lustich.de/bilder/kabelsalat.jpg&imgrefurl=http://lustich.de/lustich/bilderdb-bilder-8-62.html&h=378&w=600&sz=69&tbnid=8NJzS-Hu0skJ:&tbnh=83&tbnw=132&start=18&prev=/images%3Fq%3DKabelsalat%26hl%3Dde%26lr%3D (10.02.2005)

Schlusserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und ohne fremde Hilfe verfasst und keine anderen als die angegebenen Hilfsmittel verwendet habe.
Insbesondere versichere ich, dass ich alle wörtlichen und sinngemäßen Übernahmen aus anderen Werken als solche kenntlich gemacht habe.

Oberhausen, den .....

Unterschrift des Schülers: