

## Wireless LAN :: Unsecure Network

Informationen für Einsteiger & Fortgeschrittene  
© 2003 by M.Rogge

Immer häufiger werden in Supermärkten so genannte Wireless Netzwerkkarten und Starter-Kits für Wireless Netzwerke angeboten.

Gerade für den privaten Bereich eine sehr interessante Erweiterung, wenn man an die Vernetzung innerhalb eines Hauses von 4-5 Computern oder mehr denkt.

Ein Wireless Access Point (kurz AP) schafft schnell die Möglichkeit ein Netzwerk über Funk aufzubauen, so dass die Computer drahtlos miteinander kommunizieren können.

So verlockend die Angebote im privaten Netzwerkbereich sind, so umfangreicher und entsprechend vielseitiger sind die Möglichkeiten Wireless LAN in Firmen einzusetzen.

Jedoch steigen mit den Möglichkeiten der Nutzung von Wireless LAN auch die Möglichkeiten der Angriffe auf ebensolche Netzwerke.

Die größten Vorteile jedoch liegt auf der Hand:

- kabellose Kommunikationen von vielen Clients, Hosts und/oder Servern
- Übertragung großer Datenmengen durch Wireless LAN möglich
- grosszügige Teilung von vorhandenen Ressourcen
- schnelle Einwahl in das WWW auf verschiedene Möglichkeiten
- schnelle, bequeme und kostengünstige Erweiterung bestehender Netzwerke

Mit einem Laptop und einer Wireless Lan Karte bewaffnet kann man somit eine Reichweite von ca. 150 Meter erreichen oder in freier Natur und zusätzlichen Antennen (z.B. 5dB Abstrahler) bis zu 2,5 Kilometer.

Am Ende werde ich Ihnen weitere Lesemöglichkeiten aufzeigen, die sich grundlegend mit dem Thema des Funknetzwerkes Wireless Lan befassen.

Hier möchte ich jedoch weiter auf die Gefahren eingehen, die fast immer unterschätzt werden!

Grundsätzlich kann man derzeit noch von einer erhöhten Gefahr in Wireless LAN ausgehen, da Sicherheitsanalysen oder Sicherheitseinstellungen zu selten wahr genommen werden.

In Unternehmen oder in privaten Wireless LAN kann man sich durchschnittlich bei 7-8 von 10 Netzwerken anmelden und über die dortige Interneteinwahl bequem auf deren Kosten mitsurfen.

Des weiteren besteht somit oftmals auch die Möglichkeit, dort freigegebene Ressourcen zu nutzen und einzusehen.

Bei den meisten Netzwerken handelt es sich um Netzwerke mit Windows2000 als Server und/oder Betriebssystem und dort sind nach den Standard Einstellungen Shared Ordner freigegeben.

Diese Ordner werden natürlich der Bequemlichkeit zugute genutzt, um Daten innerhalb eines Netzwerkes zu tauschen.

Sehr fahrlässig.

Natürlich sollte hier erwähnt werden, dass es nicht nur in Wireless LANs fahrlässig ist, sondern auch in allen Netzwerken in denen Daten transparent sind.

Wireless Netzwerke sind genau wie herkömmliche Netzwerke per IP Adresse durch das Internet oder über Wireless aufzufinden und dadurch natürlich ebenfalls zu identifizieren.

Anhand des unten stehenden Bildes kann man sehr schön erkennen, wie sich die einzelnen Funknetze identifizieren und nach außen zu erkennen geben:

MAC	SSID	Name	Chan	Vendor	Type	Encryption	SNR	Signal+	Noise
00:0C:84:56	default		6	Advanced Multimedia Inte...	AP			-58	-90
00:0C:84:56			6, 11	Linksys	AP			-1	-97
00:0C:84:56			11	Agere [Lucent] Orinoco	AP			32	-94
00:0C:84:56			11	Cisco [Aironet]	AP	WEP		-40	-93
00:0C:84:56			3	Agere [Lucent] Orinoco	AP			-64	-90

Was sehen wir hier im einzelnen?

Anfangs kann man die MAC Adresse der Hardware erkennen, die verwendet wird.

Weiterhin ist die sogenannte SSID zu erkennen.

Ebenfalls ist erkennbar, dass eines von den hier 5 Wireless APs mit der WEP geschützt ist.

Was aber ist Service Set Identifier, kurz SSID genannt?

Die SSID ist für die Erkennung sowie die Unterscheidung der Netzwerke zuständig, die von Herstellern mitgeliefert wird.

Mit einer SSID identifiziert sich ein Access Point eines Wireless LAN.

Die erste Gefahr liegt also darin, dass sich ein Access Point (kurz AP) meistens in der Standard Einstellung mit seinem Namen identifiziert und somit einem Hersteller zugeordnet werden kann.

Buglisten von Herstellern sind im WWW schnell eingesehen und Exploits dafür auffindbar.

Eine Liste von Fingerprints ist hier einsehbar: [Unbolted Network](#).

Was aber ist weiterhin eindeutig erkennbar?

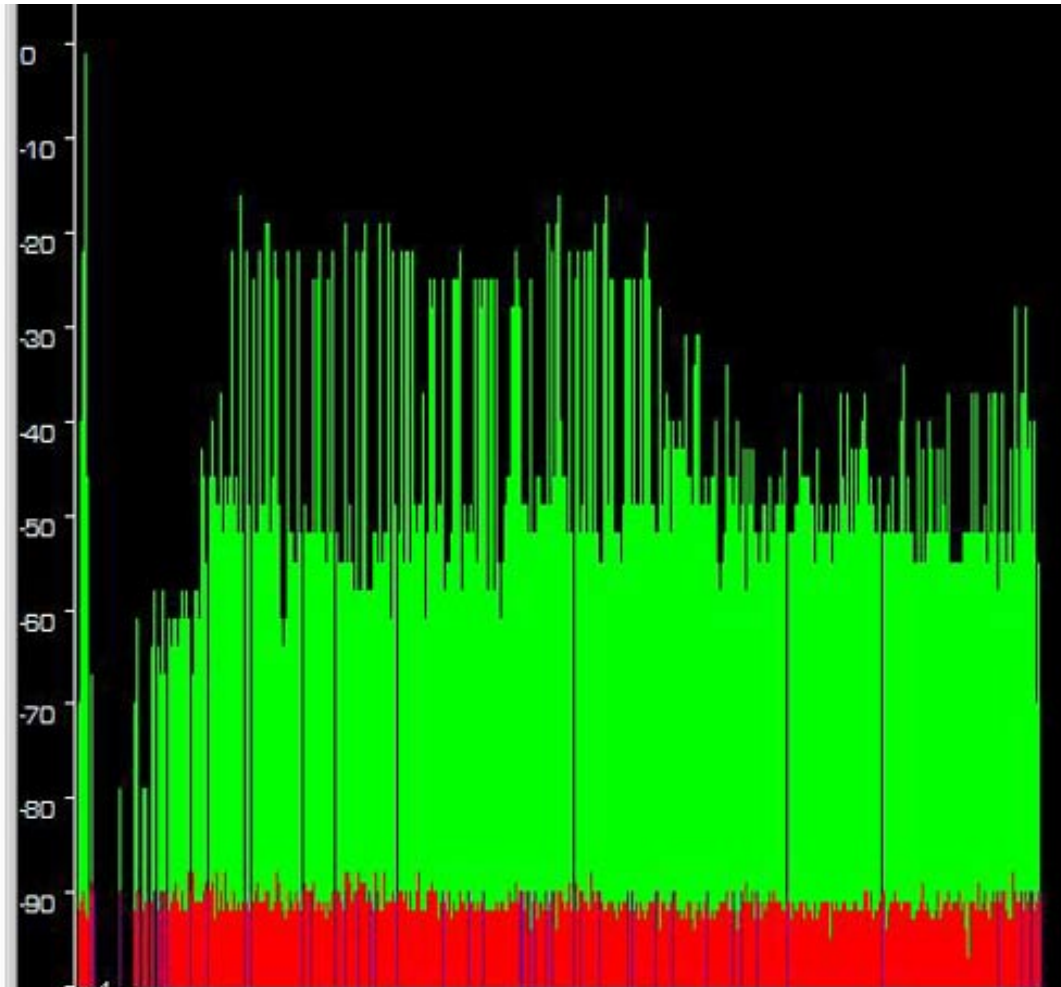
Die benutzten Kanäle über die derzeit dort kommuniziert wird sind eindeutig erkennbar.

In meinem Beispiel kann man die Kanäle 6, 11 und 3 in aktiver Kommunikation sehen.

Im Beispiel des Programmes das hier Anwendung findet wird angezeigt, welcher Hersteller sich hinter dem AP verbirgt.

So sieht man hier die Hersteller von Linksys über Lucent bis hin zu AVI.

Die Signalstärke gibt hier in diesem Programm Aufschluss darüber, wie leistungsstark die Kommunikation ist und wie sicher die Verbindung wäre, wenn man sich mit diesem Einwahlknoten von dem betreffenden Standort aus verbindet.



Anzeige der Sendeleistung mit Netstumbler

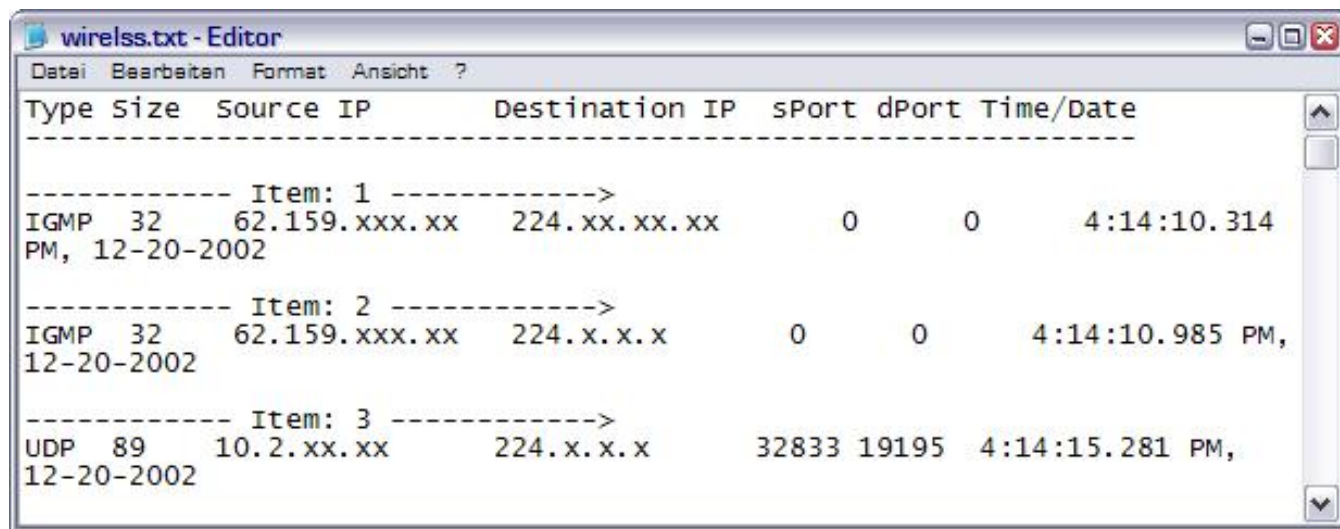
Im Beispiel des Bildes oben kann man sehen, dass die Netzwerke nicht mehr erreichbar sind, aber über eine gewisse Zeit konnten eindeutige Signale empfangen werden.

Kurzum, eine recht schnelle Analyse ist hier möglich um zu erkennen, welches Netzwerk man benutzen möchte um sich frei im Internet zu bewegen.

**WICHTIG:** Das Einwählen in fremde Netzwerke und Ausspähen von fremden Netzwerken ist NICHT LEGAL und wird auch in Deutschland mit Strafen belegt.

Ein zufälliges Antreffen eines Netzwerkes mag da schon anders aussehen, solange kein Schaden entsteht und/oder Daten entwendet werden :-)

Sollte man nun rein zufällig den Netzwerkverkehr einsehen können, so werden sich Informationen offenbaren die für einen Angreifer sehr hilfreich sein können:



Type	Size	Source IP	Destination IP	sPort	dPort	Time/Date
----- Item: 1 ----->						
IGMP	32	62.159.xxx.xx	224.xx.xx.xx	0	0	4:14:10.314 PM, 12-20-2002
----- Item: 2 ----->						
IGMP	32	62.159.xxx.xx	224.x.x.x	0	0	4:14:10.985 PM, 12-20-2002
----- Item: 3 ----->						
UDP	89	10.2.xx.xx	224.x.x.x	32833	19195	4:14:15.281 PM, 12-20-2002

Der Netzkerverkehr wird deutlich erkennbar und somit transparent für den Angreifer, der sich eines Netzwerkes bemächtigen will, zu welchem Zweck auch immer.

Hierbei ist durchaus schnell erkennbar, welcher Netzwerktraffic von welchem Client zum anderen gesendet wird oder welcher Server mit welchem Client kommuniziert.

Portzuweisungen sind ebenfalls schnell einsehbar und somit werden die Möglichkeiten der Angreifbarkeit dieses Netzwerkes immer größer.

Ich habe weiter oben bereits WEP angesprochen.

Was aber verbirgt sich hinter WEP?

Im Beispiel des ersten Bildes haben wir aber gesehen, dass es ein verschlüsseltes Netzwerk gab, dass mittels des Standards WEP verschlüsselt wird.

WEP = Wired Equivalent Privacy.

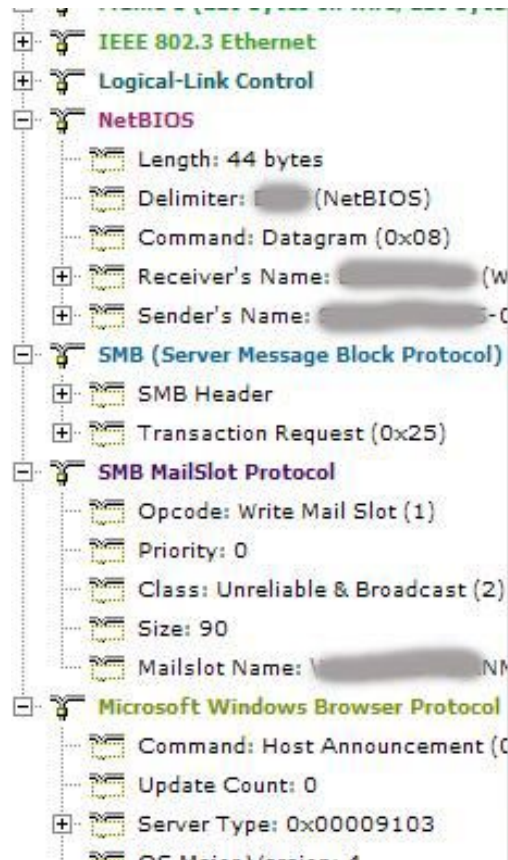
Die Verschlüsselung der Kommunikation auf diesem Wege ist bereits mehrfach kritisiert worden, da diese ebenso häufig als unsicher eingestuft wurde.

Ist aber ein Netzwerk zunächst einmal wenigstens mit einer WEP Verschlüsselung konfiguriert, so ist für einen Angreifer eine weitere Hürde die er nehmen muss, wenn er auf dieses Netzwerk zugreifen möchte.

Eine Hürde, die aber wie nachfolgend kurz aufgeführt nur von kurzer Dauer sein kann und im Falle eines Angriffes sein wird.

Im Falle das eine WEP Verschlüsselung auf dem Netzwerk zum tragen kommt, kann man beispielsweise das Programm Aircrack für Linux zur Hand nehmen, dass dafür konzipiert wurde WEP Algorithmen zu attackieren.

Eine Wireless LAN Karte mit dem Chipsatz Prism2 sowie die Softwaretreiber wlan-ng reichen beinahe schon fast aus.



Hier ist sehr schön erkennbar, wie ein Netzwerk mit seiner Struktur ausgelesen wurde.

In erster Linie ist so eine Darstellung darauf zurück zu führen, dass in den meisten Wireless Lan wie auch in herkömmlichen Netzwerken die automatische Zuweisung der IP Adresse von einem DHCP-Server erfolgt. Ist ein Wireless Access Point in ein herkömmliches Netzwerk integriert, so hat ein Angreifer die Möglichkeit alle Daten einzusehen wie jeder, der sich innerhalb dieses Netzwerkes bewegen kann.

Wie aber gelangen Angreifer nun an die Informationen, die benötigt werden um ein Netzwerk auszubeuten und für Ihre Zwecke zu mißbrauchen?

**Wardriving!**

Hierbei geht es darum, sich mit einem geeigneten Fahrzeug in einem Gebiet zu bewegen, wo ein Funknetzwerk vermutet wird.

Mit einem Laptop bewaffnet, einer entsprechenden WLAN Karte und einem Auto befahren dann Wardriver solche Gebiete und suchen es nach Funknetzen ab.

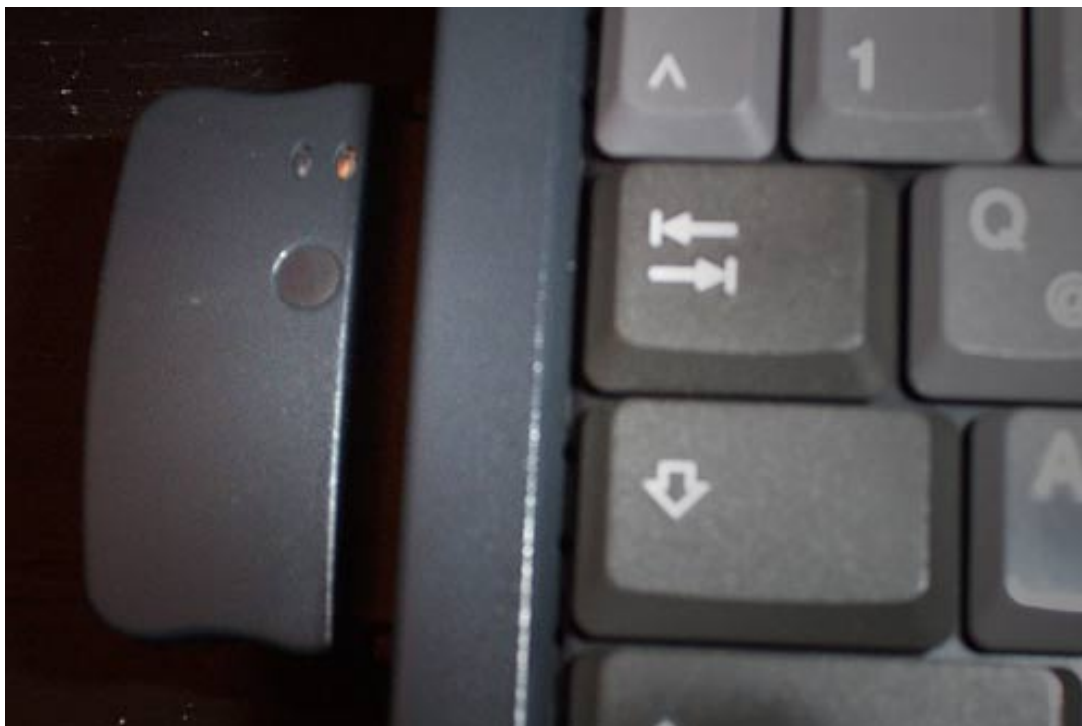
Dabei wird nach dem ersten Schema dann bereits das Funknetz mit der Signalstärke und den ersten Informationen "abgegriffen".

Solche Software ist bereits so klein programmiert worden, dass man eine entsprechende Software für Handheld PC schon bekommen kann und diese Information in einer Landkarte über GPS eingetragen werden kann.

Dies kann über ein Programm für Windows funktionieren, das Stumbverter heißt.

Das Programm ermöglicht dann die Daten die man empfangen hat per GPS in eine digitale Karte einzutragen.

([Stumbverter Homepage](#))



Eine Wireless Lan Karte in einem Notebook, kaum merklich größer.

Mit einer solchen Karte ist man dann schon einmal Empfangsbereit für Informationen aus den Funkbereichen Wireless:

<b>Kanal</b>	<b>Frequenz (GHz)</b>
1	2,412
2	2,417
3	2,422
4	2,427
5	2,432
6	2,437
7	2,442
8	2,447
9	2,452
10	2,457
11	2,462

Hat man also ein Wireless Lan gefunden und man hat die nötigen Informationen, dass keine Verschlüsselung aufliegt oder das Netzwerk per MAC Adressierung geschützt ist, kann man sich einwählen.

Dies ist per Windows in jeglicher Hinsicht relativ schnell möglich, ohne das man weitere Programme benötigt.

Im Normalfall würde in der Taskleiste ein Systemsymbol erscheinen, dass ein Netzwerk anzeigt mit einem roten Kreuz.

Man klickt dann mit der Maus drauf, geht auf die Eigenschaften und Microsoft Windows konfiguriert das Netzwerk automatisch für das Netzwerk.

In ca. 90% der angetroffenen Netzwerke bucht sich das Windows dann selbständig ein und man kann problemlos surfen.

Zur Sicherheit um die IP Adressverteilung zu prüfen, kann man den Befehl IP Config/all unter Start - Ausführen in der CMD ausführen.

Je nach dem welche Möglichkeiten zur Verfügung stehen, werden Autos, Fahrräder oder gar Flugzeuge verwendet. Dafür steht dann aber schon der Begriff Warflighing.

Viele der Wardriver die ein Funnetzwerk erreichen über das ein Zugriff ins WWW ermöglicht wird, behalten zunächst einmal diese Information für sich und werten diese aus.

Anschliessend werden durch entsprechende Symbole Hauswände markiert die einem Wardriver dann wiederum aufzeigen, ob ein Zugang möglich ist.

Momentan ist die Rechtslage nicht ganz geklärt, was die Situation des durchsuchen von Wireless Lan betrifft.

Jedoch kann man davon ausgehen, dass das stehlen und manipulieren von Daten dort genauso unter Strafe steht wie bei herkömmlichen Netzwerken.

In vielen Unternehmen wo Funknetzwerke aka Wireless LAN in der Zukunft eingesetzt werden, wird grundlegend nicht auf die Sicherheit eingegangen und das Netzwerk erstmal zum Einsatz kommen.

Die meisten Software- und Hardwarehersteller sind darauf bedacht, die Ware zu verkaufen und entsprechend bei der ersten Einrichtung behilflich zu sein.

Weitere Informationen zum Datenschutz und zur Sicherheit des Netzwerkes unter Einsatz von Wireless LAN werden fast immer vergessen?

Hierzu empfehle ich zum einen die weitergehenden Informationen sowie die Security Check Liste.

Weiterführende Informationen:

Committee IEEE LMSC

IEEE offizielle Page

Wellenreiter :: Linux & Handheld Tool, englisch

Aerosol :: Wardriving Tool für Windows, englisch

Offizielle Seite zu Netstumbler :: Tool zur Wireless Lan Analyse

WEP Analyse schnell gemacht :: WEP Crack, Linux

Airsnort :: Analyse WEP, wlan-ng Treiber etc.

Informationsseite :: Deutsch, Sicheres Funknetz

Security Paper Wireless Lan :: Deutsch, Xaitax

Dokumente Wireless Security :: Computec Webseiten

Vantronix :: Securitylösungen für Wireless Lan

Danke für Korrekturen und Vorschläge: skeptiker , V|RuS, Mixer , TheSentinal

Beste Grüße, Marko Rogge, Brain-Pro Security // www.brain-pro.de

Dieser Bericht ist in guter Absicht und mühsamer Arbeit erstellt worden, daher möchte ich Sie bitten keine Anleitung und/oder andere Texte frei zu kopieren.

Unter Angabe des Autors und der URL sowie eine Benachrichtigung per E-Mail ist eine weitere Veröffentlichung jederzeit möglich.

Danke, Ihr Marko Rogge