[ebook] WLAN – WarDriving

ripped and ebooked by
the evil dicks in 2003

WLAN

Von Martin Puaschitz (onestone)

Dieser Artikel behandelt die (oft nicht vorhandenen) Sicherheitsaspekte bei WLAN's. Es wird erklärt war WarDriving und WarChalking ist und wie es funktioniert. Des weiteren eine kleine Einführung wie man den WLAN-Verkehr abhört und die Theorie hinter einem erfolgreichen WEP-Angriff. Als Abrundung einige Tipps und Tricks für das hauseigene WLAN und wie man es schützen kann.

Inhalt

1 Einleitung

WLAN - alle reden davon, viele benutzen es, doch nur wenige wissen eigentlich, was dahinter steckt und vorallem: Welches Risiko sie teilweise eingehen. Wer sich mit WLAN genauer beschäftigt, erkennt schnell, dass nicht alles Gold ist, was glänzt. Die Technologie ist wunderbar, wenn nicht gerade grandios. Aber wie so oft, muss gerade bei neuem mit größerer Vorsicht an die Sache herangegangen werden.

Dieses Dokument soll mehrere Funktionen gleichzeitig erfüllen:

- Die Thematik möglichst Praxisnah aufgreifen & als eines der wenigen frei verfügbaren - deutschsprachigen - Dokumente den Sachverhalt erklären.
- Administratoren, die ein WLAN betreiben, Hintergrundwissen und Schutzmaßnahmen näher zu bringen.
- 'Hackern', oder solche die es sein wollen, einen interessanten, verwundbaren Punkt in fremden LAN-Strukturen zu zeigen.

Ich stehe weitere Ideen, Rat- & Vorschlägen, Verbesserungen und dergleichen offen gegenüber. Bitte einfach ein entsprechendes E-Mail an mpuaschitz@it-academy.cc senden.

2 WLAN - Eine Definition!

Die Abkürzung WLAN bedeutet 'Wireless Local Area Network' oder auch 'drahtloses Funknetzwerk'. Der Grundgedanke besteht darin, Clients via Funk an Netzwerke anzubinden und somit einen einfachen, schnellen Zugriff zu gewährleisten. Die Vorteile liegen auf der Hand: Der Arbeitsplatz kann quasi überall platziert werden und es müssen keine Kabel verlegt werden. Eine weitere interessante Anwendung ist das Anbieten von WLAN's in Hotels, Flüghäfen und Café's - somit sind Kunden immer und überall mit dem Internet verbunden und es braucht keine lästigen Kabeln, Modems, etc. Aber auch in Umgebungen, wo lediglich Datentransfer zwischen zwei Geräten gewünscht wird, bietet WLAN eine Möglichkeit ('Ad-Hoc'-Modus).

Es gibt bereits sei 1992 verschiedene Implementierungen von Funknetzwerken. Allerdings brachte erst der IEEE 802.11 Standard ein Konzept in das Chaos dass mitlerweile von allen Herstellern und Softwareproduzenten übernommen wurde. Daher ist es nun möglich, mit verschiedenen Geräten auf denen verschiedene Betriebssysteme laufen, zu kommunizieren.

IEEE 802.11b

802.11b oder auch "WiFi" (sprich: WeiFei) genannt, ist quasi der aktuelle Standard in der WLAN-Funkwelt und wird mit grundsätzlich mit 11Mbit/s betrieben (je nach Auslastung können es allerdings auch 5.5Mbit/s, 2MBit/s oder gar 1MBit/s sein). 802.11b ist im 2,4 Ghz Bereich oder ISM-Bereich (ISM = Industrial, Scientific, Medical) aktiv - einem lizenzfreien Funkraum in denen auch Geräte wie Mikrowellen oder Bluetoothgeräte arbeiten.. Die meisten WLAN's werden mit diesem Standard betrieben, daher gibt es momentan hier auch die meisten Produkte, Informationen und Tools. Die primäre Verschlüsselungsform ist WEP (Wired Equivalent Privacy). WEP kann mit 64bit oder 128bit verschlüsselt werden, allerdings ist dies abhängig von der Hardware bzw. des Chipsatzes (Prism1 für 64bit, Prism2 für 64bit & 128bit).

Verschiedene Regionen verwenden verschiedene Bandbreiten innerhalb des ISM-Bereiches:

Region	**Frequenz in GHz**	**Nutzbare Sequenzen**
USA	2,4 - 2,4835	79
Europa	2,4 - 2,4835	79
Frankreich	2,4465 - 2,4835	27
Spanien	2,445 - 2,475	35
Japan	2,471 - 2,497	23

IEEE 802.11a

Dies wird eventuell der neue Standard nach 802.11b werden (obwohl 'b' nach 'a' kommt, ist 'a' neuer!). Im Vergleich zu .11b hat .11a die Möglichkeit Daten mit 54Mbit/s zu übertragen und verwendet das 5Ghz Funkband. .11a verwendet des weiteren OFDM (= Orthogonal Frequency Division Multiplexing Encoding) - wer mehr darüber wissen möchte, empfehle ich bei google nach 'ODFM' zu suchen - diese Erklärung würde die Grenzen dieses Dokumentes sprengen.

Warum 802.11b vor 802.11a?

Vielleicht fragen sich einige Leser, warum 'b' vor 'a' gekommen ist. Dass ist nicht die Willkür des Autors in diesem Dokument sondern der Zeitpunkt der Einführung der entsprechenden Hardware. Primär wollten die Entwickler die a-Version zuerst veröffentlichen. Das Problem war allerdings, dass manche Länder in Europa das 5Ghz-Funkband als Polizei/Feuerwehr/Rettungs-Funkband benutzten. Die Gefahr von Störungen war zu groß - man wollte aber einen allgemeinen Standard weltweit durchsetzen können. Daher wurde zuerst die 'b'-Variante realisiert. Mittlererweile haben Polizei/Feuerwehr/Rettung und dergleichen umgerüstet und die Migration zu 802.11a kann beginnen.

IEEE 802.11g

Noch eine Zukunftsversion - aber was nicht ist, kann ja bald werden. 802.11g wurde möglichst abwärtskompatibel gestaltet, aher wurde der "Complementary Code Keying (CCK)" von 802.11b implementiert um Transferraten von 5.5Mbps und 11Mbps im 2.4Ghz-Band zu ermöglichen. Zusätzlich wurde 802.11g auch mit ODFM (siehe 802.11a) ausgestattet, um 54Mbps zu ermöglichen - allerdings im 2.4Ghz-Bereich! 802.11g kommt auch mit optionalen und inkompatiblen Möglichkeiten um Daten mit 22Mbps zu übertragen. Diese sind Intersil's CCK-ODFM - durch welchen eine Maximallast von 33Mbps und TI's Packet Binary Convolutional Coding (PBCC-22) - durch welche eine Maximallast zwischen 6Mpbs und 54Mbps übertragen werden kann

802.11a und 802.11g ermöglichen also 55Mbps im Testversuchen. In der Praxis wird 802.11g in ewta 6Mbps bieten können, allerdings mit einer besseren Reichweite als 802.11a und 802.11b. 802.11g kann übrigends drei Kanäle auf einmal managen (in Testversuchen sind bereits 11 Kanäle möglich - Aethero Chips ermöglichen es).

IEEE 802.11f

Trotz des Standards 802.11b gibt es teilweise immer wieder Probleme zwischen den einzelnen Access Points (siehe unten). Dies soll mit 802.11f der Vergangenheit angehören, da sich diese Arbeitsgruppe um eine verstärkte Zusammenarbeit der Hersteller bemüht. Dies ist allerdings zum aktuellen Zeitpunkt erst in Diskussion.

IEEE 802.11i

Wie auch in diesem Dokument erwähnt (siehe unten), sind die Sicherheitsmechanismen von 802.11b unzureichend. Daher sind mit 802.11i Verbesserung von Verschlüsselung und Authentifizierung in Diskussion.

3 WLAN - Hardware

Wie immer gibt es für die verschiedensten Zwecke verschiedenste Hardware. Hier ein Überblick, welches Gerät wozu existiert.

Acccess Points

Access Points (=AP) sind in größeren Büros oder Häusern sehr nützlich. Sie leiten jenes Signal, dass sie empfangen in das Netzwerk weiter - ähnlich wie ein herkömmliches HUB wo alle Clients mit Kabel verbunden werden. Hier wird das Kabel einfach nur die Funkverbindung ersetzt.

Wireless Router

Es gibt auch AP's die weitere Funktionen wie integriertes xDSL-Modem oder normales Modem mitbringen. Diese (teureren) Geräte können somit selbständig - wenn gewünsch - eine Verbindung zum Internet aufbauen wenn Clients Datenpakete in's Internet schicken möchten. Dies ist vor allem dann sinnvoll, wenn keine ständige Internetverbindung vorhanden ist, allerdings bequem und schnell eine aufgebaut werden soll.

Wireless Network Interfaces

Im Prinzip eine Netzwerkkarte wie jede andere, nur Wireless und mit Antenne. Wird genauso verwendet wie eine herkömmliche Netzwerkkarte (mit Kabel) - sollte selbsterklärend sein.

Wireless PCMCIA Karten

Diese Karten sind für mobile Geräte wie Notebooks oder Handhelds gedacht. Durch den standardisierten PCMCIA-Slot kann eine Karte meist auch in mehren Geräten verwendet werden. Die derzeit wohl beste WLAN-PCMCIA-Karte ist wohl die Orinoco Gold Prism2 Card um etwa 80€. Das soll aber nicht bedeuten, dass andere Karten nicht ausreichen sein können. Grundsätzlich ist die Empfangs- & Sendestärke bei dieser Technologie als Qualitätsmaßstab festzusetzen.

Wireless Mini-PCI-Karten

Diese Form wird meist in Notebooks verwendet, die einerseits helfen sollen Platz zu sparen, andererseits die Möglichkeit bieten die PCMCIA-Slots frei zu halten. High-End-Notebooks bieten zudem die Möglichkeit diese Mini-PCI-Karten an integrierte Antennen (meist hinter dem Display) anzuschließen und dadurch einer besseren Sende- & Empfangsleistung zu erreichen. Interessant ist, dass einige Mini-PCI-Karten lediglich verkleinerte PCMCIA-Karten sind. Das erscheint technisch nicht besonders wichtig, allerdings ist es u.a. dadurch für Linux-User einfacher, diese Karten zu betreiben (weil PCMCIA schon meist unterstützt ist).

Antennen

Es gibt verschiedene Möglichkeiten an externe Antennen heranzukommen. Entweder (wie Normalsterbliche) im Geschäft kaufen oder (wie Freaks) selber nach Internet-Anleitungen welche bauen. Der Grundgedanke einer externen Antenne ist derselbe: Mehr Leistung und daher mehr Reichweite erzeugen. Die am häufigsten verwendete Form nennt sich "Yagi" wobei es verschiedene Kriterien für die verschiedenen Typen gibt. Die wohl bekannteste Geschichte aus den Medien ist es wohl, aus einer Pringles-Dose eine Antenne selbst bauen.

Mehr dazu unter bzw. weitere Bauanleitungen:

http://www.oreillynet.com/cs/weblog/view/wlg/448
http://verma.sfsu.edu/users/wireless/pringles.php
http://home.t-online.de/home/enigma1/quad2/
http://home.t-online.de/home/enigma1/Quad/

Eine Interessante Bauanleitung findet sich unter
http://216.239.53.104/search?q=cache:ltX22XDG3_4J:www.wwc.edu/~frohro/Airport/Primestar/Primestar.html+&hl=en&ie=UTF-8 - hier wird eine Satelitenschüssel als WLAN-Antenne verwendet.

4 Was ist WarDriving bzw. WarXing?

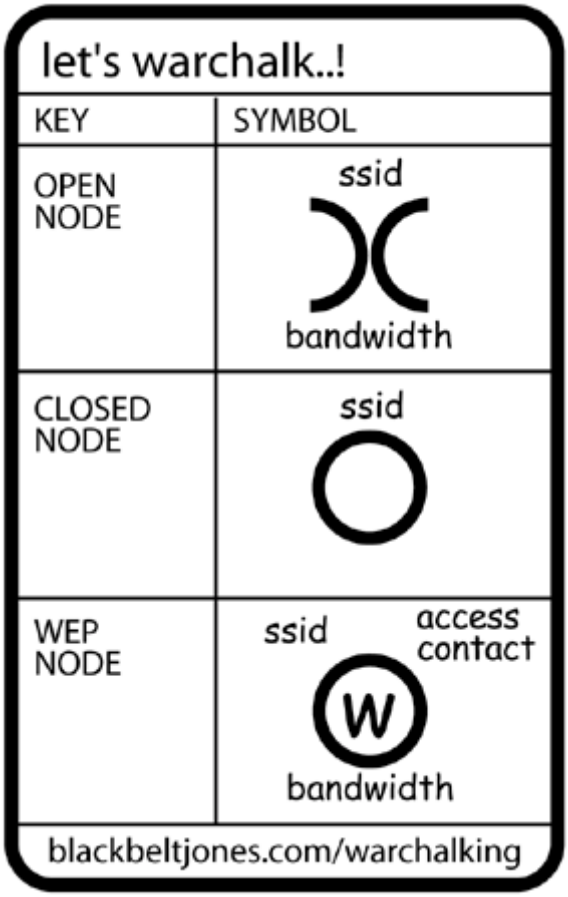
WarDriving bedeutet, mit entsprechender Ausrüstung in einem Auto herumzufahren und nach Drahtlosen Netzwerken (WLAN = Wireless Local Area Network) zu suchen. Der Ausdruck ist allerdings nur eine Abwandlung. Theoretisch gibt es auch WarBoating, WarFlying, WarWalking und vieles mehr. Das Prinzip der Namensgebung bezieht sich darauf, wie man die drahtlosen Netzwerke sucht: Im Auto, per Boot, per Flugzeug oder eben zu Fuß.

Man kann alle diese Begriffe zu "WarXing" zusammenfassen, wobei das X für die entsprechende Fortbewegungsmethode steht. Die Suche nach WLAN's und die dabei verwendete Technik ist bei allen Methoden gleich.

Das Vorwort "War" stammt vom früheren Begriff "WarDialing". WarDialing verwendete man dazu, eine Reihe von bestimmten Telefonnummern nacheinander vom Computer aus anzurufen (durch eine automatisierte Software) und herauszufinden, wo andere Modems antworten um eine Verbindung herstellen zu können. So wurden zum Beispiel alle Nummern von 555-1111 bis 555-9999 durchprobiert.

5 Was ist WarChalking?

Prinzipiell bedeutet es, mit Kreide Symbole die Details über ein WLAN verraten an die Wände zu malen. Wozu? Wenn Person A eine Gegend erkundigt (z.B. weil er Internetzugang an der Bushaltestelle möchte) und einen AP findet, der dies bietet, malt er das entsprechende Zeichen mit Kreide an die nächste Hauswand. Jeder der den Code versteht sieht somit sofort, welches Netz hier empfangen werden kann. Hier sind die ursprünglichen Symbole (viele User haben auch eigene entworfen):



Open Node

Hier befindet sich ein offnenes WLAN-Netzwerk, welches direkt Zugang ins Internet liefert und IP-Adressen per DHCP verteilt (="IP-Adresse automatisch beziehen").

Closed Node

Hier befindet sich ein geschlossenes WLAN-Netzwerk wo entweder kein Internetzugang besteht oder nicht ohne weitere Vorgehensweisen "angeboten" wird.

Wep Node

Dieser AP überträgt Daten nur mit WEP-Verschlüsselung. Hier ist kein "einfacher" Zugang möglich da zuerst der WEP-Code geknackt werden muss. Weiteres hierzu (und wie das funktioniert) in den nächsten Absätzen dieses Artikels.

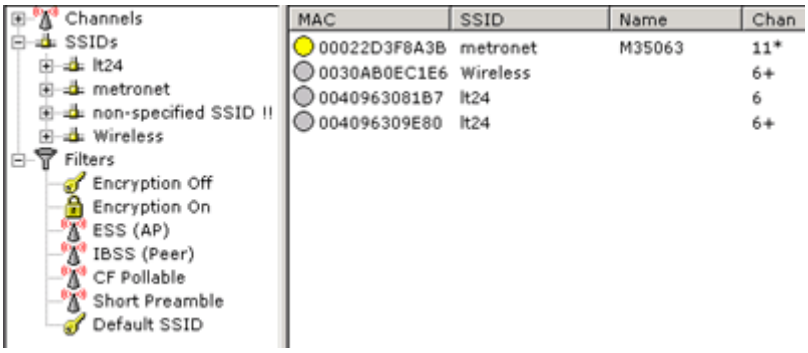
Damit es einen Beweis gibt, dass dies nicht nur eine Erfindung ist, sondern auch reell verwendet wird:

Mehr Informationen gibt es unter http://www.warchalking.org.

6 Fremde WLAN's - Suchen & Finden!

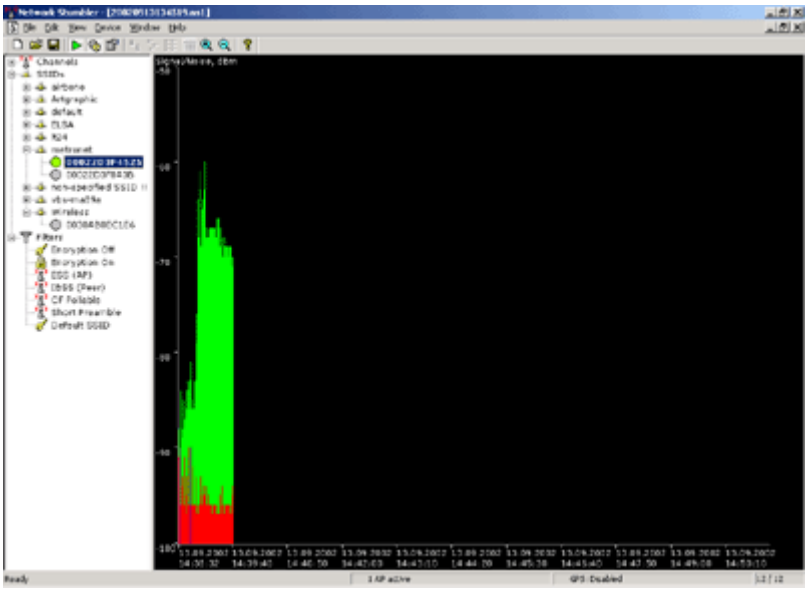
PC (Windows)

Zuerst müssen wir entsprechende AccessPoints suchen. Hierfür ist der Netstumbler (http://www.netstumbler.com) die beste Wahl. Wenn man dann unterwegs mit dem Laptop ist und man in den Einzugsbereich einiger AP's kommt sieht das ganze in etwa so aus:



Hier sieht man, anhand des gelben Kreises rechts, dass das Netz mit der SSID (SSID = Name des WLANs) 'metronet' derzeit empfangen werden kann. Alle anderen sind momentan nicht mehr erreichbar. Besonders angenehm ist, dass der Netstumbler eine optische und eine akkustische Ausgabe der Signalstärke hat. Optisch: Die Kreise können Grün, Gelb und Rot angezeigt werden (inkl. weiterer Abstufungen dieser Farben). Akkustisch: Es werden auf Wunsch MIDI-Töne ausgegeben; je höher der Ton desto besser das Signal. Sinnvolle Anwendung ist es, den Lautsprecherausgang des Notebooks an das Autoradio oder einen Kopfhörer anzuschließen - so muss man nicht ständig nachsehen ob's was neues gibt.

Hier sieht man die Signalstärke eines einzelen AP's in Grafikform. So lässt sich über einen längeren Zeitraum die Qualität des Signals angenehm darstellen:



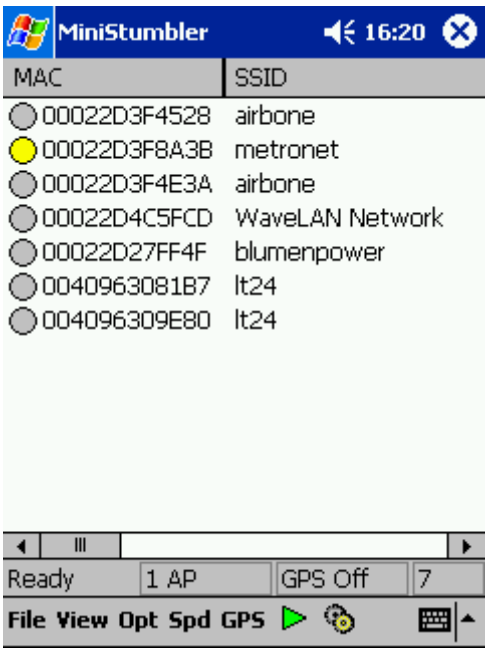
Besonders interessant ist es, wenn man den NetStumbler gemeinsam mit einem GPS-System verwendet. Dadurch wird automatisch beim auffinden eines AP's der Längen- und Breitengrad via GPS gespeichert. Somit ist das spätere Auffinden ein Kinderspiel. Es gibt auch Windows-Software wie Stumbverter (http://www.sonar-security.com) womit es möglich ist, jene numerischen Daten auf Karten Ihrer Wahl zu übertragen. Somit können Karten mit AP's der Umgebung erstellt werden. Diese sehen in etwa so aus:

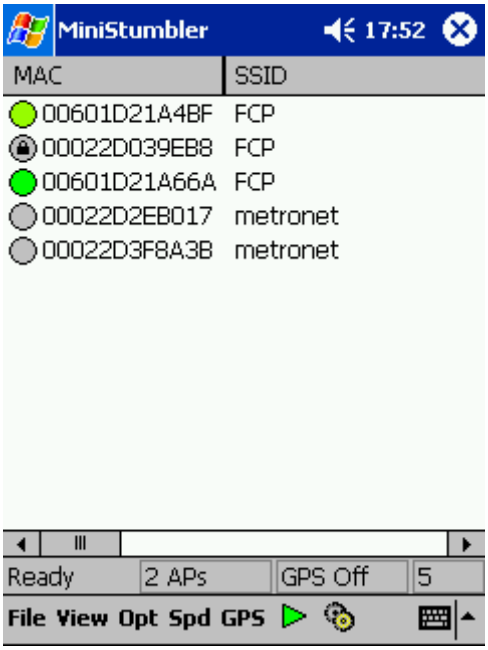
Mehr Landkarten gibt es unter http://www.nodedb.com.

PocketPC (z.B. Compaq IPAQ)

Anstatt des Notebooks kann man natürlich auch genialerweise seinen kleinen, leichten (unauffälligen!) Ipaq verwenden. Entsprechend mit einem PCMCIA-Jacket (http://www.pocket.at/pocketpc/zubehoer.htm#jackets) und mit einer WLAN-Karte inkl. Treiber (Homepage des Herstellers) ausgerüstet, kann es los gehen. Zuerst müssen wir entsprechende AccessPoints suchen. Hierfür ist der MiniStumbler (http://ww.netstumbler.com) die beste Wahl für den IPAQ. Im Prinzip ist der MiniStumbler ident zum NetStumbler, es fehlen aber einige Features wie zum Beispiel die grafische Anzeige der Signalstärke eines AP's oder die akkustische Ausgabe über das Auffinden eines AP's. Ansonsten bieten beide Programme die gleiche Funktionsvielfallt.

Wer gleich im Einzugsbereich einiger WLAN-Netze ist, sieht ein ähnliches Bild wie die beiden folgenden:

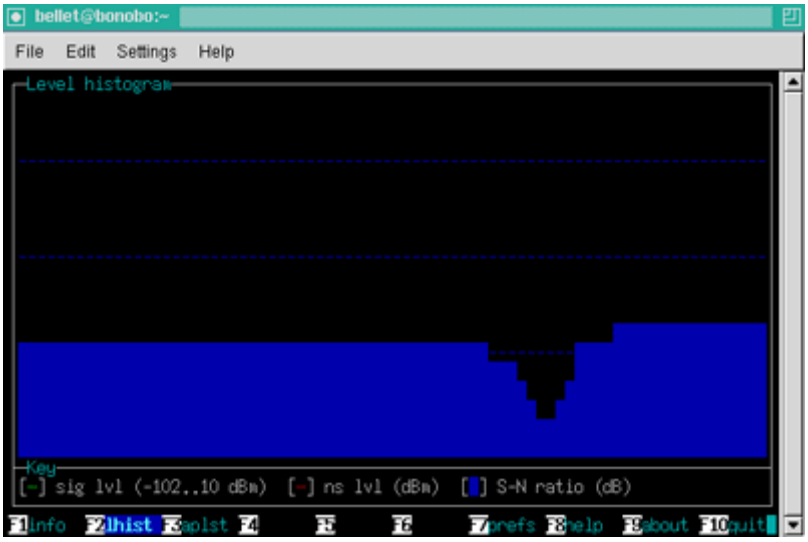




Besonders interessant ist es, wenn man den MiniStumbler gemeinsam mit einem GPS-System verwendet. Das funktioniert analog wie bei NetStumbler bei der "normalen" Windows-Version - siehe oben. Es gibt übrigends schon recht Preiswerte GPS-Systeme ab 150 € (Übersicht unter http://www.pocket.at/pocketpc/zubehoer2.htm#gps) - minimalistisch aber funktionell und genau das richtige für diese (und andere) Anwendungen.

PC (Linux)

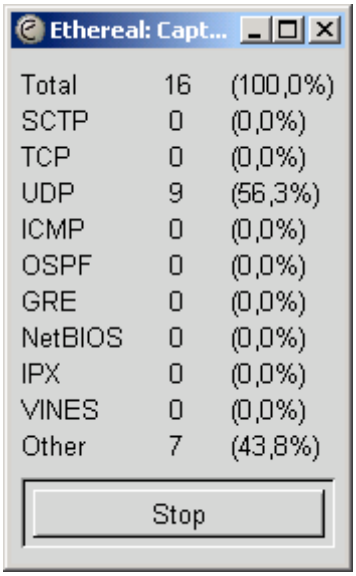
Natürlich gibt es unter Linux deutlich mehr Möglichkeiten als unter Windows nach Access-Points zu suchen. Unter anderem gibt es wavemon, das Programm bietet alle wichtigen Informationen sowie akkustische Wiedergabe wenn eine AP gefunden wird. Im Prinzip funktionieren die Programme wie der NetStumbler unter Windows. Es gibt ebenfalls Möglichkeiten über GPS die Koordinaten zu speichern um sie anschließlich auf Karten oder im Internet zu publizieren.



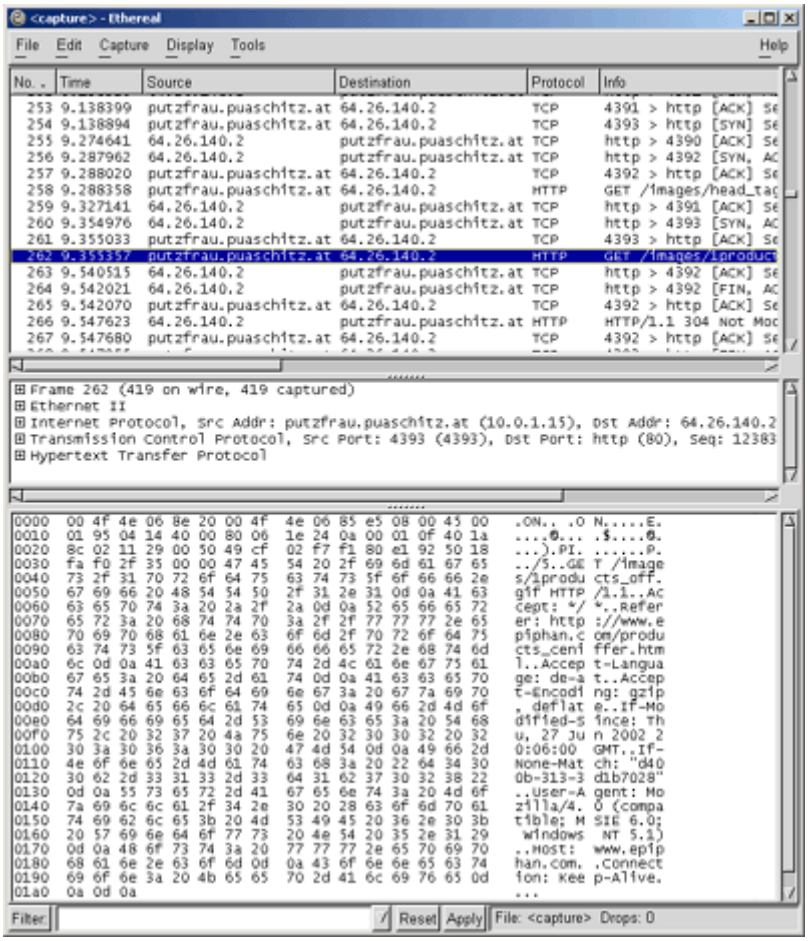
7 Mithören des Netzwerkverkehrs

PC (Windows)

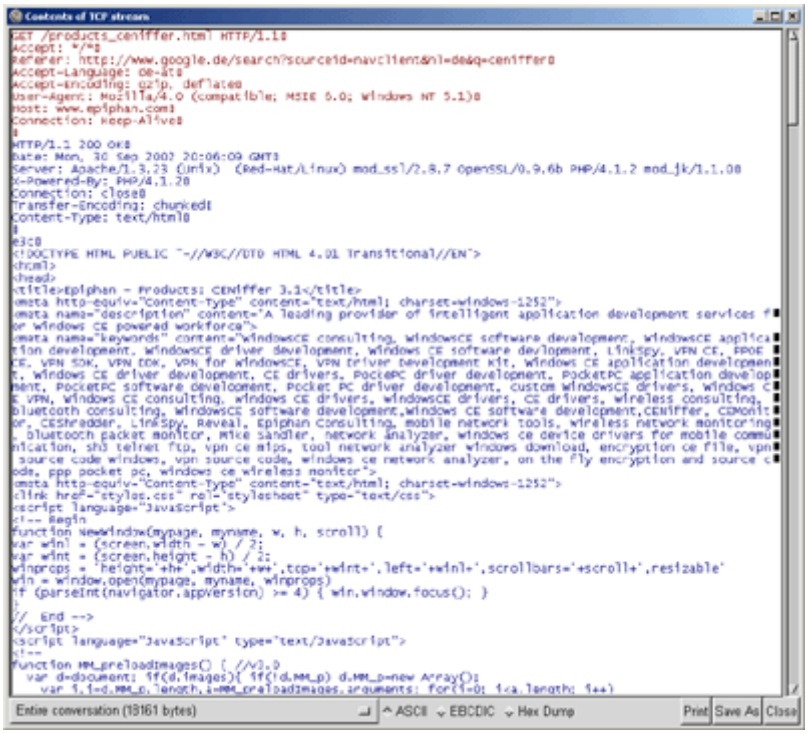
Der nächste Schritt ist nun das abhören des Netzwerkverkehrs im entsprechenden WLAN. Mit der entsprechenden Software ist das kein Problem. Ethereal (http://www.ethereal.com) bietet zum Beispiel die Möglichkeit sämtlichen Datenverkehr mitzuhören (funktioniert im lokalen Ethernet sowie bei WLAN-Netzen). Einmal auf Capture gehen, und los gehts:



Je nach belieben kann man entsprechend viel oder wenig mitlesen, danach gilt es, die gesammelten Daten auszulesen.



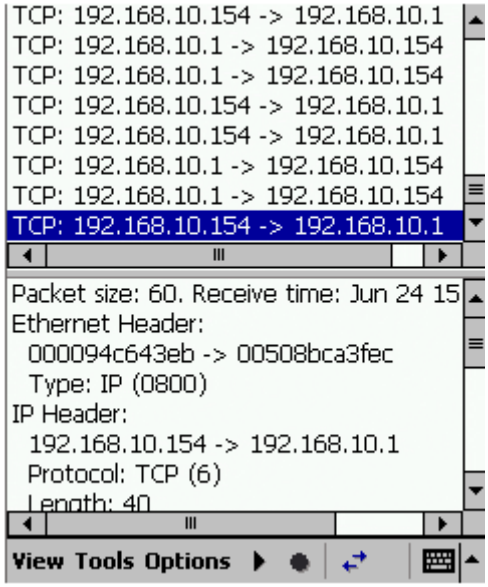
Das angenehme an Ethereal ist, dass man einen TCP-Stream komplett mitverfolgen kann und somit dann alle Daten in anschaulicher Form erkennen kann:



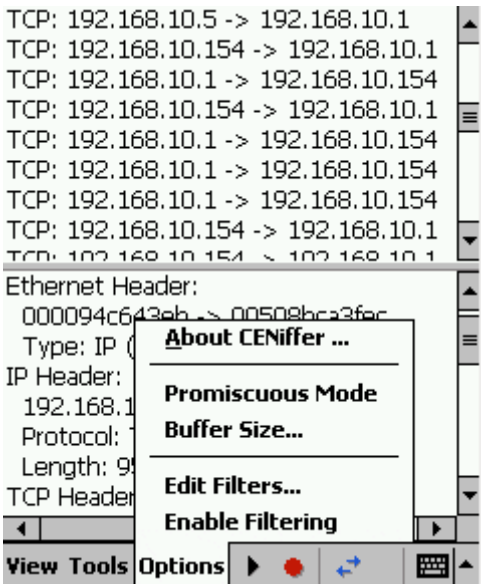
PocketPC (z.B. Compaq IPAQ)

Wer wieder einmal nicht den Laptop mit sich herumtragen möchte kann auch wiederum den IPAQ verwenden. CENiffer (http://www.epiphan.com/products_ceniffer.html) bietet im Prinzip das gleiche was Ethereal für den Desktop bietet. Man kann Daten mitlesen anher speichern und dann daheim gemütlich am Desktop auslesen.

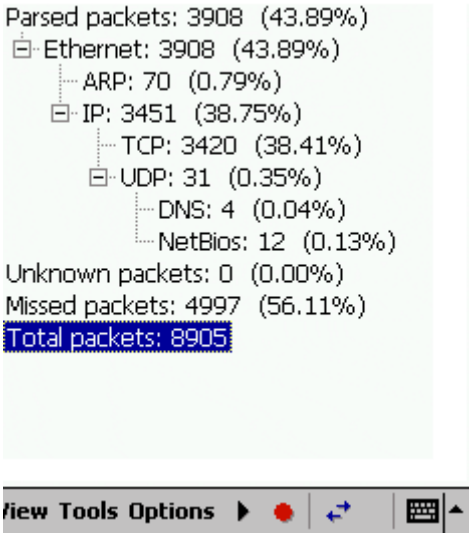
Hier sehen wir verschiedene TCP-Sessions, im unteren Fenster die Detailübersicht über dieses Packet.



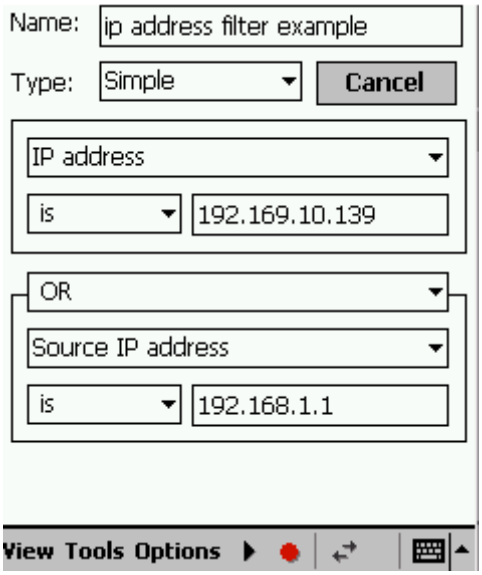
CENiffer bietet ebenfalls die Möglichkeit in den "Promiscious Mode" zu schalten - hierbei werden keine Informationen vom IPAQ über das WLAN versandt. Man bleibt also unentdeckt, erhält aber alle Datenpakete. Des weiteren ist es möglich nach verschiedenen Werten zu Filtern um nur besonders interessante Daten auszulesen.



Nun kann man sich auch ansehen, welches Protokoll am meisten verwendet wird. Dies kann recht interessant sein um z.B. Netzwerkstrukturen zu erkennen:



Wie bereits erwähnt können gesammelte Daten gespeichert werden um später bequem auf dem Desktop ausgewertet zu werden:



PC (Linux)

Auch unter Linux gibt es das gerade erwähnte Tool 'Ethereal' (http://www.ethereal.com). Die Benutzeroberfläche mit jener von Windows ident, daher gelten obige Beschreibungen hier analog. Allerdings musste ich feststellen, dass das Programm nicht sehr stabil scheint, wobei dies nur der erste Eindruck war - sobald ich mehr Erfahrungen über einen Langzeittest habe, werden diese hier eingefügt.

8 WEP-Key Cracken

Im IEEE 802.11 Standard verwendet WEP einen 40-bit langen Key der auf allen Geräten eingetragen werden muss. Jedoch unterstützen schon sehr viele Geräte Keys mit einer Länge von 104-bit. Einige Hersteller preisen ihre Produkte als '128-bit'-Hardware an. Diese sind allerdings 104-bit-Codes die einen 24-bit langen Initalisierungsvektor haben (104+24=128). Es gibt seit neustem auch Hardware die 152-bit verwendet - diese werden allerdings nicht durch alle Betriebssysteme problemlos unterstützt (Windows XP unterstützt dies lt. Microsoft nicht Standardmässig). Grundsätzlich gilt: Je länger (je höher die bit-Anzahl) der WEP-Key ist, desto besser.

Als WLAN entwickelt wurde, dachte man, dass die WEP-Verschlüsselung jegliche Sicherheitsbedenken lösen werde. Doch leider wurden bei der Konzeptionierung des Protokolls einige Fehler begangen und im Großen und Ganzen ist WEP überhaupt nicht so sicher wie gedacht.

Die Verschlüsselung verwendet einen geheimen Key "k" der sowohl dem Access-Point als auch dem Client bekannt ist. Um ein WEP-Frame zu berechnen, wir zuerst das unverschlüsselte Frame "M" mit der (unverschlüsselten) Checksumme "c(M)" verbunden. Man erhält also "M - c(M)". Als nächstes wird ein Packet-Initalisations-Vektor (IV) vor den geheimen Key "k" angehängt um daraus "IV - K" - den Paket-Key - zu verhalten. Der RC4 Stream wird dann mit diesem Paket-Key initialisiert und der Output dieses Streams sowie "M - c(M)" ergeben die Verschlüsselungssequenz:

C= (M - c(M)) - RC4(IV - k)

Die WEP-Daten sind der Packet-IV welcher vor diese Verschlüsselungssequenz C gesetzt wird.

RC4 besteht aus zwei Teilen, einem Key-Algorithmus und einer Ausgabemöglichkeit. In WEP verwendet der Key-Algorithmus entweder 64bit (40-bit geheimer Key plus 24-bit IV) oder 128-bit (104-bit geheimer Key plus 24-bit IV) um das RC4 Array "S" - das eine Zufallszahl zwischen 0 und 255 ist, aufzustellen. Die Ausgabemöglichkeit verwendet dieses Array "S" um eine Sequenz zu erstellen.

Die WEP-Attacke verwendet nur das erste Wort dieser Sequenz. Die Gleichung für dieses erste Byte der Ausgabe ergibt sich aus S[S[1]] + S[S[1]]. Nach der Erstellung des Keys, hängt dieses erste Byte der Ausgabe nur noch von drei Werten des Arrays ab: S[1], S[S[1]], S[S[1]] + S[S[1]].

Um die Attacke durchführen zu können, müssen wir nach IV's suchen, welche den Key-Setup-Algorithmus in jenen Status setzt, wo Informationen über den Key ausgelesen werden können. Es ist einfach zu testen, ob ein spezielles Packet einen IV und das Ausgabebyte anbietet. Jedes Packet liefert nur einen Teil des gesamten

Keys, daher muss vor jedem Key-Byte geraten werden, bevor ein anderes Packet weitere Informationen darüber Auskunft erteilt.

Wenn also genügend Pakete gesammelt werden können (zwischen 4 und 6 Millionen Stück) ist das Analysieren möglich und man erhält den Key. Diese Arbeit (Sammeln von Paketen, analysieren dieser) übernimmt die Software. Für Windows habe ich bisher keine solche Software gefunden, unter Linux bietet Airsnort (http://airsnort.shmoo.com) diese Möglichkeit. Wer allerdings keine Prism2-basierende Karte sein eigen nennen kann, muss sich mit entsprechenden Patches für die Hermes-Chips herumschlagen. Bisher hatte ich keine Zeit mich damit genauer zu beschäftigen - ich hoffe, ich kann im nächsten Update hier Erfahrungsberichte vorweisen. Das einzige, was ich bereits gehört habe, ist, dass es nicht so einfach ist, wie im Internet beschrieben.

9 MAC-Adressen fälschen

Fast alle Access-Points bieten die Möglichkeit, Daten nur von Autorisierten Geräten zu akzeptieren. Dafür wird die MAC-Adresse verwendet. Dies ist eine einmalige Nummer, die jeder Netzwerkkarte (also auch WLAN-Interfaces aller Art) zugewiesen wird. Um diese zu ändern gibt es grundsätzlich zwei Möglichkeiten:

Hardwarebasierend:

Manche Chips der Netzwerkkarten lassen sich einfach mit beliebigen Werten überschreiben. Dadurch können Sie mit entsprechender Software die Werte in der Netzwerkkarte direkt abändern. Das Betriebssystem übernimmt diese Werte dann einfach von der Netzwerkkarte.

Softwarebasierend:

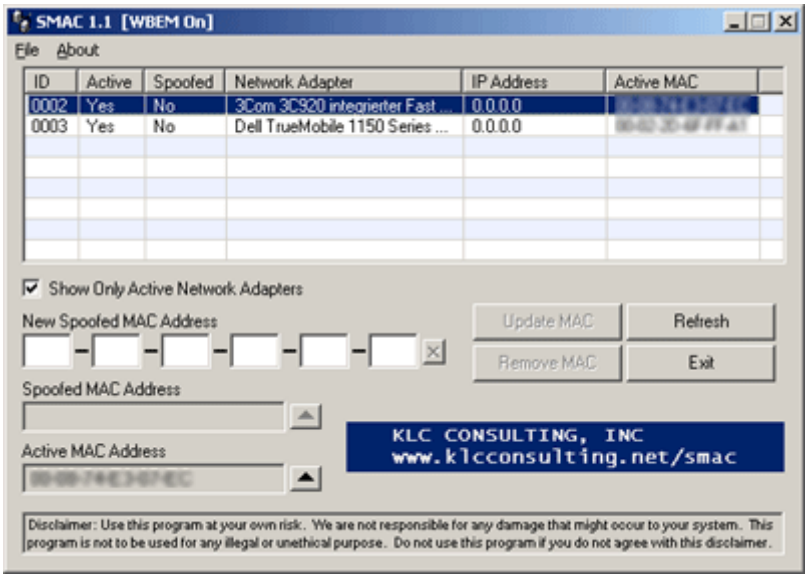
Wie gerade erwähnt, übernehmen die Betriebssystem die Werte der Netzwerkkarte. Diese werden meist zwischengespeichert und damit die einzelnen Datenpackete generiert. Nun ist es möglich, hier anzusetzen und per Software diese Einträge zu ändern. Der Code (und eventuell die Garantie) der Netzwerkkarte bleibt unberührt, die Packete erhalten aber einen anderen Absender.

Neue-MAC-Adresse:

In beiden Fällen muss beachtet werden, dass MAC-Adressen einem bestimmten Muster entsprechen. Sie sollten dies beachten und die MAC-Adresse nicht willkürlich vergeben, damit dies nicht auffällt. So ist es z.B. bei Funknetzwerkkarten immer so, dass diese mit 00:02: beginnen! Mehr über MAC-Adressen und deren Vergabe unter http://www.cavebear.com/CaveBear/Ethernet/

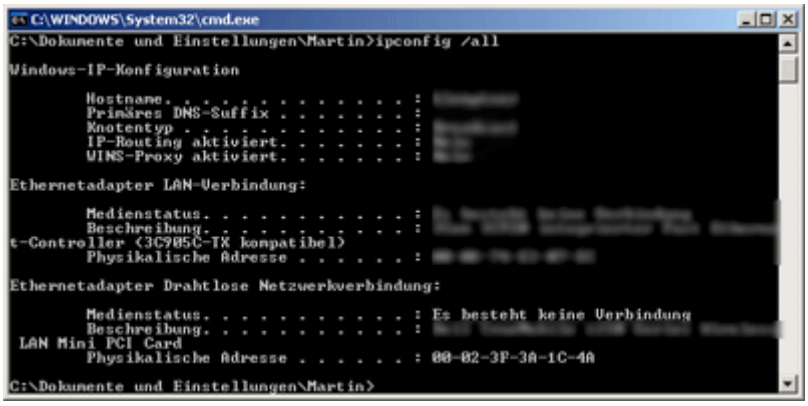
PC (Windows)

Es gibt - wie so oft - verschiendste Möglichkeiten das Ziel zu erreichen. Die einfachste erscheint das Tool 'SMAC' zu sein. Diese Software ist gratis und kann für Windows2000 und Windows XP Systeme die MAC-Adressen aller Netzwerkinterfaces abändern. Der Download ist unter http://www.klcconsulting.net möglich - bitte Bestimmungen des Anbieters beachten. Nach der Installation kann das Programm über das Start-Menü gestartet werden, es erwartet sie folgendes Interface:

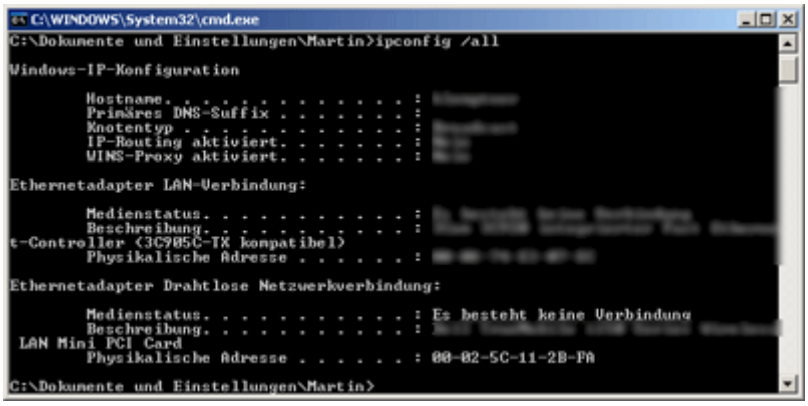


Nun kann unter 'New Spoofed IP Adress' bei jedem Interface eine neue MAC-Adresse vergeben werden. Ein Klick auf 'Update MAC' macht die Änderung aktiv, ein Klick auf 'Remove MAC' stellt die ursprüngliche Adresse wieder her. Interessant ist die Option 'Show only Active Network Adapters' zu deaktivieren. Nun können auch Interfaces wie FireWire, Parallelports und viele andere editiert werden - wird aber wohl niemand brauchen. Nach der Änderung muss die Netzwerkkarte kurz deaktiviert und aktiviert werden (oder Neustart von Windows) um die Änderung für Windows bemerkbar zu machen.

Im MS-DOS-Eingabefenster (Ausführen: 'cmd' oder 'command') kann man die Änderung mit dem Kommando 'ipconfig /all' mitverfolgen:



Und nach der Änderung via SMAC und einer Re-Aktivierung der WLAN-Karte:



PC (Linux)

Unter Linux ist dies ohne zusätzliche Tools zu bewerkstelligen. Man verwendet einfach das Tool 'ifconfig' mit den entsprechenden Parametern. Zuerst informieren wir uns über den aktuellen Status (wir nehmen an, eth1 sei dass WLAN-Interface):

```
ifconfig eth1

Link encap: Ethernet HWAddr 00:02:3F:3A:1C:4A
UP BROADCAST MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
Collisions:0 txqueuelen:100
RX bytes: 0 (0.0b) TX bytes: 0 (0.0b)
Interrupt: 11 Base Adress:0x100
```

Nun ändern wir die MAC-Adresse. Das Interface muss vorher heruntergefahren werden, danach starten wir es wieder.

```
ifconfig eth1 down
ifconfig hw ether 00:02:5C:11:2B:FA
ifconfig eth1 up
```

Nun betrachten wir die Auswirkung, wir sehen, die Änderung wurde übernommen:

```
Link encap: Ethernet HWAddr 00:02:5C:11:2B:FA
UP BROADCAST MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
Collisions:0 txqueuelen:100
RX bytes: 0 (0.0b) TX bytes: 0 (0.0b)
Interrupt: 11 Base Adress:0x100
```

Weitere Informationen und Parameter des Tools 'ifconfig' finden sich unter 'man ifconfig'.

10 Sicherheit im eigenen WLAN

Ich möchte nun einige Punkte aufgreifen die das eigene WLAN sicher machen sollen. Das bedeutet nicht, dass man sich danach keine Sorgen mehr machen sollte, aber im Großen und Ganzen sind es einige Kleinigkeiten, welche die Sicherheit gleich extrem erhöhen. Am wichtigsten ist aber, sich regelmäßig zu informieren, was sich neues in diesem Bereich tut, um entsprechende Gegenmaßnahmen zu ergreifen.

Name des WLANs

So absurd es im ersten Moment wirkt, so klar ist es jedoch wenn man darüber nachdenkt. Jedes Funknetzwerk besitzt eine SSID, quasi eine Netzkennung. Diese ist notwendig, damit die unterschiedlichen Clients die verschiedenen Netzwerke auseinander halten können. Der Sicherheitsaspekt dabei ist, dass der Wert der SSID immer - also verschlüsselt, unverschlüsselt, mit MAC-Beschränkung, ohne, etc. - übertragen wird. Daher sollte hier keine Bezeichnung wie 'Firma XY' oder 'Adresse Hausnummer Türnummer' vergeben werden. Dadurch erhält ein potentieller Angreifer nur noch mehr Informationen über das Netzwerk. Ebenfalls sind Standard-Werte dringlichst zu vermeiden, da aufgrund dieser oftmals auf den Hersteller oder den Typ des Access-Points geschlossen werden könnte.

WLAN als externes Netz betrachten

Wenn man ein Netzwerk mit WLAN plant sollte man nicht den Fehler begehen das WLAN hinter die Firewall zu positionieren. Da das Funknetzwerk leichter abgehört werden kann und es mehr Angriffsmöglichkeiten als das physische Kabel bietet, sollte es am besten wie das Internet als externes und somit "feindliches" Netzwerk angesehen werden. Es sollte nicht möglich sein, direkt sensible Daten anderer Rechner zu erreichen, nur weil man in diesem (dem WLAN-) Segment ist.

WEP verwenden

Auch wenn ich in diesem Dokument darüber geschrieben habe, dass WEP nicht unbedingt sicher ist, sollte man es verwenden. Klar, jemand der es knacken möchte kann sich die entsprechende Ausrüstung und die Zeit dafür nehmen - die Frage stellt sich allerdings, ob man sich die Arbeit antun möchte. Des weiteren schützt WEP sicherlich vor Usern, die Artikel wie diesen lesen, die Software installieren und es einfach mal 'probieren'.

Vergleichen Sie WEP mit Ihrer Wohnung: Sie können die Haustüre abschließen, oder nicht. In beiden Fällen ist es möglich in die Wohnung einzudringen, nur bei der zweiten Variante ist es schwieriger und es besteht (vielleicht) eine Hemmschwelle.

Wenn Sie WEP verwenden, sollte Sie allerdings auch in regelmäßigen Abständen den WEP-Key wiederum abändern. Dass erhöht die Sicherheit ebenso, da es bekanntlich ja doch eine Weile dauert den Key herauszufinden. Jemand, der einmal den Key hat, schaut vielleicht öfter bei Ihnen vorbei und hört den Netzwerkverkehr mit - ändern Sie den Key jedoch ab und zu, wird es ihm/ihr auf die Dauer vielleicht zu dumm, ständig ihren Änderungen nachspionieren zu müssen.

Verwenden Sie immer die höchste bit-Anzahl die Ihre Hardware untertützt und versuchen Sie die Codes möglichst zufällig, und mit keinen einfachen Kombinationen (immer dieselbe Zahl, Buchstabenreihenfolgen) zu wählen.

Auf MAC-Adresse beschränken

Viele Access-Points bieten die Möglichkeit, dass nur Daten an bekannte MAC-Adressen versendet werden. Die MAC-Adresse ist eine eindeutige Adresse einer jeden Netzwerkkarte und kommt auf der Welt nur einmal vor. Sie können in ihrem WLAN die Zugriffe auf Ihre Netzwerkkarten beschränken und somit "fremde" von vornherein ausschließen.

Doch Achtung: Es besteht die Möglichkeit diese Adressen zu fälschen und damit dem Access-Point vorzutäuschen man sei jemand anderes. Wenn Sie zum Beispiel kein WEP verwenden, werden die MAC-Adressen Ihrer Geräte ohne Verschlüsselung übertragen. Empfängt der Angreifer ein Packet, liest er die erlaubte MAC-Adresse und überträgt diese auf seine eigene Netzwerkkarte - somit glaubt der Access-Point dem Angreifer und lässt die Übertragung zu.

SSL verwenden

Es gibt einige öffentliche Netzwerke wo der Betreiber kein WEP verwendet - warum auch immer. Wenn Sie über diese Netzwerke Ihre E-Mails lesen oder sich in einem Webinterface einloggen werden ihre Daten "plain text" übertragen. Das bedeutet dass jeder Teilnehmer des Netzwerkes (des WLAN) diese Daten abhören kann und die Passwörter auf seinem/ihrem Bildschirm sieht (siehe oben).

Dies ändert sich, wenn Sie SSL verwenden. Bei SSL werden die Daten zwischen Ihrem Computer und dem Server verschlüsselt, niemand dazwischen (auch nicht der Anbieter des WLAN oder weiterer Verbindungsnetze) kann mehr die Daten einfach auslesen. Sie erkennen zum Beispiel im Internet-Explorer an einem kleinem Schloss rechts unten, dass dies eine gesicherte Verbindung ist. Jeder, der bereits Online-Banking bereits benutzt hat, hat eine SSL-Verbindung verwendet.

Sie können SSL aber nicht nur im Web einsetzen, sondern auch bei E-Mail-Protokollen wie IMAP, POP3 und SMTP - wenn ihr Provider dies unterstützt. Fragen Sie in jedem Fall nach und verwenden Sie SSL wenn vorhanden.

Wenn Sie bedenken aufgrund der Sicherheit haben, suchen Sie doch einfach im Internet über Möglichkeiten SSL zu hacken. Es gibt fast keine. Der Aufwand ist dermaßen hoch eine 128-bit Verschlüsselung abzuhören und danach zu analysieren, dass es wohl kaum jemanden gibt, der sich die Arbeit antun wird. Es sei denn, Sie planen eine Verschwörung gegen die USA, dann gibt es vielleicht Interessenten...

Gesamten Datentransfer verschlüsseln

Wie bereits erwähnt, bei SSL werden nur jene Daten verschlüsselt, wo eine SSL-Verbindung möglich und gewünscht ist. Nicht alle Anbieter von Web- oder Emaildiensten bieten dieses Service an und somit entstehen wieder Lücken in Ihrem Sicherheitssystem. Es gibt allerdings auch die Möglichkeit den gesamten Netzwerkverkehr ständig zu verschlüsseln. Somit wird jede Email, jede Internetseite die Sie ansehen, etc. sicher übertragen.

Eine gängige Variante hierfür ist zum Beispiel IPsec. Mehr Informationen gibt es unter http://www.freeswan.org

11 WLAN-Projekte/Links

Hier möchte ich verschiedene Links und Meldungen aus dem Internet aufzählen die meiner Meinung nach sehr interessantes Material bieten, kurios, lesenswert und/oder besondere bzw. kritische Beachtung erfordern.

Nachtrag

25.03.2003	slashdot.org: "Five of Asia's biggest carriers have given the public Wireless LAN market a hefty boost by announcing what they modestly claim is the world's first and largest wireless broadband alliance. Korea Telecom, China Netcom Corp. Ltd., Maxis (Malaysia), StarHub (Singapore), and Telstra Corp.(Australia) have agreed to open up their networks to allow wireless LAN users to roam from one country to another. Tests begin in July, although no specific launch date has been set. Full article is here." (http://slashdot.org/articles/03/03/25/003207.shtml?tid=193)
03.02.2003	slashdot.org: "CNet (http://news.com.com/2100-1033-982962.html) reports that the US Military and the Wi-Fi manufacturers have struck an agreement on reducing the interference on military radars by Wi-Fi equipment. [...] pcworld.com: "Navy Prepares to Navigate With Wireless LANs (http://www.pcworld.com/news/article/0,aid,109053,00.asp)."
14.01.03	Ein Ägypter schaffte es, eine Wi-Fi verbindung mit einer Geschwindigkeit von 2Mbit/s über einen Kilometer geschaffen. Mehr unter http://www.d128.com/wireless/.
14.01.03	Internet: "Die SSC (Schweden) hat einer Wi-Fi Übertragung über eine Distanz von 310 Kilometer überbrücken können. Mehr dazu: http://www.alvarion.com/RunTime/CorpInf_30130.asp?fuf=281&type=item"
14.12.02	ORF-Futurezone (http://futurezone.orf.at/futurezone.orf?read=detail&id=138639&tmp=51695): "Die Funktionen für drahtlose Netze in Windows XP bereiten Sicherheitsexperten derzeit Kopfzerbrechen. Das Betriebssystem nimmt nämlich unter Umständen mit WLANs Verbindung auf, mit denen es eigentlich nicht sprechen sollte. Demnach merkt sich Windows XP die Netzwerk-Kennung [SSID] aller Access Points, mit denen es schon einmal Kontakt hatte. Diese SSIDs schickt XP dann in Zukunft ständig aus, um nach den bekannten WLANs zu suchen. Diese Übertragungen lassen sich abfangen, da sie noch nicht verschlüsselt sind. Somit kann man XP quasi ein "falsches" WLAN unterschieben, indem man die SSID eines Access Points auf eine Adresse setzt, die der Zielrechner bereits kennt. Mit einem solchen AP nimmt Windows XP dann bereitwillig Kontakt auf. [...]"
31.10.02	"Die Wi-Fi-Allianz, ein Zusammenschluss aus 196 Unternehmen, will eine eigene Sicherheitslösung für Wireless-Netzwerke schaffen. "Wi-Fi Protected Access" (WPA) nimmt einige Elemente vorweg, die für den Standard 802.11i geplant sind, und soll aufwärtskompatibel sein. Die Allianz geht davon aus, dass bereits im Frühjahr 2003 die ersten "Wi-Fi-Certified" Geräte über diese Lösung verfügen werden. Für Geräte, die bereits auf dem Markt sind, sollen Software-Updates zur Verfügung gestellt werden. WPA soll die für Angriffe anfällige Sicherheitstechnik "Wired Equivalent Privacy" ersetzen. (http://www.weca.net/OpenSection/ReleaseDisplay.asp?TID=4&ItemID=118&StrYear=2002&strmonth=10)"
31.10.02	slashdot.org: "Over at infoworld.com (http://www.infoworld.com/) they have an article about the organization that certifies wireless LAN products under the Wi-Fi name revealed new specifications Thursday for how vendors should make their products more secure. The guidelines call for new mechanisms to replace the current security system (http://www.infoworld.com/articles/hn/xml/02/10/31/021031hnwifi.xml), based on WEP, which has come under fire for being too easy to circumvent. The certification body, Wi-Fi Alliance, plans to lay the mechanisms out as optional features beginning in February and require them for Wi-Fi compliance about six months later, said Dennis Eaton, chairman of the Wi-Fi Alliance."
18.10.02	slashdot.org: "NTT Science and Core Technology Laboratory Group has developed a wireless communications that is capable of transmitting data at speeds of up to 10Gbps. In order to achieve such high data transmission speeds, the system uses the as-yet-unused 120GHz frequency band. The actual bandwidth the system uses is 17GHz, and the method of modulation employed is amplitude shift keying (http://neasia.nikkeibp.com/wcs/leaf?CID=onair/asabt/news/212281)."

12 Software/Tools

Windows

Netstumbler/Ministumbler

Diese Software ist wohl die bekannteste im WarX'ing-Bereich. Netstumbler verwendet die Wireless-Netzwerkkarte um alle WLAN's im umliegenden Bereich zu erkennen. Es werden die SSID, der Channel, WEP-Option, Signalstärke, und vieles mehr angezeigt. Eine sehr interessante Variante ist das Zusammenspiel mit einem GPS-System wodurch die genaue Position von Access Points mitprotokolliert wird - dadurch ist das spätere Auffinden der Funknetzwerke ein leichtes. Auf der Homepage gibt es eine Landkarte (leider nur USA) wo alle Netzwerke grafisch aufgezeigt werden.

Besonders interessant ist, dass der MiniStumbler auch auf Hanhelds mit dem PocketPC-Betriebssystem verwendet werden kann. Somit kann z.B. mit dem Compaq IPAQ auch nach AP's suchen, ohne großartig aufzufallen.

» http://www.netstumbler.com

Stumbverter

Stumbverter bietet die Möglichkeit NetStumbler-Files in das Programm MapPoint 2002 von Microsoft zu importieren. Alle mitprotokollierten AP's werden mit kleinen Icons auf den Landkarten angezeigt. Informationen wie MAC-Adressen und weitere Notizen können hinzugefügt werden.

» http://www.sonar-security.com

AiroPeek

AiroPeek ist eine sehr interessante Software für 802.11b-Netzwerke welches alle höheren Protokolle wie TCP/IP, AppleTalk, NetBEUI und IPX unterstützt. Die Funktionen sind ähnlich dem Softwarepacket Etherpeek, nur vollständig auf Drahtlose Netzwerke angepasst. Desweiteren kann AiroPeek Sicherheitsprobleme isolieren, die Performance des Netzes messen und detailierte Informationen wie Signalstärke, Channels, uvm. angeben.

» http://www.wildpackets.com/products/airopeek/

Etherpeek

EtherPeek ist quasi das Pendant zu AiroPeek, allerdings für "normale" (kabelbetriebene) Netzwerke. Für mich ein sehr interessanter Punkt ist, dass man den gesammten Netzwerkverkehr mithören kann. Innerhalb der Software war es mir auch möglich, als Device die WLAN-Karte anzugeben. Somit kann man mit wenigen Mausklicks alle Datenpackete speichern, die über das Netzwerk laufen und sich anher (z.B. daheim) genau anschauen welche Daten übertragen werden.

» http://www.wildpackets.com/products/etherpeek/

PocketPC (z.B. Compaq IPAQ)

CEniffer

Software, die es am PocketPC/Ipaq ermöglicht, Netzwerkverkehr mitzulesen und zu speichern.

» http://www.epiphan.com/products_ceniffer.html

Mini-Stumbler

Software zum auffinden von WLAN's am PocketPC/Ipaq.

» http://www.netstumbler.com

Macintosh

MacStumbler

MacStumbler ist ein kleines Programm um die Funktionen von NetStumbler (Windows) und Kismet (Linux) auf einem Macintosh zu emulieren. Leider funktioniert die Software nur mit Apple Airport Karten und die Sotware ist noch im Beta-Test-Stadium.

» http://www.macstumbler.com

istumbler

Findet Funknetzwerke und gibt Informationen über diese aus.

» http://homepage.mac.com/alfwatt/istumbler/

KisMAC

Diese Software findet Funknetzwerke unter MacOS X und setzt die WLAN-Karte in den Monitor-Modus (mit dem 'viha' Treiber). Im Gegensatz zu vielen anderen Applikationen sendet diese Software keine Requests und arbeitet somit unsichtbar für die WLAN-Betreiber.

» http://www.binaervarianz.de/projekte/programmieren/kismac/

Viha MacOS X Wireless Tools

Viha ist eine größere Sammlung verschiedener Tools für drahtlose Netzwerke. Derzeit wird folgendes entwickelt: Ein eigener AirPort-Treiber der das abfangen von Packeten ermöglicht, ein Framework um den Treiber anzusteuern und 801.11-packet deconstruction sowie ein Tool um Drahtlose Netzwerke aufzuspüren (Kommandozeile).

» http://www.dopesquad.net/security/

Linux

Freeswan

Eine Möglichkeit unter Linux IPsec über WLAN's zu verwenden. Wahrscheinlich die derzeit sicherste Variante Daten via WLAN zu übertragen.

» http://www.freeswan.org

ssidsniff

Kleines Tool, welches Access Points findet und Traffic speichern kann. Kommt inklusive Konfigurationsskript und unterstützt Cisco Aironet und verschiedene prism2-Karten.

» http://www.bastard.net/~Ekos/wifi/

Kismet

Dieses Tool ist ein 802.11b wireless Netzwerk sniffer. Damit ist es möglich, mit fast jeder WLAN-Karte die durch Linux unterstützt wird (auch Prism2-Karten die vom Wlan-NG-Projekt unterstützt werden oder Karten die via libpcap arbeiten), den Netzwerkverkehr mitzuhören.

» http://www.kismetwireless.net

Mognet

Ein Open-Source Wireless sniffer/analyzer, der in Java programmiert wurde. Ursprünglich für den Compaq Ipaq geplant, läuft natürlich auch auf Desktop-Systemen.

» http://chocobospore.org/mognet/

AP-Utils

Ein Seit von Tools zum Managen von Access Points unter Unix/Linux/FreeBSD/NetBSD/AIX via SNMP-Protokoll.

» http://ap-utils.polesye.net/

WEPCrack

Dieses Tool war das erste mit welchem es möglich war, WEP-Keys zu knacken. Es sind Perl-Skripts, die anhand von empfangenen Packeten den WEP-Key auslesen können. Wer es nur testen möchte (ohne den Netzwerkverkehr abhören zu wollen oder zu können) kann mit einem beliegenden Skript empfangene Packete simulieren.

» http://wepcrack.sourceforge.net

AirSnort

Airsnort bietet die Möglichkeit die verschlüsselten WEP-Keys durch abhören des Netzwerkverkehrs herauszufinden. Es werden in etwa 5-6 Milionen verschlüsselte Packete gebraucht um Rückschlüsse auf den WEP-Key zu schließen.

» http://airsnort.shmoo.com

FakeAP

Dieses Tool ist zum steigern der Sicherheit des eigenen WLAN's genial. Durch FakeAP werden 53.000 verschiedene AP's vorgetäuscht. Dadurch werden Programme wie NetStumbler ziemlich unnötig, weil es einfach zu lange dauert, alle verfügbaren AP's durchzuprobieren. Die einzige Variante besteht dann darin, via BruteForce-Programmen einen nach dem anderen zu probieren.

» http://www.blackalchemy.to/Projects/fakeap/fake-ap.html

Wireless Security Auditor

Wireless Security Auditor, oder WSA, ist ein Tool aus dem IBM-Labor welches auf dem Linux-Betriebssystem von Ipaq's läuft. WSA sucht automatisch nach schlechter Sicherheitskonfiguration um Netzwerkadministratoren Sicherheitsprobleme aufzuzeigen. Noch im Beta-Stadium.

» http://researchweb.watson.ibm.com/gsal/wsa/

THC-WarDrive

Wer mit GPS-Device unterwegs ist, kann mit THC-WarDrive auf einer persönlichen Karte der Umgebung alle AccessPoints aufzeichnen lassen. Ein wirklich wichtiges Tool für alle WarDriver...

» http://www.thehackerschoice.com/

THC-Rut

Wenn Programme wie FakeAP laufen bietet THC-Rut eine BruteForce-Methode um einen AP zu knacken. Es bietet Informationen wie Hersteller, spoofed (gefälschte) DHCP, BOOTP, ARP, ICMP und Router-Discovery Techniken.

» http://www.thehackerschoice.com/

PrismStumbler

Dieses Tool scanned ständig auf allen Kanälen und zeigt alle Pakete darin auf.

» http://prismstumbler.sourceforge.net/

WarLinux

Dies ist ein interessantes Betriebssystem (ich glaube, basistechnisch ist es Debian) welches verschiedene Tools bereitstellen soll um WarX'ing ermöglichen zu können. Eine Installation gibt es meiner Erfahrung nach nicht, ISO runterladen, das CD-Image brennen, damit booten und benutzen.

» http://sourceforge.net/projects/warlinux

Wellenreiter

Wellenreiter ist ein Perl-Programm durch welches es einfacher wird 802.11b-Netzwerke auszuforschen. Der Scanner kann AP's, networks und ad-hoc systeme ausfindig machen. Broadcasting sowie Non-Broadcasting Netzwerke können automatisch aufgefunden werden. Der Scanner zeigt übliche Informationen an und bietet angenehme Sound-Einstellungen die es möglich machen, nicht ständig auf das Display schauen zu müssen und akkustisch über AP's informiert zu werden.

» http://www.remote-exploit.org

WaveStumbler

Dieses Tool zeigt generelle Informationen über einen AP an wie Kanal, WEP, ESSID, MAC und so weiter. Das Tool unterstützt Hermes-Karten (Compaq, Lucent, Agere, ...). Es ist noch in Entwicklung, scheint allerdings stabil zu laufen.

» http://www.cqure.net/tools08.html

SSID Sniff

Ein nettes, kleines Tool um nach AP's zu suchen und entsprechenden Traffic abzuhören. Das Tool kommt mit einem Konfigurationsskript und unterstützt Cisco Aironet und verschiedene Prism2-basierende Karten.

» http://www.bastard.net/~kos/wifi/

Wavemon

Wavemon arbeitet mit Orinoco-Karten zusammen und ist eine ncurses-basierende Applikation für WLAN's.

» http://www.jm-music.de/projects.html

AirTraf

Dieses Tool bietet eine Menge verschiedener Möglichkeiten. AirTraf kann Packete mitsniffen und auch dekodieren. Desweiteren kann die Software natürlich auch AP aufspüren und entsprechende Daten liefert. Desweiteren bietet AirTraf die Möglichkeit alle empfangenen Daten in einer Datenbankform abzuspeichern, dadurch können verschiedene Tools auf die gleichen Daten zugreifen. AirTraf ist noch in Entwicklung, es gibt allerdings auch stabiles Releases.

» http://airtraf.sourceforge.net/index.php

AirJack

Dieses Tool bietet die Möglichkeit eine Verbindung zu einem AP zu übernehmen. Zuerst wird eine Denial of Service-Attacke am AP durchgeführt indem möglichst viele ARP-Pakete an den AP gesendet werden. Irgendwann gibt der AP den Geist auf und muss neu starten. Sobald der Client die Verbindungen resetet suchen alle Clients nach einem neuen AP - allerdings ist der einzige AP im Moment unser eigener. Sobald der richtige AP wieder online ist, werden alle Daten vom fingierten weitergesandt und niemand (weder Clients noch AP) merken etwas davon. Dies nennt sich "Man-in-the-middle-Attack".

» http://802.11ninja.net/

BSD

AirTools

Die BSD-AirTools bieten ein komplettes Toolset für 802.11b. Neben einem ähnliches Tool wie NetStumbler gibt es auch eine Möglichkeit WEP-Codes zu knacken. Grafiken für den gesamten Verkehr sowie für einzelne AP's sind ebenso dabei wie weitere Tools damit alle 14 debug-modes der Prism2-Karten genutzt werden können.

» http://www.dachb0den.com/projects/bsd-airtools.html

13 Literaturverzeichnis & weiterführende Links

Websites in Deutscher-Sprache

[1] "Wireless LAN - eine Kurzübersicht"
http://www.it-academy.cc/content/article_browse.php?ID=549

[2] "Wireless Lan Technical Informations and Software"
http://www.monolith81.de

[3] "Wireless LAN 802.11x"
http://www.monolith81.de/software_linux.htm

[4] "Die Funknetze kommen"
http://www.tecchannel.de/special/1044/index.html

[5] "Sicherheit in Wireless LANs"
http://www.tecchannel.de/special/1046/index.html

[6] "Funknetze im Überblick"
http://www.tecchannel.de/special/1047/index.html

Websites in Englischer Sprache

[6] "The Definitive Guide to Wireless WarX'ing"
http://www.kraix.com/downloads/TDGTW-WarXing.txt

[7] "Wireless LAN Security : 802.11b and Corporate Networks"
http://documents.iss.net/whitepapers/wireless_LAN_security.pdf

[8] "Wireless HOWTO for Linux"
http://www.ibiblio.org/pub/Linux/docs/HOWTO/other-formats/html_single/Wireless-HOWTO.html

[9] "Hacking the Invisible Network : Insecurities in 802.11x"
http://www.net-security.org/dl/articles/Wireless.pdf

[10] "Cracking WEP Keys : Applying Known Techniques to WEP Keys"
http://www.lava.net/~newsham/wlan/WEP_password_cracker.ppt

[11] "The Need for a 802.11 Wireless Toolkit"
http://www.packetfactory.net/projects/radiate/802.11_toolkit-2.0.pdf

[12] "Wireless LAN Security"
http://www.packetninja.ca/starrrt.html

[13] "Linksys BEFVP41 VPN Router to OpenBSD IPSec Server + Wireless Mini HOWTO"
http://ruff.cs.jmu.edu/~beetle/download/befvp41.html

[14] "SSID Defaults"
http://www.wi2600.org/mediawhore/nf0/wireless/ssid_defaults/ssid_defaults-1.0.5.txt

[15] "What's Up With WEP"
http://www-106.ibm.com/developerworks/library/s-wep/?article=wir

[16] "Default List of Passwords for routers, firewalls, etc."
http://www.aaws25.hemscott.net/Default%20password%20list.htm

[17] "PersonalTelCo"
http://www.personaltelco.net/index.cgi/WarDriving

[18] "WarChalking.org"
http://www.warchalking.org/

[19] "Wardriving.com"
http://www.wardriving.com

[20] "MAC-Adressen-Tool für Windows"
http://www.klcconsulting.net

[21] "MAC-Adressen"
http://www.cavebear.com/CaveBear/Ethernet/

[22] "Slashdot.org - WLAN News"
http://slashdot.org/search.pl?topic=193