

## Wireless LAN - Einführung

- [+] Was ist das Eigentlich?
- [+] Aufbau-Möglichkeiten
- [+] Begriffserklärung
- [+] Was ist WEP?
- [+] WEP unsicher!
- [+] WLAN absichern!
- [+] WLAN hacking & Wardriving
- [+] Eigenes WLAN auf Schwächen testen!
- [+] Wardriving Hardware

-----  
-- WTF? Was ist das eigentlich?  
-----

WLAN bedeutet 'Wireless Local Area Network' und heisst soviel wie Funknetzwerk od. auch WaveLan. Also ein normales Netzwerk zwischen zwei oder mehreren PC's nur werden eben alle Daten anstatt durch den Kabelsalat per Funk hin und hergeschickt.

-----  
-- Aufbau-Möglichkeiten  
-----

Arten wie ein WLAN aufgebaut sein kann:

- Infrastructure Mode:

Die Verbindung wird über einen Accesspoint aufgebaut. Jeder Client muss eine Wireless LAN-Card besitzen um Daten zum Accesspoint zu schicken und Daten von dort auch wieder zu empfangen.

- Ad-hoc Mode:

Bei dieser Variante stellen die Clients untereinander eine Verbindung her und können ohne Accesspoint Daten austauschen.

-----  
-- Begriffserklärung  
-----

.802.11b

802.11b ist der meist verbreitete WLAN-Standard, entwickelt vom IEEE Komitee. Die maximale Bandbreite beträgt bis zu 11 MBit/s und läuft im 2,4 GHz-Band. (dieses Tutorial handelt hauptsächlich über 802.11b)

.802.11a:

Ein neuer Standard mit maximaler Übertragungsgeschwindigkeit von 54 Mbit/s, 802.11a läuft im 5 GHz-Band.

.802.11g:

Der G-Standard unterstützt 802.11b sowie auch 802.11a clients.

.AccessPoint

Ein AccessPoint ist eine Art Basisstation für WLAN's welcher Verbindungen zu den Clients aufbaut um Datenpakete austauschen zu können. Der AccessPoint muss gezielt platziert werden und die beiden an ihm befestigten Antennen müssen in die Richtung des Klienten gerichtet werden um optimalen Empfang zu gewährleisten.

.Reichweite:

Die Reichweite von WLAN's beträgt auf flachen und offenen Gelände 160 Meter und in halboffenen Gelände 50 Meter (802.11b)

Es wird aber daran gearbeitet diese geringe Reichweite auszuweiten..  
<http://www.heise.de/newsticker/data/ea-05.11.02-001/>

.SSID:

SSID bedeutet "System Set Identifier" und ist der Netzwerk-Name des WLAN's welcher frei wählbar ist.

.Wi-Fi:

Wi-Fi war ein Warenzeichen der WECA (Wireless Ethernet Compatibility Alliance) und der Industriestandard der für spezielle bedürfnisse von WLAN's entwickelt wurde.

Jedoch hat sich WECA dann in Wi-Fi Alliance umbenannt. Als Begründung wurde der Verbreitungsgrad des Begriffes Wi-Fi genannt.

<http://www.weca.net>

.IEEE:

IEEE bedeutet "Institute of Electrical and Electronics Engineers" und ist der weltweit größte Verband der Elektrotechniker und Informatiker. Der IEEE kümmert sich um die Belange der Elektrotechnik, organisiert Konferenzen,

legt Standards fest und dient als Veröffentlichungsmedium für wissenschaftliche Arbeiten im Bereich der Elektrotechnik und Informatik.

<http://ieee.org>

.MAC:

Jede Netzwerkkarte hat eine sogenannte MAC-Adresse (Media Access Control) auch die WLAN-Karte, (zB: 00 09 5B 24 D7 8B )

Jede MAC-Adresse ist einzigartig und kein zweites mal vorhanden.

Viele AccessPoints können nach Mac-Adresse der Clients filtern sodass diesem nur Zugang zum Netz gewährt wird wenn er eine bestimmte MAC-Adresse hat. Aber auch dies ist kein absoluter Schutz, denn es gibt auch Mittel und Wege MAC-Adressen zu spoofen!

.WPA:

WPA heisst "Wi-Fi Protected Access" und ist ein neues Sicherheitsverfahren für WLAN's welches WEP ablösen soll.

Es wurde am 31.10.2002 von der Wi-Fi-Alliance angekündigt kam aber erst im ersten Quartal 2003 auf dem Markt.

Die Sicherheit vom Nachfolger der WEP-Verschlüsselung lässt aber zu Wünschen übrig und ist fast genauso unsicher.

<http://www.golem.de/0311/28361.html>

-----  
-- Was ist WEP?  
-----

WEP (Wired-Equivalent-Privacy) wurde zum Schutz von Funknetzwerke entwickelt. WEP basiert auf den RC4-Algorithmus.

Dies funktioniert so das zB vom AccessPoint ein bestimmter Key definiert wird und nur Clients mit dem selben Key mit diesem in Verbindung treten können. Zur Auswahl gibt es die 40bit und die 104bit Variante.

Es gibt auch noch den 256-Bit Schlüssel jedoch wird dieser bisher nur beim Linksys WAP11 (AccessPoint) angeboten.

Beispiel:

40bit:

12 23 45 68 90

104bit:

12 34 56 78 90 12 34 56 78 90 12 34 56

-----

-- WEP unsicher!

-----  
WEP ist nicht als sicher eingestuft, Studenten der Rice Universität haben dies zusammen mit zwei AT&T-Labs-Angestellten bereits Ende Juli 2001 festgestellt und WEP gecrackt.

Ihre Vorgehensweise wird hier beschrieben:  
[http://www.cs.rice.edu/~astubble/wep\\_attack.pdf](http://www.cs.rice.edu/~astubble/wep_attack.pdf)

Die Sicherheitslücke befindet sich jedoch nicht in der inkorrekten Umsetzung vom RC4-Algorithmus wie vorerst angenommen sondern in WEP das einen zu schwachen Schlüssel generiert.

Diese Schwäche wird von Programmen wie WEPCrack und AirSnort ausgenutzt um unberechtigt an den Key zu gelangen.

Es werden Datenpakete gesammelt und verglichen, Airsnort braucht dazu ca. 5-10 Millionen solcher Pakete und die Dauer bis ein Angreifer diese gesammelt hat hängt vom Traffic im WLAN ab und kann auch mehrere Tage dauern.

Bis der WEP-Key berechnet ist hängt auch noch vom Alter des Accesspoints ab. Während es bei älteren Modellen mit alter Firmware relativ schnell geht dauert es bei den neueren schon ziemlich lange oder ist fast kaum mehr möglich da diese

nur noch sehr wenige schwache Pakete versenden.

Deshalb wurde WEPplus von Agere Systems in die Welt gerufen. Dies ist eine Verbesserung von WEP und wurde auf der Basis der ORiNOCO-Technik entwickelt. Alle die kein Agere-Produkt ihr eigen nennen können müssen zu anderen Mitteln greifen.

Infos zu WEPplus:  
<http://www.orinocowireless.com/upload/documents/WEPplusWhitepaper.pdf>

Die neueren APs wurden aber schon ein wenig weiterentwickelt so dass der Accesspoint mit WEP-Verschlüsselung nicht mehr ganz so viele unsichere Pakete versendet.

-----  
-- WLAN absichern!

-----  
Es gibt die Möglichkeit das WLAN durch ein VPN (Virtual Private Network) zu sichern und den WLAN-Clients den Zugang nur noch via VPN zu ermöglichen, dann kann nicht einfach jemand von aussen mit unverschlüsselten Protokollen "dazwischenfunken". Jetzt fragen sich sicherlich einige was ein VPN ist.. In einem VPN werden mit Hilfe von Chiffrier- und Authentifizierungstechniken vertrauliche Daten über ein öffentliches Netz abhör- und manipulationssicher zwischen zwei Kommunikationspartnern ausgetauscht.

Darauf will ich aber nicht näher eingehen, mehr infos dazu hier:  
<http://www.tecchannel.de/internet/306/>  
[http://www.msisafaq.de/Anleitungen/Sicherheit/VPN\\_1.htm](http://www.msisafaq.de/Anleitungen/Sicherheit/VPN_1.htm)

-----  
-- WLAN hacking & Wardriving

-----  
Die Verschlüsselung sollte grundsätzlich aktiviert werden da sonst jeder der sich mit seinem WLAN tauglichen Notebook in der Nähe des Funknetzwerkes aufhält darauf Zugriff erhält und sich beliebig darauf austoben kann.

Viele Leute vergessen ganz einfach darauf, oder sind sich der Gefahr nicht bewusst und sichern ihr WLAN nicht ab.  
Da sind wir auch schon beim nächsten Thema, "Wardriving":

WAR steht für Wireless Access Revolution und driving kann auch durch beliebige andere Fortgewegungs-Arten ausgetauscht werden zB Warflying, Warwalking, etc..

Wardriving nennt man es wenn Leute mit dem Auto durch die Gegend fahren und WLANs suchen. Wardriver erstellen für gewöhnlich nur Statistiken mit verschlüsselten und unverschlüsselten Wireless LANs und machen Karten davon. Sie führen nichts illegales im Schilde wie das von den Medien meist falsch dargestellt wird. Wardriving ist einfach nur ein Hobby das sich mit dieser Technologie auseinandersetzt.

Dann gibt es aber noch andere die in fremden Netzwerk herumzustöbern möchten oder einen Gratis Internet-Zugang suchen. Das sind dann keine Wardriver mehr.

Es sei angemerkt das das suchen von unverschlüsselten WLANs legal ist da es kein Gesetz gibt das dies verbietet.  
Illegal wird es ab dem Zeitpunkt an dem vertrauliche Daten von Computern im WLAN gestohlen oder manipuliert werden, Rechner angegriffen werden oder Industriespionage betrieben wird und die Daten zB weiterverkauft werden oder wenn die aktivierte WEP-Verschlüsselung gecrackt wird!  
Diese Leute können leider kaum zurückverfolgt werden weil sie meist unerkannt mit dem Auto in der Nähe des offenen Wavelans parken und nach ihrem "Geschäft" gleich wieder wegfahren!

Windows XP hat sogar bei Standardeinstellungen die unangenehme Eigenschaft sich bei Verfügbarkeit eines WLANs von selbst darauf einzuloggen ohne eine Meldung oder Nachfrage!

Es ist wohl klar was zB passieren würde wenn fremde Leute bei euch ins Internet gehen würden und über eurer WLAN die einen Angriff auf einen Webserver durchführen würden ..oder zB euren Traffic mitsniffen, Daten die über Telnet gesendet werden (zB: Username und Passwort bei einer POP3-Anmeldung, ein Login auf einen FTP-Server, ..etc.. ) kann der Angreifer wenn er den Traffic mittels Sniffer 'abhört' im Klartext abfangen.

Wenn jemand seine WLAN-Karte in den Monitor-Mode gesetzt hat muss er sich nichtmal in das entsprechende offene WLAN einloggen um den Traffic zu sniffen.. die Daten fliegen einfach durch die Luft und jeder der sich mit einem Packetsniffer in der Nähe befindet fängt sie ein!

Wardriving entwickelte sich mit der Zeit zu einer Art Volkssport unter Geeks.. Es hat sich in den Kreisen der Wardriver auch eine eigene Hobo-language ("Warchalking") entwickelt. Sie besteht aus Kreidezeichen die auf Hausmauern od. Stassen angebracht werden.  
So wird Gleichgesinnten angezeigt "Hier gibts was" ...

Beispiel:

```
hansi
)(      = offenes WLAN, Netzwerkname (SSID) = hansi, Bandbreite = 2MB/s
2,0
```

```
hansi
(       = geschlossenes WLAN, Netzwerkname = hansi
```

```
hansi AC
```

(w) = Ein mit WEP geschütztes WLAN, Bandbreite = 2MB/s  
2,0 Netzwerkname (SSID) = hans\_i,  
Access Contact (AC) = beliebige Kontakt-Info zum Betreiber

-----  
-- Eigenes WLAN auf Schwächen testen!  
-----

Dein WLAN selbst testen kannst du mit den selben Tools die auch zum Wardriving verwendet werden. Damit wird nach WLAN's gescannt und bei finden eines ungeschütztem WLAN's wird eine Verbindung mit diesem hergestellt..

Windows:

- Netstumbler -- <http://www.netstumbler.com>
- AiroPeek -- <http://www.wildpackets.com/products/airopeek>
- Aerosol -- <http://www.sec33.com/sniph/aerosol.php>
- ApSniff -- <http://www.bretmounet.com/ApSniff>
- Wlan-expert -- <http://www.vector.kharkov.ua/download/WLAN/wlanexpert.zip>

Linux:

- Kismet -- <http://www.kismetwireless.net>
- PrismStumbler -- <http://prismstumbler.sourceforge.net>
- Wellenreiter -- <http://www.remote-exploit.org>
- WaveMon -- <http://www.jm-music.de/projects.html>
- AirTraf -- <http://airtraf.sourceforge.net>
- Gwireless -- <http://gwifiapplet.sourceforge.net>

Macintosh:

- MacStumbler -- <http://www.macstumbler.com>
- KisMAC -- <http://kismac.binaervarianz.de>
- Airport -- <http://homepage.mac.com/macstumbler/airport.tar.gz>
- AP Scanner -- <http://homepage.mac.com/typexi/Personall.html>

BSD:

- AirTools -- <http://www.dachb0den.com/projects/bsd-airtools.html>

-----  
-- Wardriving Hardware  
-----

Also erstmal wird ein Notebook oder ggf. ein PDA benötigt.  
Geeignet ist alles über einem 486er mit PCMCIA Steckplatz.

Weiters braucht man eine WLAN-Karte, am besten mit Prism2 Chipsatz.  
Dann einfach die Karte in den PCMCIA Slot schieben, installieren,  
passende Software holen und es kann schon losgehen.

Jedoch wird jemand der mit einer Antenne unterwegs ist mehr finden.  
Bei Antennen ist es so das ~3dB eine Leistungsverdoppelung bringen,  
und zB 9dB würden eine Leistungssteigerung um das dreifache bringen.  
Dazu geeignet sind vier verschiedene Arten  
Dipole, Vertical, Parabolic und die Yagi Antennen  
(besonders bekannt geworden durch die Pringles-Antenne)

Von manchen wird auch gern GPS für die genaue Ortung und  
Kartographische Aufzeichnung verwendet.

GPS zeichnet Longitude und Latitude (also die genauen Koordinaten)  
des Accesspoints auf und man kann danach mittels Landkartensoftware  
(zB Mappoint od. Autoroute) einen genauen Plan erstellen.

Es gibt GPS-Module und GPS-Mäuse, Module haben meistens keine integrierten Antennen oder kein Gehäuse.  
Mäuse hingegen haben das alles.  
Weiters ist es wichtig das die Hardware über einen Datenausgang über USB od. seriell zum Notebook verbunden ist.  
Die GPS-Maus muss mit dem NMEA-Protokoll arbeiten um mit Wardriving-Software wie zB Netstumbler kompatibel zu sein!

---