WLAN Vortrag

Linux DemoDay 2003

von Stefan Triller

- **802.11b**

- 2,4 Ghz Bereich bzw. ISM-Bereich
  - (ISM = Industrial, Scientific, Medical)
- lizenzfreier Funkraum in dem auch Geräte wie Mikrowellen oder Bluetoothgeräte arbeiten.
- 11Mbit/s (5,5 ; 2 oder 1 bei niedrigem Signal)
- WEP als Verschlüsselung (64bit oder 128bit)

- **Frequenzen (802.11b):**

Region	**Frequenz in Ghz**
USA	2,4 - 2,4835
Europa	2,4 - 2,4835
Frankreich	2,4465 - 2,4835
Spanien	2,445 - 2,475
Japan	2,471 - 2,497

- **802.11a:**

- ja "a" kommt hier nach "b"
- Grund: Frequenzen für Polizei + Rettungsdienst
- 54Mbit/s
- 5Ghz Funkband
- OFDM (Orthogonal Frequency Division Multiplexing Encoding)

- **802.11g:**

- wurde möglichst abwärtskompatibel gestaltet
- am 12.06.2003 beschlossen
- 5.5Mbps und 11Mbps im 2.4GHz-Band
- 54Mbit/s per OFDM im 2,4GHz-Band
- bisher inkompatible 22Mbit/s (Ti – Chipsatz)
- kann 3 Kanäle zugleich managen

- **Ergänzungen:**

- **802.11f:**
- soll Kompatibilitätsprobleme zw. AP – Herstellern beseitigen

- **802.11i:**
- soll verbesserte Verschlüsselung und Authentifizierung mit sich bringen

- **Datenrate in der Praxis**

- bei momentanen 11Mbit/s ca 5Mbit/s
- bei 22Mbit/s (Ti-Chip) ca 5,5 Mbit/s
- bei 54Mbit/s ca 6Mbit/s (mit 802.11g, also 2,4GHz)

- **Modes**
- **Infrastruktur:**
- ein oder mehrere APs zentral
- best. Anzahl von Clients die sich zu den Aps verbinden
- äquivalent zu Hub / Switch im Kabelnetz

Ad-hoc:

- zwei oder mehr Clients kommunizieren ohne AP
- Äquivalent zu "Crossover-Kabel", aber mit der Möglichkeit mehrere Clients zu verbinden

- **1.1 Accesspoint (AP)**

- Wireless HUB
- bekommt einen Namen (SSID) damit die Clients wissen wo sie sich einloggen sollen
- nötig für Infrastruktur Mode
- Zugang zum Kabelnetzwerk (1x TP Kabel)
- organisiert WEP Verschlüsselung
- kann zu anderen Aps "bridgen", also zwei oder mehr Netzwerke verbinden

- **1.2 Accesspoint (AP)**

- kann als Repeater eingesetzt werden
- nützlich in Büros, da als Gegenstelle immer verfügbar
- Kein Paketfilter (nur Optionen zum Selbstschutz)
- Möglichkeit unter Linux einen Host-AP aufzusetzen, also PC als AP zu nutzen

- **WLAN-Router**

- Vorsicht bei dieser Bezeichnung (routet der?)
- bekommt einen Namen (SSID) damit die Clients wissen wo sie sich einloggen sollen
- eingebauter HUB / Switch für Kabelnetz
- evtl. eingebautes xDSL Modem oder ISDN Karte
- verbindet mehrere Kabelnetz PCs mit dem WLAN (Achtung! Will man das?)
- eingeschränkte Paketfilteroptionen

- **WLAN-Karte**

- erhältlich als PCMCIA, PCI, Mini-PCI, Compact Flash
- Mini-PCI: in Notebooks eingebaut, Antenne meist im Display
- PCI: native oder als Adapter für PCMCIA
- bekommt der Client (=wie beim Kabelnetz)
- versch. Chipsätze => unterschiedliche Fähigkeiten
- hat eine interne Antenne (meist 53mW)
- evtl. externen Antennenanschluß

- **Chipsätze:**

- Prism2: Monitor Mode, Host-AP, Fake-AP
- Orinoco: "Standard Chip", Monitor Mode (Patch!)
- TI: 22Mbit/s nicht Standardkonform

- **Reichweite**

- als Faustregel gilt: Sichtkontakt sollte vorhanden sein zw. den zu vernetzenden Punkten
- **laut Hersteller:**
  - in Gebäuden: 50m
  - im Freien 300m
- **Realität:**
  - in Gebäuden: je nach Wänden ca. 30M
  - im Freien: ca. 150-200m

- **Störfaktoren:**

- Stahlbeton ist sehr schlecht für den Empfang
- im Freien: Bäume, Stäucher, Häuser
- Mikrowellen stören (2,4GHz)
- bei mir zu Hause, max. durch 1 Decke

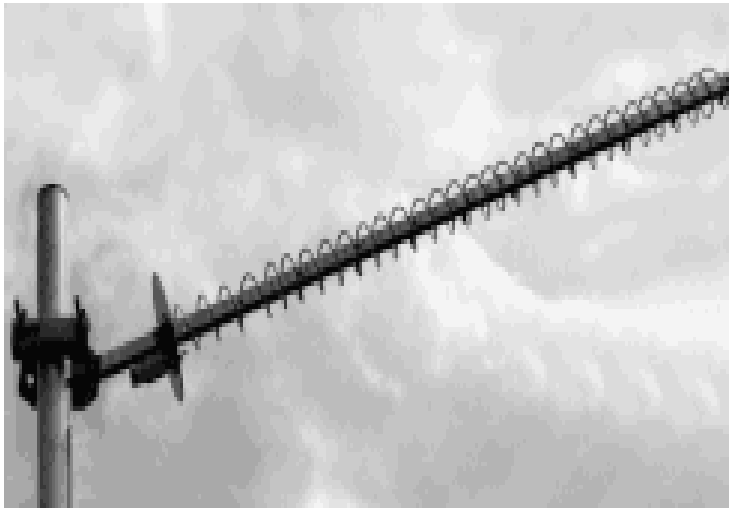
- **Omnidirektionale Antennen:**

- sehen aus wie ein "Stab"
- 360° Rundstrahler
- Reichweite, je nach Gewinn zw. 500m und 2km
- ideal für Bürgernetze, da Abdeckung in alle Richtungen

- **Richtantennen**

- geeignet für Punkt zu Punktverbindungen
- bessere Reichweite als Omnidirektionale, da gerichtete Strahlen
- Reichweite je nach Gewinn ca 2 - 3km
- versch. Bauarten:
  - Yagi
  - Helix
  - Flachpanel
  - Schüssel

- **Richtantennen**



- **WLAN Sicherheit (Fakten)**

- in das private Kabelnetz kann nur der, der die physische Möglichkeit besitzt sich einzustöpseln
- WLAN macht an den Grundstücksgrenzen nicht halt
- WLAN als externes Netz ansehen, wie das Internet

- **WLAN Sicherheit (Technik)**

- MAC Adressfilter im AP (Spoofing)
- WLAN "verstecken", also keine SSID senden
- WEP anmachen (shared Key)
- SSL verwenden (https, pop3s, imaps, ...)
- VPN Tunnel (sicherste Methode)

- **WEP Verschlüsselung (Fakten)**

- "Wired Equivalent Privacy"
- 64Bit Version und 128Bit Version
- hat Schwächen im Entwurf
- jeweils 24Bit Initialisierungsvektor => 40 und 104Bit

- **WEP Verschlüsselung (Technik)**

- 64Bit: 2^40 = 109.951.162.777 Möglichkeiten
- Brutefoce Attack braucht ca. 10Min

- 128Bit = 2^104 Möglichkeiten
- IV's suchen, welche den Key-Setup-Algorithmus in jenen Status setzt, wo Informationen über den Key übertragen werden.
- 4-6 Mio. Pakete sammeln und man hat den Key

- **VPN Verbindung**
- Tunnel zw. zwei PCs (oder Client und AP)
- fast beliebig große Verschlüsselung
- Shared Key- oder Public Key Verschlüsselung
- Public Key hat den Vorteil das einzelne Keys gesperrt werden können, bei Shared Key ist das Netz bei bekanntem Key "offen"
- im Gegensatz zu WEP kann hier kein Key erraten werden
- Authentifizierung kann gewährleistet werden (ipsec)

- **Wardriving (Begriff):**

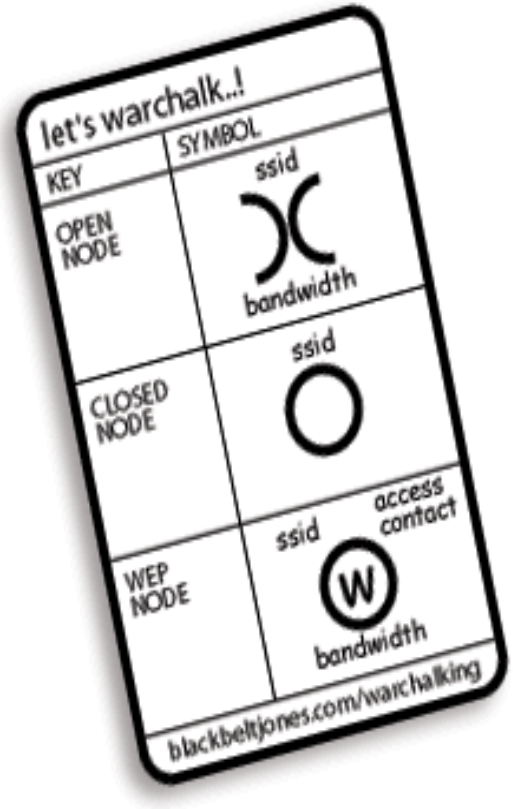
- Begriff: kommt von "Wardialing"
  - Ausprobieren von Telefonanschlüssen
- Was man braucht:
  - Fortbewegungsmittel (Auto, Fahrrad...)
  - Laptop, oder PDA
  - WLAN Karte
  - Software (Kismet + div. Sniffer)

- **Warum Wardriving ?**

- WLANs finden und karthographieren (GPS)
- gucken wer wo ein offenes WLAN hat
- Neugier, was in den Netzen so passiert
- Kostenlos (und völlig annonym) im Internet surfen
- bei besonders kritischen Fällen Besitzer informieren (2001 – Krankenhäuser in Berlin)

- **Warchalking**

- makieren von gefundenen Aps für andere Wardriver und Leute die "Netz" brauchen



- **Links**

- http://www.it-academy.cc/content/article_browse.php?ID=593
- http://hostap.epitest.fi/
- http://www.worldwidewardrive.org/
- http://www.wardriving-forum.de/
- http://www.doc-x.de/cgi-bin/wiki.pl?WarChalking