

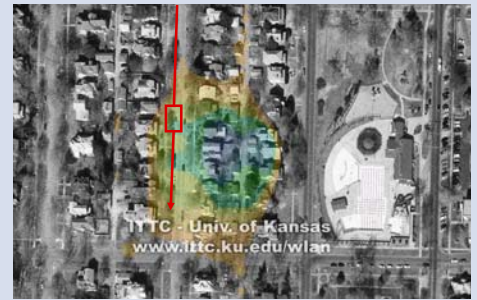
Wie sichere ich mein WLAN?



Andreas Steffen

Dr. sc. techn., Dipl.-Ing. ETH
 Leiter der ZHW Security Group
 Zürcher Hochschule Winterthur
 andreas.steffen@zhwin.ch

WLAN War Driving



WLAN Sniffer

MAC	SSID	Chan	Vendor	Type	Encry	SSID#	Latitude	Longitude
0000651D0484	erika:tos Computer	1	Apple	AP	WEP	11	N46.889517	E7.952600
0002A56F10CE	ego:Tap1	3	Compaq	AP		10	N46.954983	E7.474467
00032071E18E	top	6	GGT Linksys	AP		23	N46.945750	E7.464762
0006B31F4F31	FHA11M	7	Z-Com	AP		15	N46.948080	E7.431550
00094B8A72D2	tsnet	1	Gentek (D-Link)	AP	WEP	16	N46.940217	E7.435767
0000CC3838BD	GROUP:SEBID	14.1	AP			21	N46.943000	E7.428533
0002CC3838AE	Helenone	1.4	AP			22	N46.948733	E7.447950
000255316A41	home	8.14	Linksys	AP		31	N46.849500	E7.576700
0000651921DF	HOME:BERT	11	Apple	AP	WEP	17	N46.889500	E7.943833
0006B31F868B	HOME1	11.14	Z-Com	AP		9	N46.902200	E7.539183
00065565E939	home_network	1.14	Linksys	AP		22	N46.822233	E7.596517
0040864F6E22	hotspot:bal	13	Cisco (Aironet)	AP		14	N46.945783	E7.430550
0040864E3CA3	hotspot:bal	6.14	Linksys	AP		23	N46.942767	E7.430450
00324818F3C3	bluetooth:home	11.14	Delta (Fujitsu)	AP	WEP	37	N46.933083	E7.489117
0002CD1EA88B	INTERMEC	11	Agere (Lucent) Omnicast	AP		9	N46.895700	E7.546050
0009B786C2C7	spab	5	Advanced Multimedia	AP	WEP	5	N46.954767	E7.476767
000186878174	Linksys:Zurich:Hotspot:bal	6	Advanced Multimedia	AP	WEP	26	N46.943767	E7.430500
00065565F2D2	Linksys	6	Linksys	AP	WEP	7	N46.945083	E7.427167

- NetStumbler erhältlich von <http://www.netstumbler.com>
- Laptop or PDA ausgerüstet mit GPS

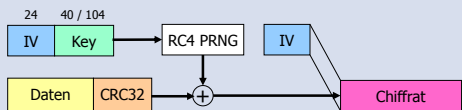
War Driving Karte von Zürich



Mehr als 700 Access Points, die meisten ohne WEP Verschlüsselung

Quelle: Tages-Anzeiger 14. Okt. 2002

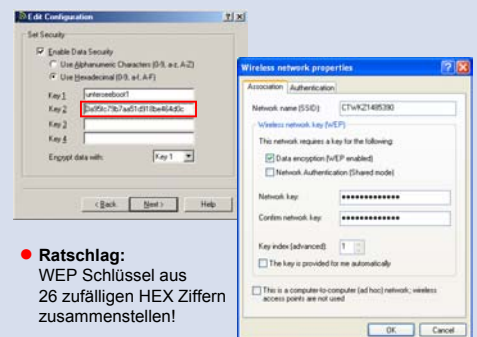
Wired Equivalent Privacy (WEP)



- Durch Sammeln von 3000-5000 schwachen Initialisierungsvektoren kann jeder 104 Bit RC4 Schlüssel innerhalb von Stunden bis Tagen bestimmt werden.
- Attacke implementiert durch AirSnort Tool.
- Häufig direkte Abbildung von ASCII Passwörtern in WEP Schlüssel (5 oder 13 Zeichen).
- Schwache Passwörter können durch Wörterbuchattacke in Minuten geknackt werden. ZHW Diplomarbeit 2002. <http://wepattack.sourceforge.net>

➡ WEP ist schwach und praktisch nutzlos!

Eingabe der WEP Schlüssel



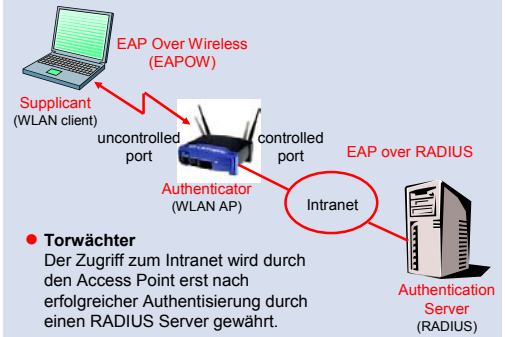
- **Ratschlag:** WEP Schlüssel aus 26 zufälligen HEX Ziffern zusammenstellen!

Wi-Fi Protected Access (WPA)

- **Temporal Key Integrity Protocol (TKIP)**
 - Vergrößerter Initialisierungsvektor
 - Kryptografisch gesicherte WLAN Pakete durch Message Integrity Check (MIC)
 - Periodisches Re-Keying vorgesehen (jede Stunde)
- **Extensible Authentication Protocol (EAP)**
 - IEEE 802.1x Protokoll regelt Netzwerkzugriff
 - EAP-TLS, respektive Protected EAP (PEAP) authentisieren den Benutzer via RADIUS-Server.
 - Für den SOHO Bereich sind weiterhin Passwörter vorgesehen → **Wörterbuchattacke !**
- **WPA ist eine Übergangslösung**
 - WPA ist ein vorwärtskompatibles Subset des kommenden IEEE 802.11i WLAN Security Standards.



IEEE 802.1x Authentisierung



- **Torwächter**
Der Zugriff zum Intranet wird durch den Access Point erst nach erfolgreicher Authentisierung durch einen RADIUS Server gewährt.

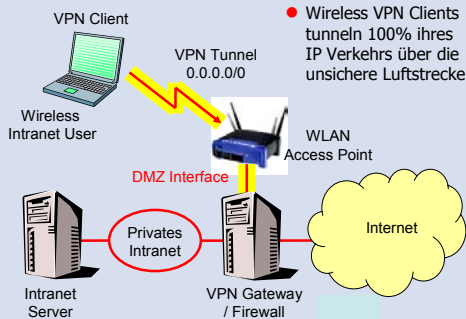
IEEE 802.1x mit EAP-TLS

- Unterstützung durch Windows XP

IEEE 802.1x mit PEAP

- Unterstützung durch Windows XP

Sicherheit durch VPN (IPsec)



Linux FreeS/WAN VPN Gateway

- OpenSource IPsec Stack für Linux
- Authentisierung durch Zertifikate entwickelt an der **ZHW !**
- Unbegrenzte Anzahl von VPN Tunnel
- Linux FreeS/WAN auch als VPN Client geeignet
- Erhältlich als SuSE/RedHat/Debian/Mandrake RPM
- Kommerzielle CD-Firewall Version: www.astaro.de
- Einfache Konfiguration:

```
conn vpnclients
right=%any
rightsasigkey=%cert
left=%defaultroute
leftsubnet=0.0.0.0/0
leftcert=gwCert.pem
auto=add
```

Windows VPN Clients

- Windows 2000/XP hat einen eingebauten IPsec Stack
- Konfiguration über Management Konsole (mmc) ist extrem mühsam und fehleranfällig.
- Open Source IPsec Tool von <http://vpn.ebootis.de> lädt Konfiguration direkt in die Windows Registry:

```
conn client-gateway
 left=%any           # insert client IP
 right=10.1.0.1     # gateway IP
 rightsubnet=*      # tunnel all traffic
 rightca="C=CH,O=ZHW,CN=ZHW CA"
 network=lan
 auto=start
```

- Kommerzielle Windows VPN Clients
 - SSH Sentinel: www.ssh.com
 - SafeNet / SoftRemote: www.safenet-inc.com

Zusammenfassung

- WLANs auch mit WEP Schlüssel sind extrem gefährdet!
- Neue WLAN Access Points werden mit WPA ausgeliefert.
- WPA stopft die grössten WEP Sicherheitslöcher.
- WPA ist nur mit einer RADIUS Infrastruktur und EAP-TLS Verbindung wirklich sicher.
- Die "arme Leute" Lösung wird weiterhin auf [schwachen] Passwörtern basieren.
- Ein äusserst sichere Alternative ist ein überlagertes Virtual Private Network auf IPsec Basis.
- Kostengünstige VPN Lösungen unter Linux, Windows und MacOS sind verfügbar.

Weitere Informationen unter <http://security.zhwin.ch>