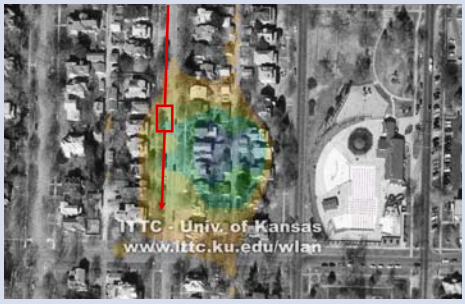
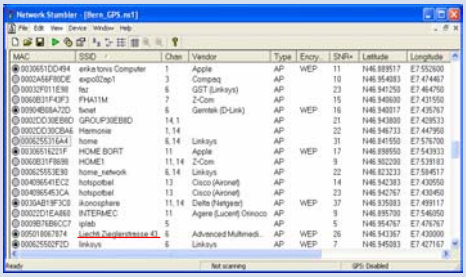
Wie sichere ich mein WLAN?

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

WLAN War Driving



WLAN Sniffer



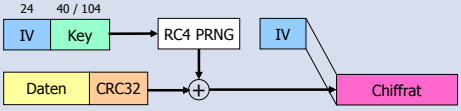
- NetStumbler erhältlich von http://www.netstumbler.com
- Laptop or PDA ausgerüstet mit GPS

War Driving Karte von Zürich

Mehr als 700 Access Points, die meisten **ohne** WEP Verschlüsselung

Quelle:
Tages-Anzeiger
14. Okt. 2002

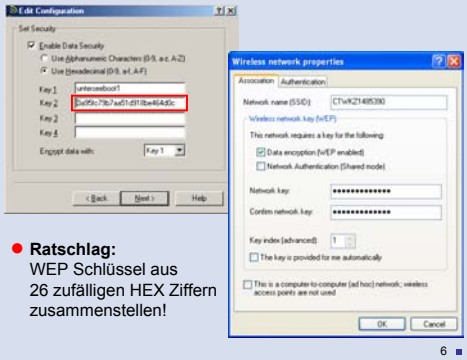
Wired Equivalent Privacy (WEP)



- Durch Sammeln von 3000-5000 schwachen Inititalisierungsvektoren 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

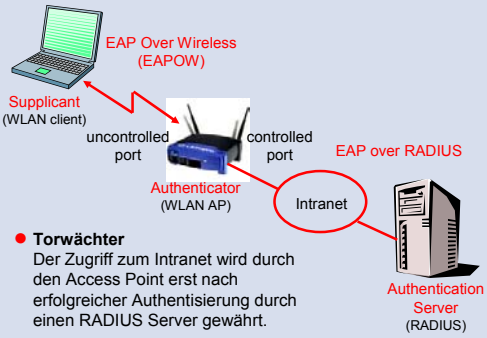


- **Ratschlag:**
  WEP Schlüssel aus 26 zufälligen HEX Ziffern zusammenstellen!

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.

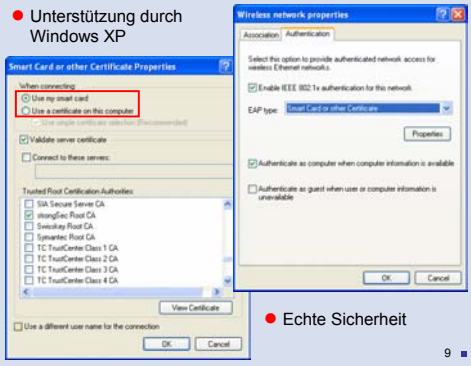
IEEE 802.1x Authentisierung



- **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

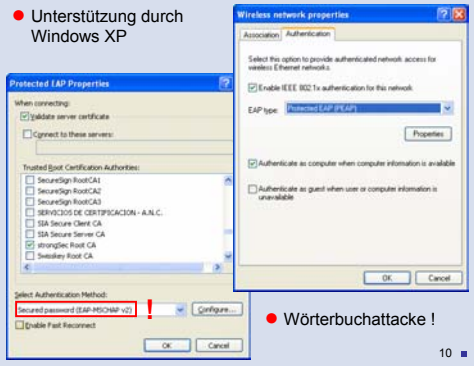
- Unterstützung durch Windows XP



- Echte Sicherheit

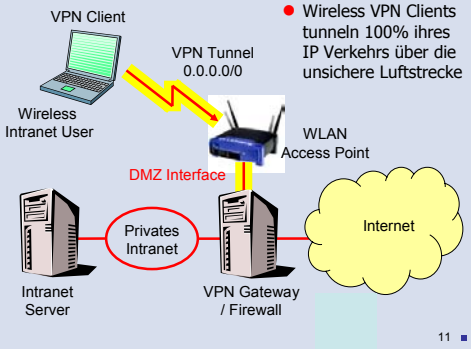
IEEE 802.1x mit PEAP

- Unterstützung durch Windows XP



- Wörterbuchattacke !

Sicherheit durch VPN (IPsec)

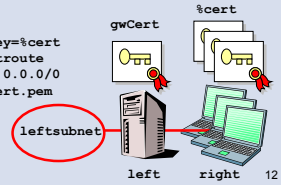


- Wireless VPN Clients tunneln 100% ihres IP Verkehrs über die unsichere Luftstrecke

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
     rightrsasigkey=%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 gröbsten 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**