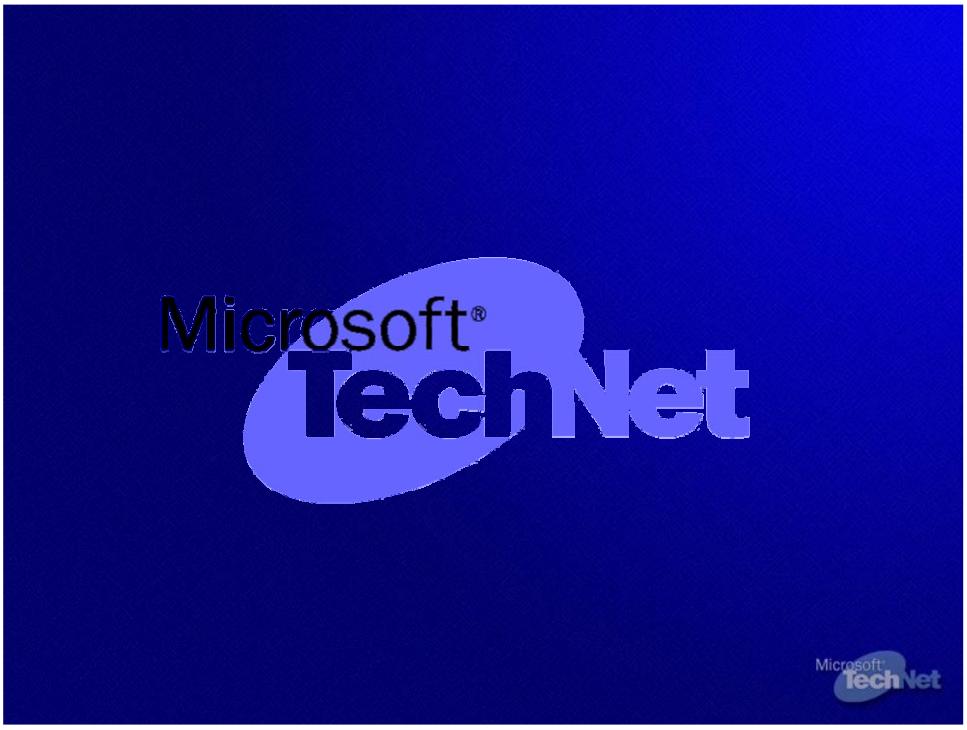


Microsoft Security

Installation und Sicherheit mit Windows im Wireless-LAN

Verwalten Mobiler Clients

Wojciech Micka
Microsoft Presales Consultant

Agenda

Microsoft Security

- IEEE 802.11 Grundlagen
  - Standards
  - Sicherheitsmerkmale
- WLAN Sicherheit
  - Authentifizierung
  - Verschlüsselung
  - EAP, RADIUS, IAS
- Wireless Deployment
  - Windows XP & Windows Server 2003
- Ausblick

Microsoft TechNet

IEEE 802.11 – Grundlagen
Standards

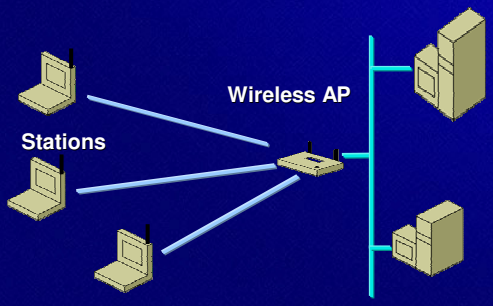
Wi Fi The Standard for Wireless Fidelity

- IEEE 802.11
  - IEEE & Wireless Ethernet Compatibility Alliance
- IEEE 802.11b
  - Bis zu 11 Mbps auf dem 2.45 GHz Band
- IEEE 802.11a
  - Bis zu 54 Mbps auf dem 5.8 GHz Band
- IEEE 802.11g
  - Bis zu 54 Mbps auf dem 2.45 GHz Band

Microsoft TechNet

IEEE 802.11 – Grundlagen
Netzwerk Komponenten

- Client = Station (STA)
- Wireless Access Point (AP)
  - Bridge zwischen verkabeltem und drahtlosem Netzwerk



IEEE 802.11 – Grundlagen
Client Initialisierungsprozess

- Client scant nach APs (Infrastructure) oder anderen Clients (Ad Hoc - Modus)
- Wählt einen AP zum Verbinden aus nach
  - Signalstärke = signal strenght
  - Netzwerkname = Service Set Identifier (SSID)
- “authenticate” und “associate” mit AP
- Fortlaufendes Scannen und “Re-association” am Access Point
- Evtl. Roaming zwischen den APs

IEEE 802.11 Grundlagen
Security

- Authentifizierung
  - Open System authentication
  - Shared Key authentication
- Vertraulichkeit der Daten
  - Wired Equivalent Privacy (WEP)
    - Entwickelt um drahtlose Netzwerke so sicher wie verdrahtete Netzwerke zu machen
    - Standard definiert nur 40/64 Bit Verschlüsselung
    - Kein Schlüssel Management

IEEE 802.11
Windows Support

- Voller Support für IEEE 802.11 in Windows XP und Windows Server 2003
  - IEEE 802.11b/g
  - IEEE 802.11a
  - Ad-hoc und Infrastructure Mode
- Authentifizierung
  - Open System authentication
  - Shared Key Authentication
  - IEEE 802.1X Authentication – EAP
- WEP Verschlüsselung mit 40/104 Bit

IEEE 802.11
Windows XP Support

- Wireless Autokonfigurations-Service
  - Wireless Netzwerkadapter übergibt sämtliche Informationen über WLANs an Windows
  - Betriebssystem ermöglicht automatische Konfiguration des Wireless Netzwerks
  - Windows cached die Einstellungen
  - Bevorzugte Reihenfolge
- Roaming support
  - Roaming zwischen APs bei schlechter Signalstärke
- Ältere Windows Versionen sind auf Tools der Hersteller angewiesen

WLAN Security
Authentifizierung

- Open System Authentication
  - Für Authentifizierung nur das Wissen über SSID und Kanal notwendig
  - Jeder anfragende Client wir authentifiziert
- Möglicher Schutz durch Hidden SSID
  - SSID nicht mehr broadcasten
  - Durch Sniffen von Steuerpaketen ermittelbar

WLAN Security
Authentifizierung

- Shared Key Authentication
  - Gemeinsamer 40 oder 104 Bit Schlüssel muss sowohl AP als auch Client kennen
  - Key kann auch zur Verschlüsselung mit statischen WEP verwendet werden
- Möglicher Schutz durch MAC- Filterung
  - Pflege der MAC-Adressen sehr aufwendig
  - Brute Force auf MAC relativ simpel, da Adressbereich eines Herstellers nur 2^{24} Bits
  - Kein Schutz vor MAC-Spoofing

WLAN Security
WEP Encryption

- WLAN Verschlüsselung ist wichtig!
  - Remote sniffing
- Zwei Shared Keys:
  - Ein Multicast / Global Key
  - Ein Unicast Session Key
- 40 oder 104 Bit Verschlüsselungs Key
- Symmetrischer Streamcipher → RC4
- 24 Bit Initialisierungsvektor (IV)
  - Low : 64 Bit = 40 Bit Key + 24 Bit IV
  - High : 128 Bit = 104 Bit Key + 24 Bit IV

WLAN Security
Schwachstellen von WEP

- WEP Keys
  - Erzeugung und Verteilung der WEP Keys ist im IEEE 802.11 Standard nicht definiert
- Algorithmus
  - RC4 Streamcipher ist bei statischen WEP Keys nicht ausreichend
  - viel bekannter Plaintext wie z.B. TPC/IP-Header, ICMP, ARP Pakete, bestimmte Webseiten, Spam
  - Generalschlüsselproblem von statischem WEP
- Initialisierungsvektor (IV)
  - Verwendung der IVs nicht definiert
    - Reset des IV auf 0 beim Restart, „IV Reuse“
  - Erzeugung von zufälligen IVs nur schwer möglich
  - IV Kollision statistisch nach 4.000 Paketen

Microsoft TechNet

WLAN Security
Angriffe auf WLANs

- Diverse aktive und passive Attacken
  - Keystream Reuse
  - Known Plaintext
  - “Bit-Flipping” Attacken
- Tools längst verfügbar
  - WEPCrack
    http://sourceforge.net/projects/wepcrack
  - AirSnort
    http://airsnort.shmoo.com/

Microsoft TechNet

WLAN Security
Lösung Security Problems

- Offenes WLAN mit VPN
  - Manuelle Reconnect / Roaming
  - Computerpolicies
  - VPN Serverlast
  - Quarantäne für unsichere Clients
- WEP+ und “Weak Key Avoidance”
- Dynamic WEP mit IEEE 802.1X (EAP)
  - Erfordert Rekeying am RADIUS Server
- IEEE 802.11i
  - Superset von WPA

WLAN Security
IEEE 802.11i – WPA

- Wi-Fi Protected Access (WPA)
  - Subset von 802.11i
  - seit Anfang 2003 verfügbar
  - Softwareupdate für Wi-Fi konforme Geräte notwendig
- IEEE 802.1X (EAP) Authentifizierung
  - Periodisch wechselnder Key bei Re-Authentication

WLAN Security
IEEE 802.11i – WPA

- Verbesserte Datenverschlüsselung mit TKIP
  - Temporal Key Integrity Protocol (TKIP)
  - Vergrößerter Initialisierungsvektor (IV)
  - Re-Keying Mechanismen
  - Message-Integrity-Check (MIC)…
- WPA Wireless Security Update für Windows XP ab dem 30.03.04 verfügbar:

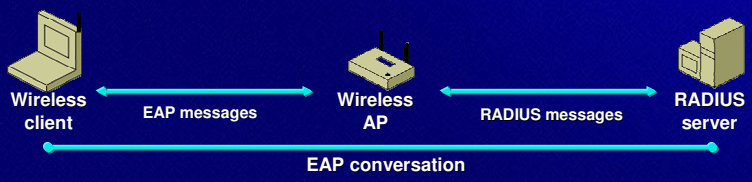
  Q815485
  http://support.microsoft.com/default.aspx?scid=kb;en-us;815485&Product=winxp

WLAN Security
IEEE 802.11i – Zunkunft

- IEEE 802.11i Verbesserungen
  - Verwendung von Advanced Encryption Standard (AES) an Stelle des RC4 Streamcipher
  - Benutzung der Kerberos Authentifizierung bei 802.1X – EAP
  - Dynamisches WEP mit Rekeying
  - Secure De-Authentication und Disassociation

WLAN Security
Mögliche Lösungen

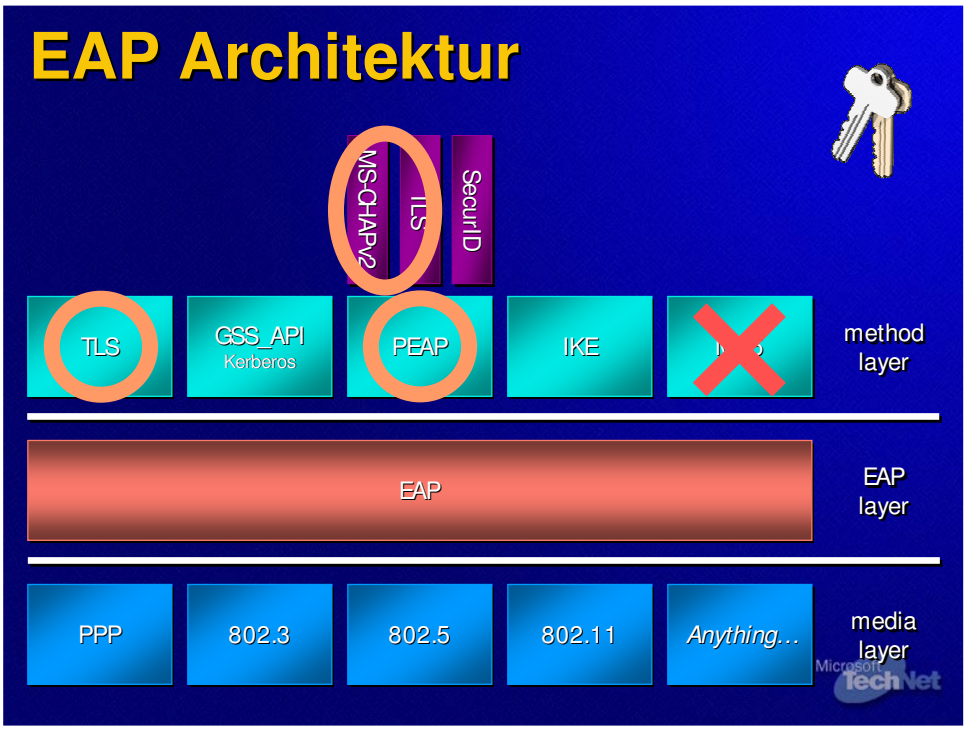
- IEEE 802.1X - EAP und RADIUS
  - Station = EAP Client
  - Access Point = RADIUS Client
  - Microsoft IAS = RADIUS Server
    - erzeugt dynamische WEP Keys per Session
  - User werden am AD validiert



IEEE 802.1X - EAP
Definition

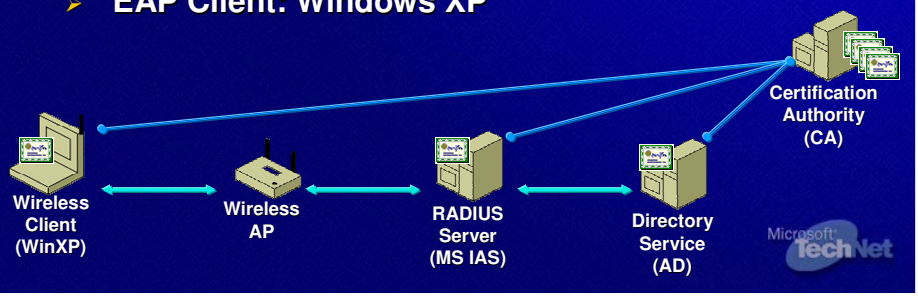
- Erweiterung von PPP für Port-basiete Zugriffskontrolle
  - Authentifizierung an Ethernet Switches
  - Später auf IEEE 802.11 adaptiert
- Erfordert Authentifizierung bevor Datenaustausch mit dem Netz erlaubt ist
- Verwendet Extensible Authentication Protocol (EAP)
- IEEE 802.1X definiert “EAP over LAN” (EAPOL)

EAP Architektur



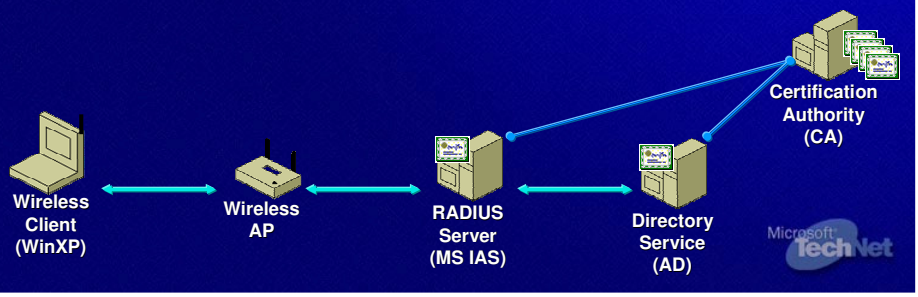
EAP
EAP Typen unter Windows

- EAP-TLS (Transport Layer Security)
  - Für Zertifikatsbasierte Umgebungen (PKI)
  - Setzt Benutzerzertifikat voraus
    - Computerzertifikat für Client optional
  - RADIUS Server: Windows 2000 SP3 + Hotfix
  - EAP Client: Windows XP



EAP
EAP Typen unter Windows

- PEAP (Protected EAP)
  - Erweiterung zu EAP mit MS-CHAPv2
  - Zertifikatsfreie Anmeldung mit Benutzername und Passwort
  - RADIUS Server: Windows Server 2003
  - EAP Client: Windows XP SP1



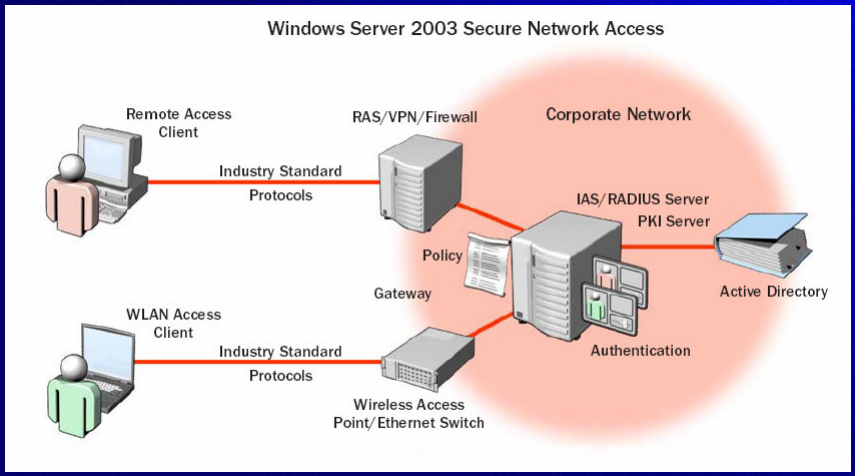
EAP
Andere EAP Lösungen

- LEAP (Ciscos Wireless EAP)
  - Ähnlich wie EAP-TLS
  - Für Windows 9x, NT, 2000, sowie XP verfügbar
  - Clientsoftware von Cisco
  - z.B. der Benutzername und das Passwort für eine beidseitige Authentifizierung
  - Informationen werden im Speicher der Netzwerkkarte festgehalten bis Computer ausgeschalten oder Netzwerkkarte entfernt wird.
  - RADIUS Server: Cisco Secure Access Control Server Version 2.6

RADIUS / IAS
Überblick

- Internet Authentication Service
  - Microsoft® RADIUS Server Implementierung
    - Windows 2000 Server Family (ab SP3)
    - Windows Server 2003
- Benutzt Active Directory als Benutzerdatenbank
- Remote Access Policy
  - Conditions
    - NAS-Port-Type=Wireless-IEEE 802.11
    - Windows-Groups=WirelessUsers
  - Profile settings
    - Strongest encryption
    - EAP-TLS oder PEAP authentication method

RADIUS
RADIUS Infrastruktur



Wireless Deployment
EAP Szenario

- Konfigurieren einer Public Key Infrastructure (PKI)
- Konfigurieren des Active Directory (2000 oder 2003)
  - Globale Gruppe “Wireless User”
- Konfigurieren des primären IAS Server
  - Windows 2000 Server für EAP-TLS
  - Windows Server 2003 für PEAP/EAP-TLS
  - Conditions
    - NAS-Port-Type=Wireless-IEEE 802.11
    - Windows-Groups=WirelessUsers
- Konfigurieren des AP als RADIUS Client
  - Shared Secret mindestens 22 Zeichen und komplex
- Installieren von Benutzer und Computer Zertifikaten

Wireless Deployment
EAP Szenario – PKI

- Enterprise Root CA oder Alleinstehende CA von Windows 2000 oder Windows Server 2003
- Installieren von Computer Zertifikaten für
  - EAP-TLS: auf Wireless Clients (optional) und RADIUS Server
  - PEAP: nur auf dem RADIUS Server
- EAP-TLS: Installieren von Benutzer Zertifikaten für die Wireless User
- Jeder muss in der Lage sein, dass Zertifikat des anderen zu validieren
  - Wireless client ▸ IAS Server’s Zertifikat
  - IAS Server ▸ Wireless Clients’ Zertifikat
- Installieren des Root Server Zertifikats auf allen Maschinen

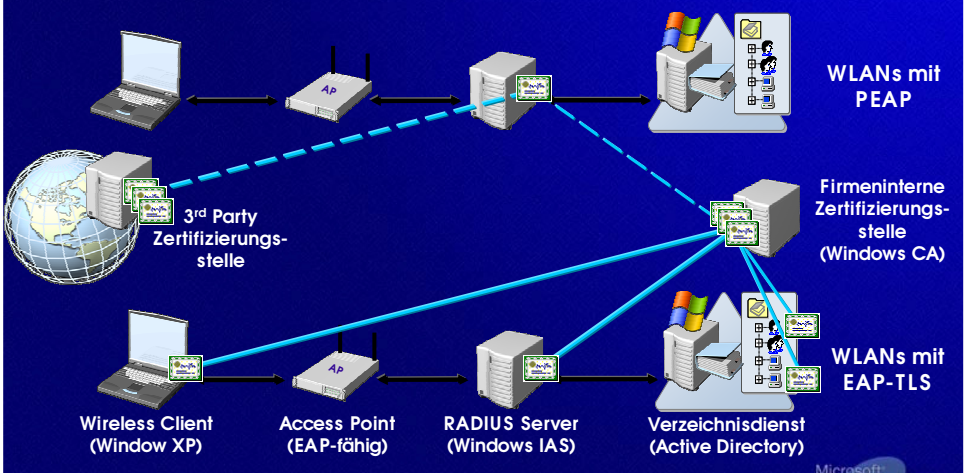
Wireless Deployment

PKI – Welche Serverversion ist die Richtige?

- Externes Trustcenter
- Windows Server 2003 Standard Edition CA
  - Für alle Grundlegenden WLAN PKI Anforderungen ausreichend
- Windows Server 2003 Enterprise Edition CA
  - Unterstützt hilfreiche neue Funktionen:
    - Zertifikatsvorlagen Version 2
    - Zertifikatsautoenrollment (auch für Benutzer)
    - Private Key Archival

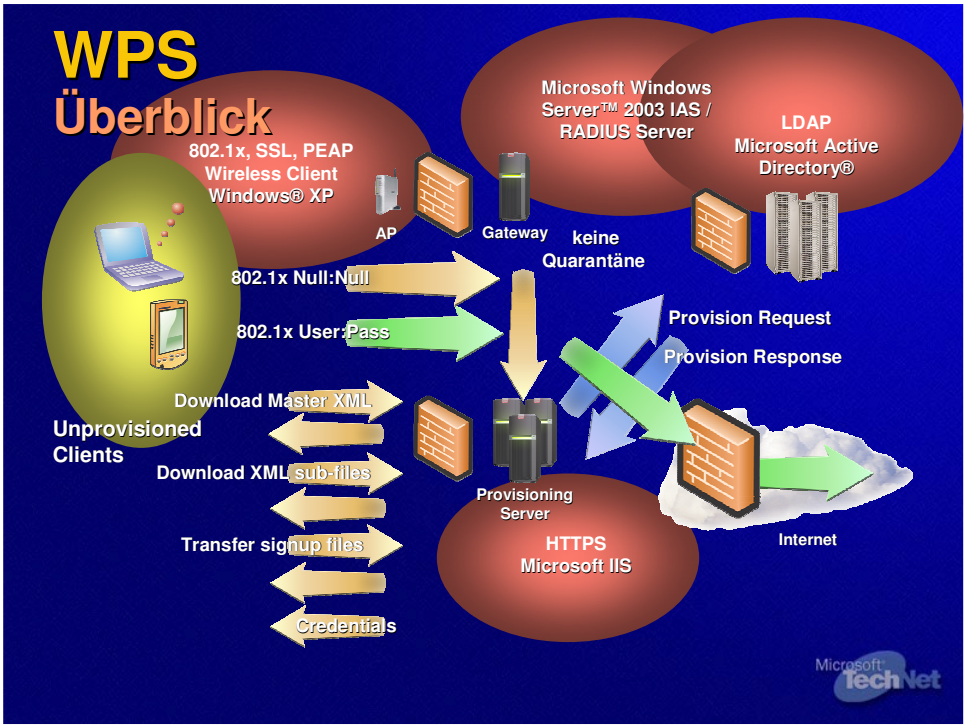
Wireless Deployment

PEAP & EAP-TLS Szenario



Wireless Provisioning Services

- Erweiterung des Autokonfigurations-dienstes von Windows
  - Integriert in Windows XP SP2 & Windows Server 2003 SP1
- Basiert auf Standards
  - XML, 802.1x
- Ermöglicht alternative Verfahren zur WLAN Client Anmeldung an Hot Spots
- Cable Guy Artikel unter: http://www.microsoft.com/germany/ms/technetdatenbank/showArticle.asp?siteid=600286



Fazit

- 802.11 hat diverse Sicherheitsschwächen
  - Keine Per-User Identifikation und Authentifizierung
  - Kein Per-Session Key Management
  - WEP Problematik
- Betrieb eines sicheren WLANs ist möglich
  - Als Hotspot im Perimeternetzwerk mit VPN
  - Mittels IEEE 802.1X – EAP Authentifizierung
    - Microsoft IAS Server ist RADIUS Server
    - Keymanagement mit dynamischen Session Keys
    - Windows PKI und Windows XP

Ausblick

- IEEE 802.11i
  - Vergrößerter Initialisierungsvektor auf 128 Bits
  - Benutzung von Kerberos für die Authentifizierung
  - Verwendung von Advanced Encryption Standard
- IEEE 802.1X Clients mit EAP-TLS und PEAP mit MS-CHAP Version 2
  - Windows 2000, Windows NT® 4, Windows 98, Windows Millennium Edition, Pocket PC 2003
- Support von Cisco's Lightweight Extended Authentication Protocol (LEAP) ist nicht geplant
  - Proprietäres Authentifizierungsverfahren

Ressourcen

- Wi-Fi in Windows
  http://www.microsoft.com/windows2000/technologies/communications/wifi/default.asp
- Wireless 802,11 Security in Windows XP
  http://www.microsoft.com/windowsxp/pro/techinfo/administration/wirelesssecurity/default.asp
- Making IEEE 802.11 Networks Enterprise-Ready
  http://www.microsoft.com/technet/itsolutions/network/deploy/depovg/ieee802.asp
- NetStumbler Homepage – WLAN Sniffing Tool
  http://www.netstumbler.com/
- Warchalking und WLAN Sniffing
  http://www.warchalking.org/