Virtuelle Präsenz

Sicherheit und Privatsphäre in WLAN Technik

Xu,Wenjia

Überblick

- **Privatsphäre**
- **Standard im Bereich WLAN**
- **WEP - Wired Equivalent Privacy**
- **Sicherheit in WLAN Netzwerken**

1 Einleitung

- Was ist WLAN
- Die Geschicht von WLAN

- erst im Industriebereich durchgeführt
- vorallem an Netzen mit hohen Übertragungsraten von bis zu 100 Mbit/s
- 1997 Frequenzbereich zwischen 2,4 GHz und 5 GHz im komerziellen Bereich
- später durch die verschiedenen IEEE 802.11 Standards und durch den HomeRF-Standard und durch HIPERLAN
- in den letzten Jahren in vielen professionellen und semiprofessionellen Umgebungen

2 Privatsphäre

- **die Anlagen des WLAN**
  - **Access Point**
  - **Antenne**
  - **Wireless Lan Karte**
  - **PDA**

2.1 Access Point

- Übergang zwischen einem drahtgebunden zu einem drahtlosen Netz herstellen
- viele WLAN-Clients (Endgeräte) einbuchen über den AP Daten austauschen
- Anbindung von PCs an das Internet über einen ADSL oder ISDN Anschluss

2.2 Antenne

Die Aufgabe:

- hochfrequente Energie in Form eines elektromagnetischen Feldes abzustrahlen
- ein elektromagnetisches Feld auffangen
- in hochfrequente Energie umformen

2.3 Wireless Lan Karte

- PC Card mit einem PCI-Adapter oder ein (USB)-Gerät

2.4 PDA

- mit einem schnell startenden Betriebssystem
- Anwendungen unter dem Begriff PIM-Software
- Adressbuch, Terminplaner, Kalender, Notizblock, Aufgabenplaner, E-Mail und Projektmanagement
- textverarbeitung, Tabellenkalkulation, Taschenrechner und Spiele
- Abspielen von Musik (MP3) ,aufnehmen von gesprochenen Notizen , Geräuschen
- software nachladbar
- mit Mobiltelefon verbinden

3 Standard im Bereich WLAN

3.1 IEEE 802.11

- Frequenzband: 2.4 GHz
- Modulation: FHSS (Frequncy Hopping Spread Spectrum) oder DSSS (Direct Sequence Spread Spectrum)
- Max. Datentransferrate (Brutto): 1Mbit, 2Mbit
- erste Standard im Bereich WLAN

3.5 HomeRF

- Frequenzbereich: 2,4 GHz-ISM-Band
- Modulationsverfahren: 75 Kanäle mit einer Bandbreite von 1 MHz
- Reichweiten: 50 m
- Datenraten und Verkehrstypen: Daten ‚Sprach- und Multimediaverkehr
- Vorteile: kostengünstig

3.6 **Bluetooth** (1)

- Frequenzband: 2.4 GHz
- Modulation: FHSS
- Max. Datentransferrate (Brutto): bis 1Mbit
- Max. Datentransferrate in der Realität (Netto)(mit aktivierter Verschlüsselung): maximal 720kbit/s (=90kByte/s) bei idealen Bedingungen (1m Distanz, 1 Client)

3.6 **Bluetooth** (2)

- eine 'End-to-End'-Schnittstelle
- mit Bluetooth Maus, Tastatur, Modem, Drucker, Mobiltelefon, Organizer und Videokamera an den PC anbinden
- Audio-Anwendungen, z.B. drahtlose Kopfhörer oder Freisprecheinrichtungen
- Charakteristisch:
  - Geringe Stromverbrauch
  - Geringe Reichweite
  - billig

4 WEP - Wired Equivalent Privacy

- Verschlüsselungsverfahren
- ein sicherer Schlüssel hinterlegen
- Funktionen für die Paketverschlüsselung und zur Authentifizierung zur Verfügung stellen

4.1 Authentifizierung

- zwei Verfahren
- Open System Authentication : für ein WLAN alle Clients frei schalten
- Shared Key Authentication :mittels einem Challenge-Response-Verfahren mit einem geheimen Schlüssel zur Authentifizierung

4.2 Verschlüsselung(1)

- Bestandteil vom WEP-Datenpaket :

-geheimer WEP-Schlüssel mit 40 oder 104 Bit

-32-Bit-Prüfsumme der unverschlüsselten Daten

-24-Bit Initialisierungsvektor (IV)

4.2 Verschlüsselung(2)

- Zusammensetzen des Datenpakets
- Mit der IV-WEP-Schlüssel-Kombination verschlüsseln
- IV vorangestellt:den RC4-Schlüssel zusammensetzen,verschlüsselten Daten entschlüsseln

4.3 Sicherheitsproblem

- Schlüssel knacken
- WLAN-Kommunikation abhören
- handelsübliche Hardware nötig
- 6777216 (224) Schlüsselmöglichkeiten
- 11 MBit-Access-Point in ca. einer Stunde wiederholen
- Entschlüsseln

6 Sicherheit in WLAN Netzwerken

grundlegende Regeln

- Konfigurations-Passwort setzen
- Fernkonfiguration deaktivieren
- WLAN-Verschlüsselung aktivieren
- automatische Schlüsselübertragung deaktivieren
- SSID Broadcasts abschalten
- MAC-Adressen anlegen
- IP-Adressen explizit festlegen

End