Wireless LAN

Georg Lukas, 2004-12-07

MDLUG Themenabend

http://op-co.de/wlan/

Gliederung

- Technik
  - Allgemeines
  - Betriebsarten
  - Standards
- Sicherheit
  - Probleme
  - Standards

WLAN - Technik allgemein

- ursprünglich ISM-Band 2400 - 2500 MHz
  - Industrial Scientific Medical Band
  - HomeRF, Bluetooth, Mikrowellen
- Service Set Identifier (SSID)
  - Identifikation eines Netzes
  - 32 Zeichen
- gemeinsame Mediennutzung
  - Kollisionen sehr "teuer"
  - CSMA/CA (Kollisionsvermeidung)
  - Wartezeiten zwischen Paketen (Inter-Frame-Space)
- Netto-Datenrate ca. 50%

WLAN - Betriebsarten

- Ad-Hoc
  - alle Stationen gleichwertig
  - gemeinsame BSSID (Basic SSID)
  - Independent Basic Service Set (IBSS)
  - oft fehlerhaft implementiert
- Infrastruktur
  - erfordert AccessPoint(s)
  - gemeinsame ESSID (Extended SSID)
  - 10 Beacon-Frames/s
    - Typ, Datenrate, Verschlüsselung
    - Einfache Entdeckbarkeit
    - ESSID verstecken

WLAN - Standards 1

- IEEE 802.11 (1997)
  - max. 2 MBit/s brutto
  - 2400-2500 MHz
  - 13 Kanäle (EU)
  - nur drei überlappungsfrei
  - 100mW Sendeleistung
- IEEE 802.11b (1999)
  - 11 MBit/s
- IEEE 802.11g (2003)
  - neues Modulationsverfahren - 54 MBit/s
  - Mischbetrieb mit 802.11b problematisch

WLAN - Standards 2

- IEEE 802.11a (2003)
  - 54 MBit/s
  - mehrere Bereiche über 5 GHz
  - unterschiedliche Nutzungsauflagen
  - Deutschland: 19 überlappungsfreie Kanäle
  - bis zu 200mW mit 802.11h (dynamische Anpassung)
  - teuere Karten und Antennen
- Proprietäre Erweiterungen
  - "802.11b+" - 22 MBit/s
  - "TurboMode" - 108 MBit/s auf 802.11a/g
  - herstellerspezifisch
  - Zertifizierung?

Sicherheit - Problematik

- Datenübertragung über offenes Medium
- physische Zugangssicherung kaum möglich
- Sicherheitsprobleme
  - Zugangsschutz
  - Vertraulichkeit
  - Authentizität
- Lösungsmöglichkeiten
  - MAC-Filter
  - WEP
  - ...

Sicherheit - WEP

- Wired Equivalent Placebo
- Shared-Key-Verfahren
- keine einheitliche Authentifizierung
- Verschlüsselung mit RC4
  - 24-bit Initialisierungs-Vektor (im Klartext übertragen)
  - 40- oder 104-bit Schlüssel (geheim)
  - RC4-Stream XOR Daten
- "Integritätssicherung" mit CRC
- zahlreiche Angriffe möglich

➜ unsicher!

Sicherheit - WPA

- Wi-Fi Protected Access
- Vorgriff zu 802.11i
- EAP (Extensible Authentication Protocol)
- "Personal Mode" (EAP-PSK)
  - pre shared key
  - Authentifizierung
- "Enterprise Mode" (EAP-TLS, -TTLS, ...)
  - Port-basierte Sicherheit
  - Authentication Server (RADIUS)
  - 802.1X für Zugang und Key-Management
- TKIP (Temporal Key Integrity Protocol)
  - dynamisch generierte Session Keys
  - RC4 mit 128 bit, 48-bit IV
  - Integritätssicherung (Michael)
  - für WEP-Hardware ausgelegt

Sicherheit - WPA2

- Vollständige 802.11i-Implementierung (2004)
- "Personal" und "Enterprise Mode"
- CCMP
  - 128-bit AES
  - 48-bit IV
  - Counter Mode with CBC-MAC (CCM)
  - Integrität und Verschlüsselung
- WPA weiterhin sicher
- AES für "behördentaugliche" Sicherheit

Fazit

- Infrastruktur-Netzwerke einsetzen
  - Linux-AP-Treiber für mehrere Chipsätze
- 802.11b/g für möglichst günstige Netze
- 802.11a als Ausweg der Kanalverknappung

- WEP fast so unsicher wie keine Verschlüsselung
- WPA/WPA2 oder VPN für Netzbetrieb
  - Clients ohne VPN nicht rausrouten

Fazit

- Infrastruktur-Netzwerke einsetzen
  - Linux-AP-Treiber für mehrere Chipsätze
- 802.11b/g für möglichst günstige Netze
- 802.11a als Ausweg der Kanalverknappung

- WEP fast so unsicher wie keine Verschlüsselung
- WPA/WPA2 oder VPN für Netzbetrieb
  - Clients ohne VPN nicht rausrouten

- Fragen?