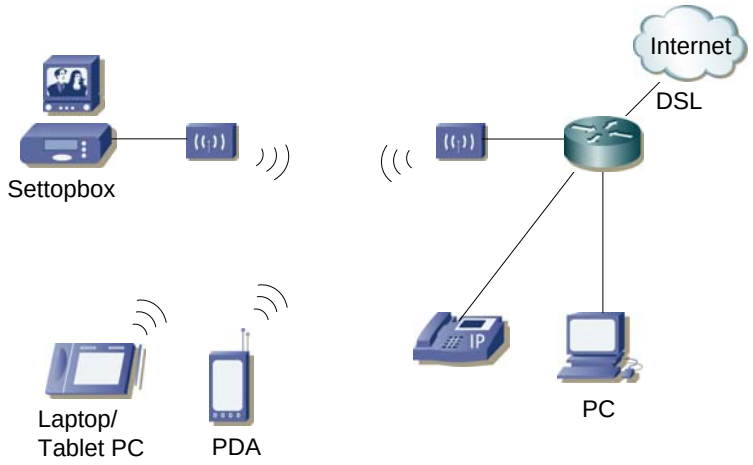
Wireless im Heimnetzwerk

Hans-Jörg Elias
HP Network Competency Center
Ratingen

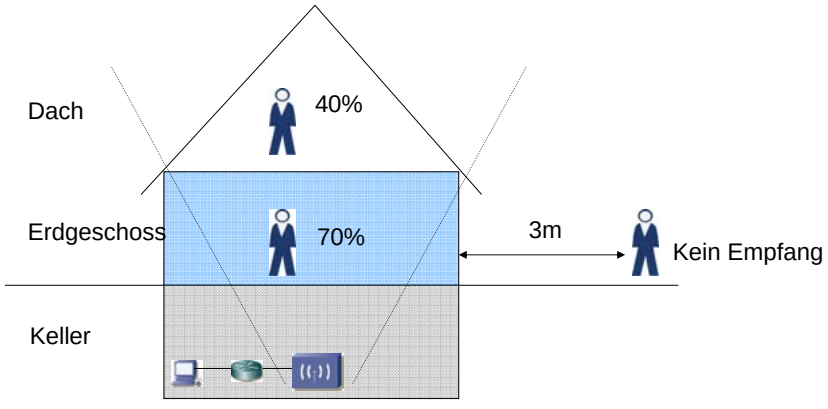
Übersicht

- Wie sichere ich mein Heimnetz?
- Physikalische Sicherung, Kanalwahl
- SSID
- Mac-Filter
- WEP, Home-WPA und 802.11i Verschlüsselung
- Dynamisches Re-keying mit WEP
- Überprüfung der Sicherheit

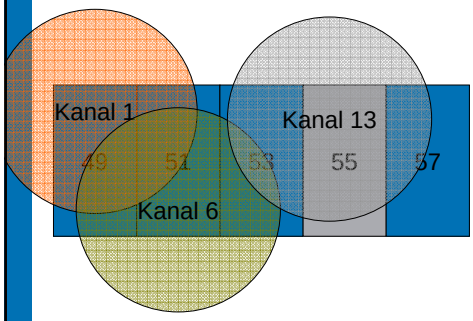
Das (un)typische Heimnetz



Physikalische Sicherheit



Die richtige Kanalwahl



Typische Reihenhaussiedlung

- Überschneidungsfrei:
  1-6/7-13
- Minimale Überdeckung:
  1-4-8-13

Was liegt noch in 2.4Ghz:

Bluetooth!!, Mikrowellen, Amateurfunker

Service Set Identifier (SSID)

- Bestimmt den Namen des Wireless-Netzes
- Wenn möglich SSID-Broadcast ausschalten
- Was ist besser, Shared oder Open Mode authentifizierung??
- Open Mode: AP antwortet nur wenn Packet richtig verschlüsselt
- Shared Mode: Authentisierung über Challenge/Response

➔ Am besten immer Open Mode benutzen!!

MAC-Filter

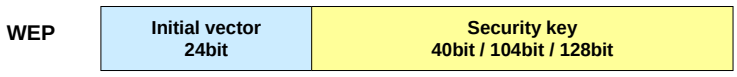
- Nur Geräte mit bekannter MAC-Adresse werden in das Netz gelassen

Nachteile:

- MAC-Adress spoofing einfach zu realisieren
- Kein Schutz gegen Abhören
- Können nicht alle Access Points
- Konfigurationsaufwand

WEP Verschlüsselung

- RC4 Verschlüsselung mit 24bit IV



Nachteile:

- Entschlüsselung schon nach 1 Million Pakete (=9 Minuten), bei Wörterbuchangriffen schon in 1s bis 1 Minute.
- Hauptproblem sind Kollisionen des IV
- Kein Key-Management, nur 4 Statische Schlüssel

Wi-fi Protected Access (WPA)

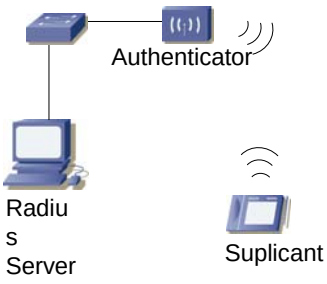
- Home WPA mit preshared-key Autorisierung
- WEP (AES optional) Verschlüsselung
- dynamischer Keywechsel (128bit)
- 64bit Message Integrity Code (MIC)
- 64bit IV

802.11i (WPA2)

- AES Verschlüsselung
- Preshared-key Autorisierung (WPA2-Personal)
- dynamische, rotierende Keys

- Der Standart für sichere Wireless Netzwerke

WEP mit rotierenden Keys

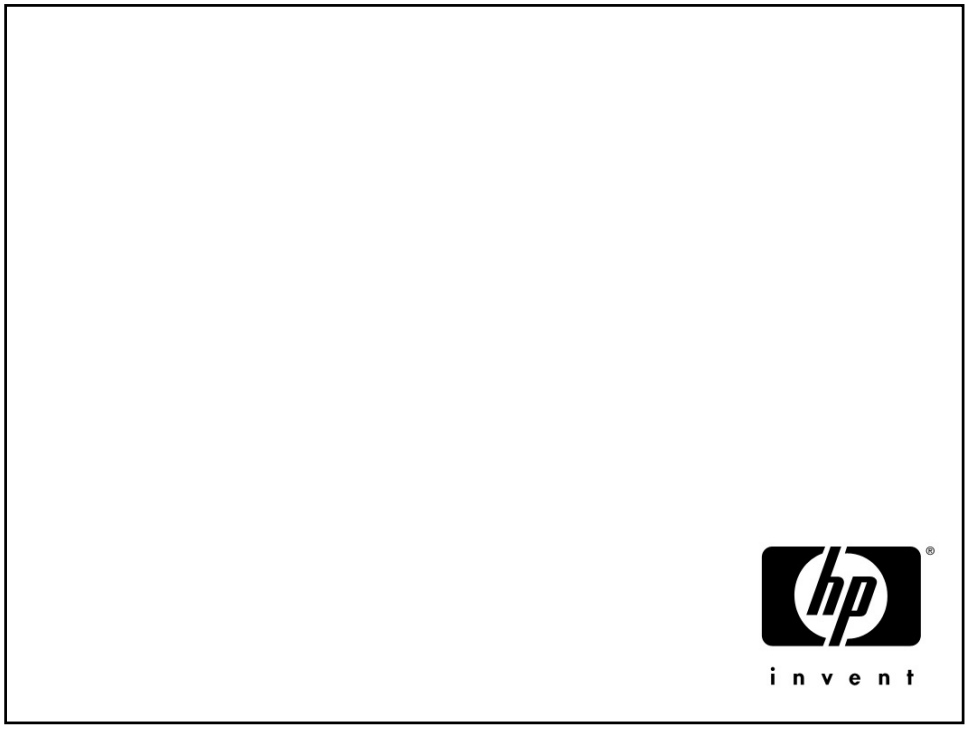


- 802.1x (EAP-TLS) ermöglicht rotierende WEP Keys auch mit einfachen AP‘s
- Radius Server mit Zertifikaten
- Client benötigt auch Zertifikate
- Jedes Wireless Gerät bekommt eigene WEP Keys

Sitesurvey (Laptop)

Von www.knoppix-std.org (oder www.knoppix.net) booten und eines der folgenden Tools benutzen:

- **airsnarf** : rogue AP setup utility
- **airsnort** : sniff, find, crack 802.11b
- **airtraf** : 802.11b network performance analyzer
- **gpsdrive** : use GPS and maps
- **kismet 3.0.1** : for 802.11 what else do you need?
- **kismet-log-viewer** : manage your kismet logs
- **macchanger :** change your MAC address
- **wellenreiter :** 802.11b discovery and auditing


invent