

WLAN-Cracking / WLAN-Sicherheit



Inhalt

- Grundbegriffe bzgl. WLAN
- Verschlüsselung
- Sonstige Sicherheitsvorkehrungen
- Rechtliches
- Verwendete Tools
- Wardriving

Grundbegriffe

BSSID

→ *Basic Service Set Identifier*

→ eindeutige Bezeichnung eines Access Points (MAC-Adresse)

SSID

→ *Service Set Identifier*

→ frei wählbarer Name eines Funknetzes

Grundbegriffe

Beacons

→ englisch für Leuchtfener, Lichtsignal

→ enthält den Namen des WLANs (SSID), Angaben zur Geschwindigkeit und zur Verschlüsselung

WPA-Handshake

Wenn ein Client sich zu einem WPA/WPA2 Funknetzwerk verbindet, so findet ein Vier-Wege-Handshake des TKIP-Protokolls statt.

Grundbegriffe

MAC-Adresse

→ *Media-Access-Control-Adresse*

→ eindeutige Hardware-Adresse jedes einzelnen Netzwerkadapters

ARP

→ *Address Resolution Protocol*

→ Netzwerkprotokoll für die Zuordnung von IP-Adresse zu MAC-Adresse

→ Zuordnungen werden im ARP-Cache gespeichert

→ Bsp.: *fritz.box (192.168.12.1) auf 00:1c:4b:94:f6:99 [ether] auf wlan0*

Verschlüsselung

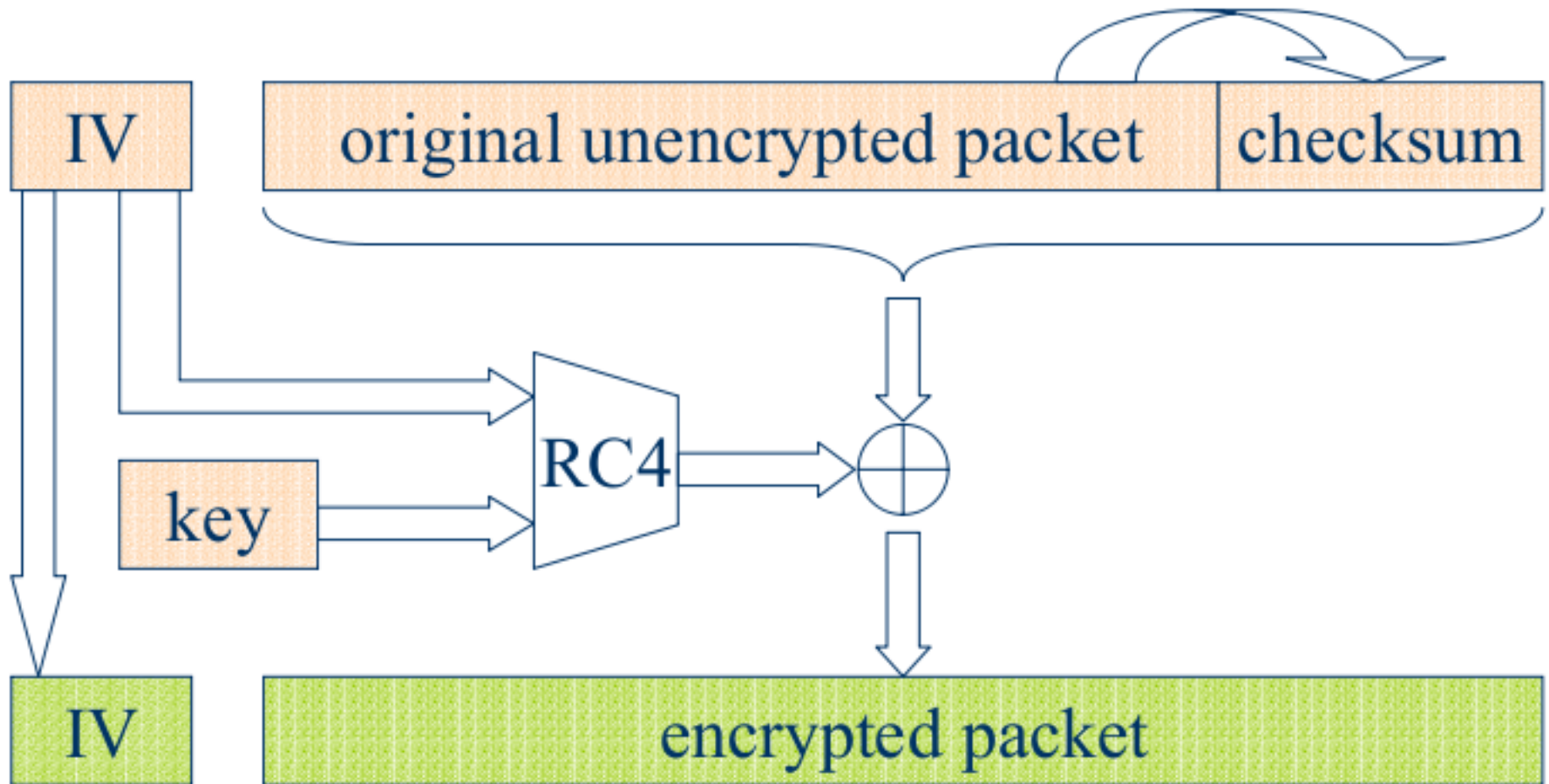
- WEP
- WPA
- WPA2

WEP

- 1997: Als Standard definiert durch IEEE.
(Institute of Electrical and Electronics Engineers)

- 2000: Erste Entdeckung von Lücken.

WEP



(c) David Wagner, University of California

WEP - Angriffsmöglichkeiten

- Es werden die Initialisierungsvektoren gesammelt.
- Durch sich wiederholende IVs kann die Passphrase geknackt werden.

- Neuer und schneller: PTW-Attacke
- Benötigt komplette Pakete

- Manipulation von Clients oder dem AP möglich um schneller Pakete zu sammeln
- Replay-Attacke: Ein abgefangenes Paket wird beliebig oft wieder gesendet

WPA

- 2003: Als Standard durch IEEE definiert.
- 2004: Wörterbuchangriff auf WPA-Handshake möglich.
- 2008: Wörterbuchangriff durch Nutzung der GPU bei einem Experiment um Faktor 10.000 schneller.
- 2008: Möglichkeit einzelne Pakete zu entschlüsseln, zu manipulieren und wieder ins Netzwerk einzuschleusen.

WPA - Angriffsmöglichkeiten

- Wörterbuchangriff auf WPA-Handshake
- Einzelne Pakete entschlüsselbar, Manipulation und Wiedereinschleusen in Netzwerk möglich

WPA – Unterschied zu WEP

- Nutzt ebenfalls RC4 → aber dynamischer Schlüssel (Per-Packet-Key-Mixing-Funktion)
- „Zutaten“:
 - Pairwise Transient Key
 - Sender-MAC
 - Seriennummer des Paketswerden zu einem Schlüssel gehashed.

WPA2

- 2004: Als Standard durch IEEE definiert.
- Wörterbuchangriff auf WPA-Handshake möglich.
- Nutzt AES statt RC4. (Ebenfalls mit dynamischen Schlüsseln.)
(AES = Advanced Encryption Standard)

Sonstige Sicherheitsvorkehrungen

- Hidden SSID
 - Der AP sendet keine Beacons aus
 - Clients müssen die SSID/BSSID kennen, um sich zu verbinden

- Angriffsmöglichkeit:
 - BSSID/MAC-Adresse des AP aus Paketen auslesbar
 - Voraussetzung: Ein Client kommuniziert mit dem AP

Sonstige Sicherheitsvorkehrungen

- MAC-Filter
 - Verbindung zum AP nur mit bestimmten MAC-Adressen möglich
 - Umsetzung mit White-/Blacklisting
- Angriffsmöglichkeit:
 - MAC-Adresse eines Clients aus Paketen auslesbar
 - Voraussetzung: Ein Client kommuniziert mit dem AP
 - Mit Tools (z.B. macchanger) MAC des Clients verwenden

Rechtliches

- Aus Sicht des WLAN-Betreibers
 - BGH-Urteil, 12. Mai 2010: Betreiber haftet für nicht oder unzureichend gesichertes/verschlüsseltes WLAN
 - Jedoch maximal 100€ Abmahnungsgebühr, kein Schadensersatz

Rechtliches

- Aus Sicht des Angreifers/Nutzers
 - Eindringen in ein verschlüsseltes Netz nach §202b StGB verboten!
 - Verbinden zu einem offenen Netzwerk grenzwertig, da die Daten
 - „[...] nicht für einen bestimmt [...]“ sind (privates WLAN)
aber auch nicht
 - „[...] gegen unberechtigten Zugang besonders gesichert sind [...]“.
(laut §202a StGB)
 - Könnte als Abhören von Funkanlagen nach §89 TKG gewertet werden.

Verwendete Tools

- Aircrack-ng
„Aircrack-ng is a set of tools for auditing wireless networks“.
aircrack-ng.org
- Ettercap-ng
„Ettercap is a suite for man in the middle attacks on LAN. It features sniffing of live connections, content filtering on the fly and many other interesting tricks.“
ettercap.sourceforge.net

Aircrack-ng

- Airmon-ng
→ Versetzt WLAN-Device in den Monitor Mode. (Alle Pakete lesen.)
- Airodump-ng
→ Speichert den gesamten Netzwerkverkehr. (Dank Monitor Mode.)
- Aireplay-ng
→ Erzeugt Traffic durch das Senden von ARP-Paketen. (Beschleunigt das Sammeln von Datenpaketen.)
- Aircrack-ng
→ Knackt den WEP-Schlüssel mit Hilfe der gesammelten Datenpakete.

Ettercap-ng

- Unterstützt ARP-Spoofing/ARP-Poisoning um MITM-Attacken durchzuführen
MITM = man in the middle
 - Angreifer teilt dem Router mit er sei der Client.
 - Angreifer teilt dem Client mit er sei der Router.
 - Datenverkehr läuft über den Angreifer
- So ist eine Analyse und vor allem eine Manipulation des Datenverkehrs möglich.

Live Demo



Ettercap - Angreifer



Ettercap - Opfer



Wardriving

- Wardriving ist das systematische Suchen und Erfassen von *Wireless Local Area Networks* (WLAN) mit Hilfe eines Fahrzeugs.
- Nur Erfassung:
 - Keine Sicherheitsvorkehrungen werden umgangen.
 - Es wird keine Verbindung zu den Netzwerken aufgebaut.
 - Sollte somit legal sein.

Wardriving

- Kismet
 - „Kismet identifies networks by passively collecting packets and detecting standard named networks, detecting (and given time, decloaking) hidden networks, and inferring the presence of nonbeaconing networks via data traffic.“
 - kismetwireless.net*
- Wir haben damit
 - Netzwerke gesucht und
 - mit GPS geografisch eingeordnet.

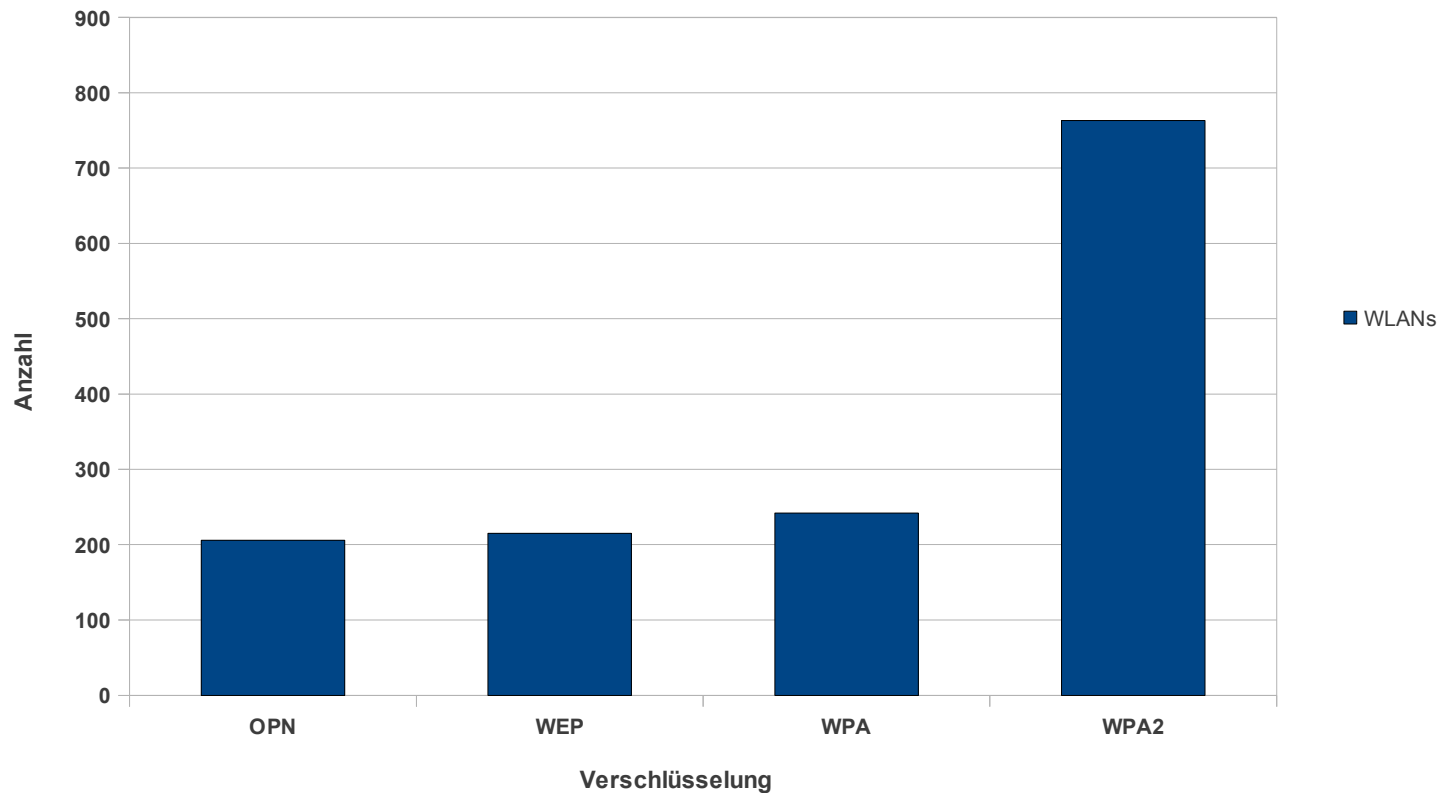
Wardriving

- Zur Auswertung der gesammelten Daten wurden zwei Programme entwickelt und eines modifiziert:
 - merge-netxml.py
 - Fügt mehrere Kismet-Logfiles zusammen und entfernt doppelte Datensätze.
 - statistic-netxml.py
 - Erstellt eine Statistik aus Kismet-Logfiles über Verschlüsselung, Funkkanäle, Hersteller des AP und die SSID gefundener Netzwerke.
 - pykismetkml.py
 - Konvertiert Kismet-Logfiles vom NETXML-Format ins KML-Format um von google-earth verwendet werden zu können.

Wardriving in Aalen - Verschlüsselung

VERSCHLÜSSELUNG

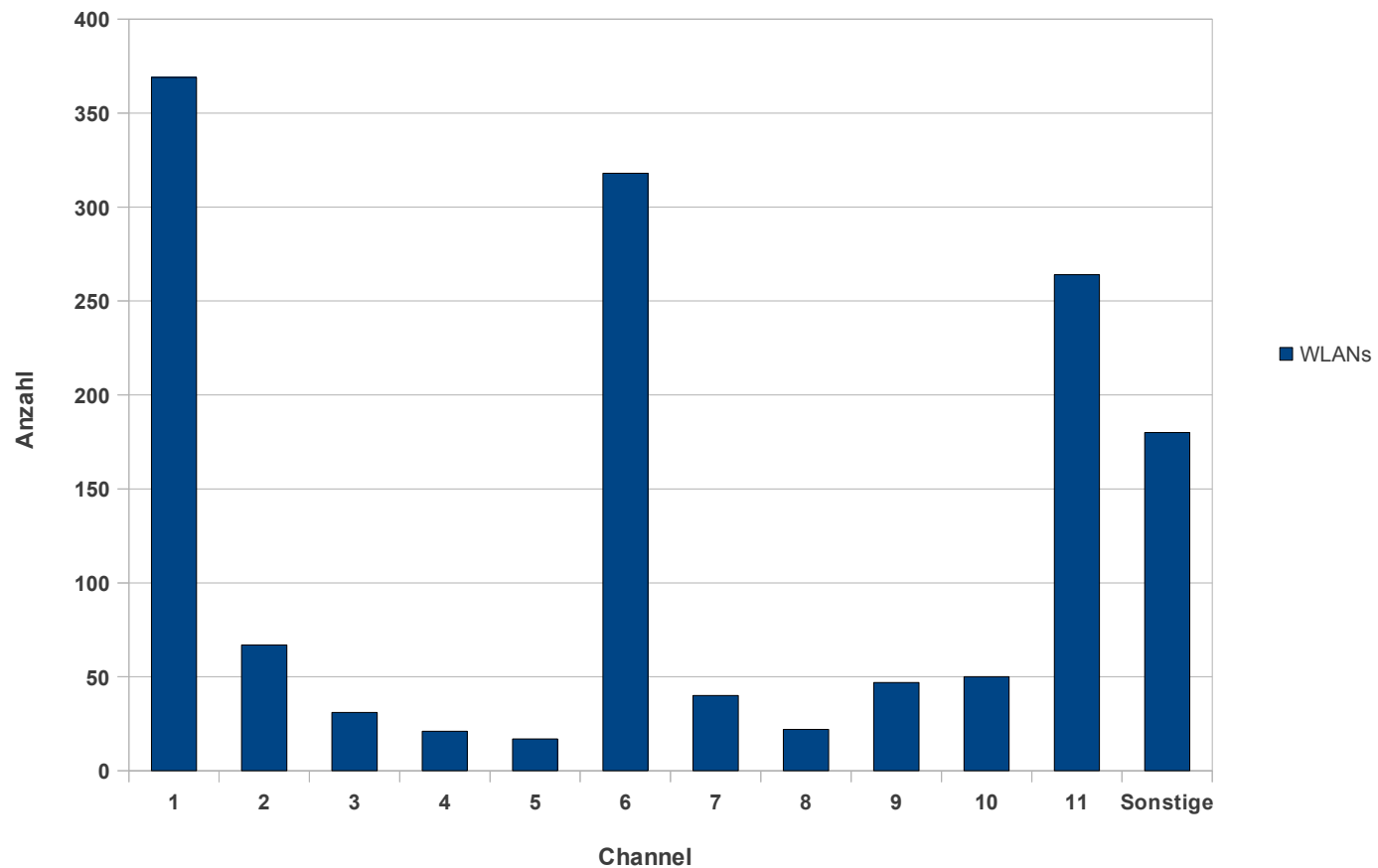
(1426 WLANs in Aalen)



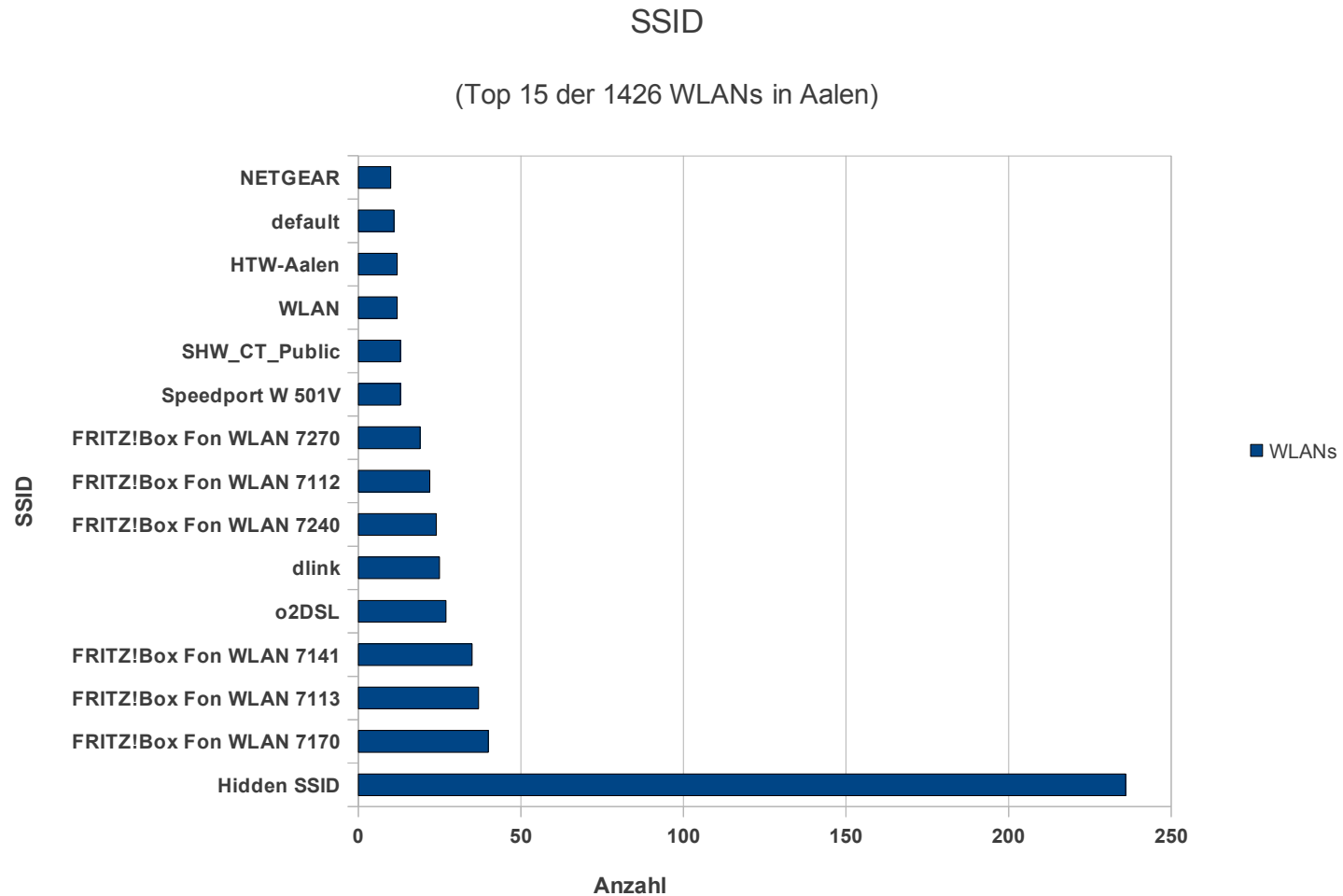
Wardriving in Aalen - Channels

CHANNELS

(1426 WLANs in Aalen)



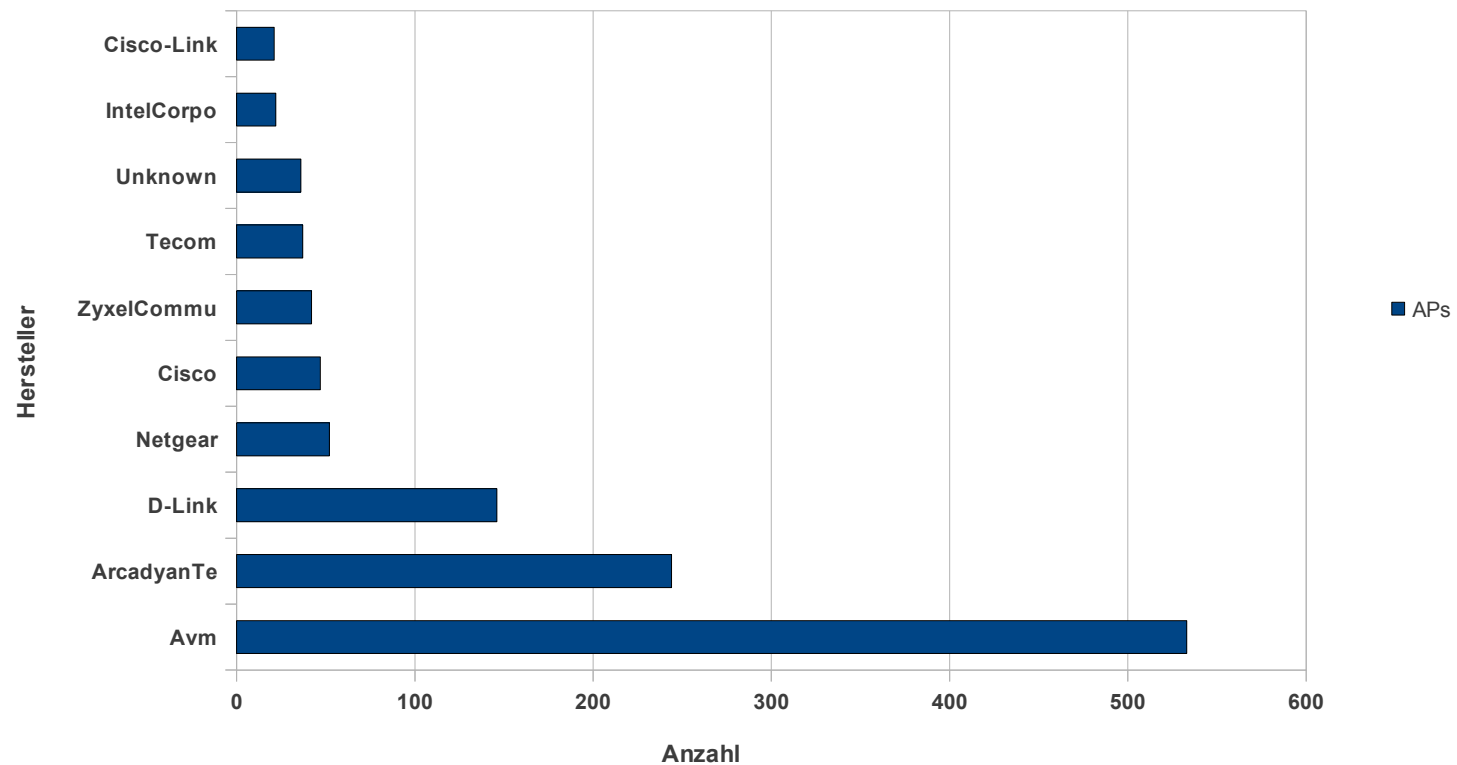
Wardriving in Aalen - SSID



Wardriving in Aalen - Hersteller

HERSTELLER

(Top 10 der 1426 WLANs in Aalen)



WLANS in Aalen

- Präsentation in google-earth