WLAN – Sicherheit

Dokumentation eines Projekts im Rahmen der Vorlesung
„Aktuelle Themen der IT-Sicherheit“
von Andreas Jansche und Gerhard Klostermeier

Inhaltsverzeichnis

Theorie

Grundbegriffe

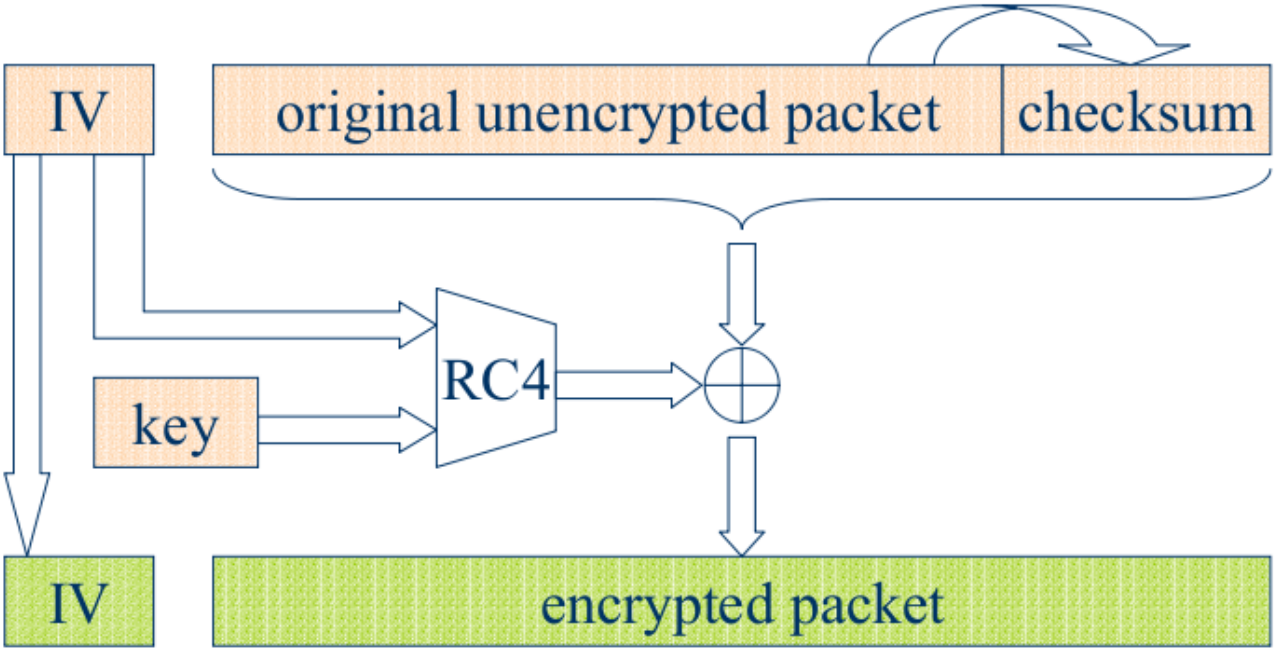
- **BSSID**
  Basic Service Set Identifier, kurz BSSID, ist die eindeutige Bezeichnung eines Access Points in einem WLAN.
- **SSID**
  Service Set Identifier, bezeichnet in Funknetzen (WLANs) nach dem Standard 802.11 den frei wählbaren Namen eines solchen Funknetzes.
- **Beacons**
  Damit WLAN-Adapter einen Access Point - oder einen Adapter im Adhoc- Modus - bemerken, sendet dieser regelmäßig ein *Beacon* (englisch für Leuchtfeuer, Lichtsignal) aus. Das ist ein Funksignal, das den Namen des WLANs (die SSID) und Angaben zur Geschwindigkeit und zur Verschlüsselung enthält.
- **MAC-Adresse**
  Die MAC-Adresse *(Media-Access-Control-Adresse)* ist die Hardware-Adresse jedes einzelnen Netzwerkadapters, die zur eindeutigen Identifizierung des Geräts in einem Rechnernetz dient.
- **WPA-Handshake**
  Wenn ein Client sich zu einem WPA/WPA2 Funknetzwerk verbindet, so findet ein Vier-Wege-Handshake des TKIP-Protokolls statt.
- **ARP**
  Das *Address Resolution Protocol* (ARP) ist ein Netzwerkprotokoll, dass zu einer Netzwerkadresse der Internetschicht die physikalische Adresse (Hardwareadresse) der Netzzugangsschicht ermittelt und diese Zuordnung gegebenenfalls in den so genannten ARP-Tabellen der beteiligten Rechner hinterlegt.

Verschlüsselung

WEP

- **Historie**
  - 1997 Als Standard definiert durch IEEE.
  - 2000 Erste Entdeckungen von Schwachstellen. (Statischer RC4 Schlüssel)
- **Angriffsmöglichkeiten**
  - Es können IVs (Initialisierungsvektoren) gesammelt werden, über die dann (statistisch) die WEP-Passphrase geknackt wird. Eine neuere Methode (PTW) benötigt die kompletten (Daten-) Pakete. Sie ist um einiges schneller (meist zwischen ein und zwei Minuten).
  - Um schneller Pakete zu sammeln kann ein Access-Point (AP) oder ein Client so manipuliert werden, dass sie zusätzliche Pakete senden.

- **Funktionsweise**



Der RC4-Algorithmus wird als Pseudozufallszahlengenerator (PRNG) genutzt. Als „Seed“ dient IV (Initialisierungsvektor, 24Bit) und der WEP Schlüssel. Der vom PRNG erzeugte Bitstrom wird mit dem Datenpaket XOR-verknüpft. Das entstandene, verschlüsselte Paket bekommt noch den IV voran gesetzt und ist nun für den Funkverkehr fertig gestellt.

WPA

- **Historie**
  - 2003 Als Standard definiert durch IEEE.
  - 2004 Wörterbuchangriff auf den WPA-Handshake möglich.
  - 2008 Wörterbuchangriff durch Grafikkarte bis zu 10000% schneller.
  - 2008 Möglichkeit einzelne Pakete (mit großem Aufwand) zu entschlüsseln, teils zu manipulieren und wieder ins Netz einzuschleusen.
- **Angriffsmöglichkeiten**
  - Wörterbuchangriff auf den WPA-Handshake möglich.
  - Einzelne Pakete können entschlüsselt, teils manipuliert und wieder eingeschleust werden.
- **Unterschied zu WEP**
  Basiert auch auf RC4, allerdings mit dynamischen Schlüsseln (Per-Packet-Key-Mixing-Funktion). Als Zutaten dienen der vom Pairwise Master Key abgeleitete Pairwise Transient Key, die MAC-Adresse des Senders und die Seriennummer des Paketes, die mit einer Hash-Funktion zum Schlüssel verarbeitet werden.
  (Weitere Zusatzfunktionen: Re-Keying-Mechanismus und Message Integrity Check)

WPA2

- **Historie**
  - 2004 Als Standard definiert durch IEEE.
- **Angriffsmöglichkeiten**
  - Wörterbuchangriff auf den WPA-Handshake möglich.
- **Unterschied zu WPA**
  Basiert auf der AES Verschlüsslung.
  (Dynamische Schlüssel werden weiterhin verwendet.)

Sonstige Sicherheitsvorkehrungen

Hidden SSID

- **Funktionsweise**
  Der AP wird so konfiguriert, dass dieser keine Beacons mehr sendet. Wenn ein Client dann eine Verbindung zum AP aufnehmen will, so muss er von der Existenz des APs wissen ebenso wie dessen MAC. Mit diesen Daten stellt der Client aktiv eine Verbindung her.
- **Angriffsmöglichkeiten**
  Aus dem Funkverkehr können Pakete analysiert werden. Wenn aus diesen hervorgeht, dass ein Client mit einem AP kommuniziert (Infrastructure), so ist die MAC des APs direkt ablesbar.

MAC-Filter

- **Funktionsweise**
  Der AP hat eine von Hand konfigurierte Black- oder Whitelist, auf der MAC-Adressen stehen die zu Filtern sind.
- **Angriffsmöglichkeiten**
  Aus dem Funkverkehr können Pakete analysiert werden. Wenn aus diesen hervorgeht, dass ein Client mit dem gewünschten AP kommuniziert, so kann die MAC-Adresse des Clienten abgelesen werden. Anschließend manipuliert man die eigene MAC-Adresse (MAC-Spoofing) so, dass sie der des Clienten entspricht.

Rechtliches

- **Aus Betreibersicht**
  Aus einem wegweisenden Urteil des BGH vom 12. Mai. 2010 geht hervor, dass der Betreiber für ein „unzureichend“ (bzw. nicht „marktüblich“) verschlüsseltes Netzwerk haftet.
  Allerdings können diese nicht auf Schadensersatz verklagt werden. Es folgen „nur“ Abmahnungsgebühren (100€).
- **Aus Nutzersicht**
  Das Eindringen in ein verschlüsseltes Funknetzwerk ist nach §202b StGB verboten. Legale Tätigkeiten in offenen Netzwerken sind grenzwertig, da die Daten möglicherweise „[...] nicht für einen bestimmt [...]“ sind (Privates WLAN), aber nicht „[...] gegen unberechtigten Zugang besonders gesichert sind [...]“ (§202a StGB). Außerdem könnte die Benutzung als Abhören einer Funkanlage gewertet werden, was verboten ist nach §89 TKG.

In der Live Demo verwendete Tools

Aircrack-ng

- „Aircack-ng is a set of tools for auditing wireless networks“.
- airmon-ng: Setzt WLAN Karte in „Monitor-Mode“ (Alle Pakete lesen).
- airodump-ng: Speichert den gesamten Funknetzverkehr (da Monitor-Mode).
- aireplay-ng: Erzeugt künstlich Datenverkehr (ARP-replay), um das Sammeln von Paketen zu beschleunigen.
- aircrack-ng: Knackt den WEP WLAN-Schlüssel über die gesammelten Pakete.

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.“
- In der Demo wird ARP-Spoofing verwendet um eine *Man in the Middle Attack* (MITM) auszuführen. Hierbei wird dem Client X vorgemacht, dass man selbst der Router sei. Analog wird der Router manipuliert, sodass er glaubt man selbst sei der Client X.
- Der gesamte Datenverkehr läuft dank MITM nun über einen selbst und kann mittels Filtern analysiert und editiert werden.

Wardriving

Wardriving ist das systematische Suchen nach *Wireless Local Area Networks* (WLAN) mit Hilfe eines Fahrzeugs.

Rechtliches

- Das reine Wardriving sollte nicht illegal sein, da es rein passiv abläuft. Es werden also keine Sicherheitsvorkehrungen gebrochen oder Verbindungen aufgebaut.
- Dennoch wird es rechtlich kritisch gesehen. So wurde ein „Wardriver“, der allerdings eine Verbindung zu einem Netzwerk aufgebaut hatte, vom Wuppertaler Gericht 2007 verurteilt. Es blieb dabei jedoch nur bei einer Verwarnung. Alle weiteren Anklagen gegen Wardriver wurden fallen gelassen.

Kismet

- „Kismet identifies networks by passively collecting packets and detecting standard named networks, detecting (and given time, decloaking) hidden networks, and infering the presence of nonbeaconing networks via data traffic.“
- In diesem Zusammenhang wurde Kismet nur eingesetzt um Funknetzwerke zu finden und mit GPS geografisch einzuordnen.

Python Scripts

Die folgenden drei in Python geschriebenen Scripts wurden selbst entwickelt. Lediglich pykismetkml basiert auf einem bereits vorhandenen Script. Die Funktionen die sie bieten, sind naheliegend (für Wardriving), da sich jedoch in den neusten Versionen von Kismet (Kismet-2010-01-R1) das Format der Logfiles änderte, gab es noch keine Programme oder Scripts die diese Aufgaben erledigten.

pykismetkml.py

Dieses Tool ist dazu da, um eine Kismet Logfile (.netxml - ein XML Format) in KML (ein anderes XML Format) zu konvertieren. Die .kml Dateien können dann von Google Earth gelesen werden.

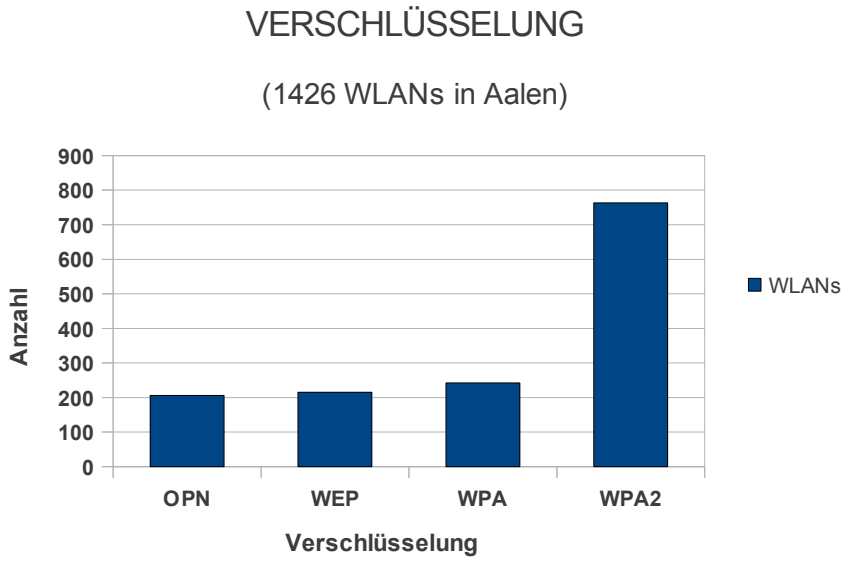
merge-netxml.py

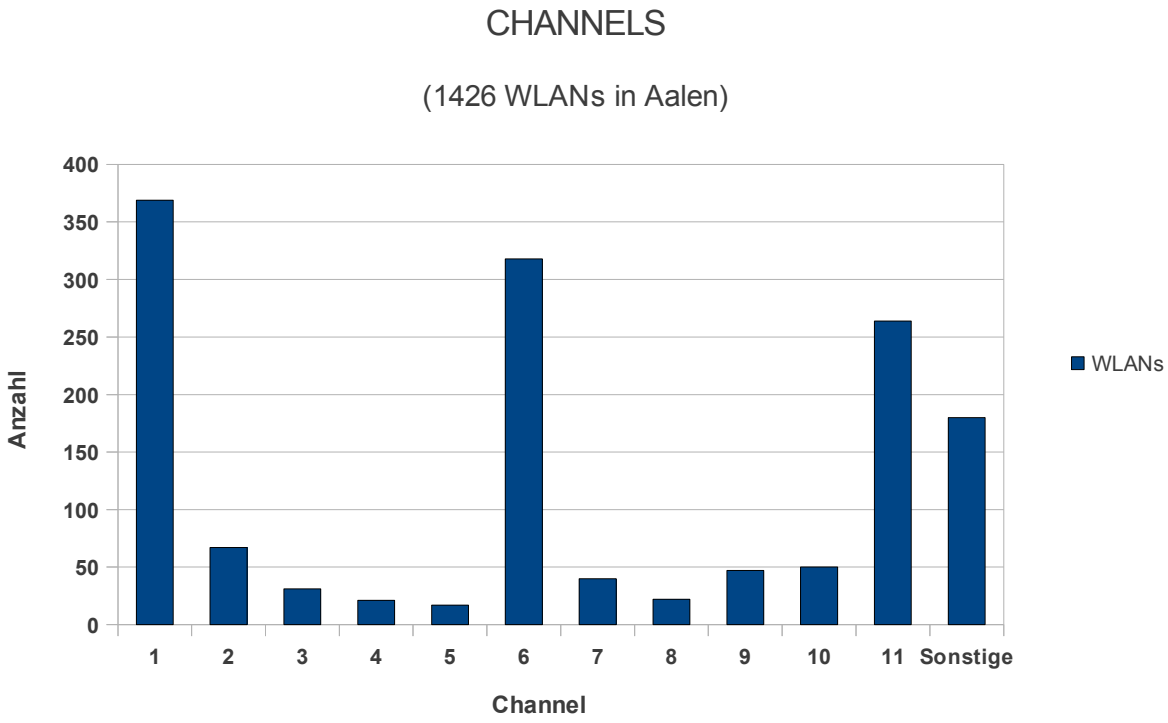
Das Script liest mehrere Kismet Logfiles (.netxml) ein, löscht doppelt vorkommende Netzwerke und schreibt dann alle zu einer Logfile zusammen.

statistic-netxml.py

statistic-netxml.py erstellt eine Statistik aus der eingelesenen Kismet Logfile (.netxml). Hierbei kann es Aussagen treffen über die Verschlüsslung, die Funkkanäle, die Hersteller und die SSID.

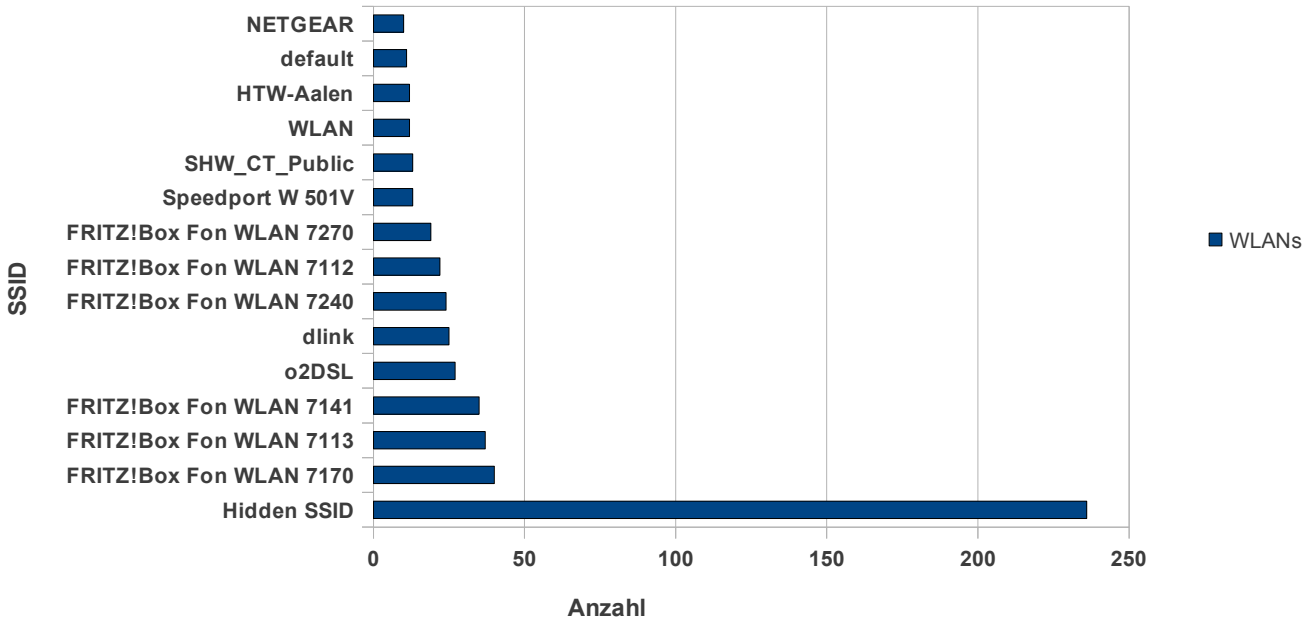
Statistische Ergebnisse





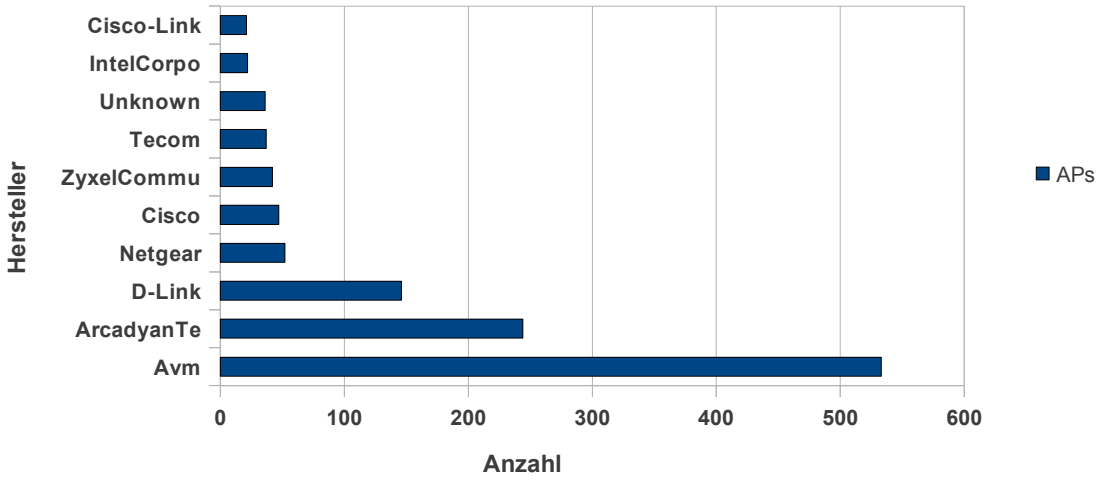
SSID

(Top 15 der 1426 WLANs in Aalen)



HERSTELLER

(Top 10 der 1426 WLANs in Aalen)



Quellen

http://www.heise.de/newsticker/meldung/WPA-angeblich-in-weniger-als-15-Minuten-knackbar-215626.html

http://de.wikipedia.org/wiki/Wi-Fi_Protected_Access

http://de.wikipedia.org/wiki/Wired_Equivalent_Privacy

http://www.fcc.gov/realaudio/presentations/2002/042902/wagner.pdf

http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2010&Sort=3&nr=51934&pos=0&anz=101

http://www.heise.de/newsticker/meldung/BGH-schraenkt-Folgen-der-Stoererhaftung-fuer-WLAN-Betreiber-ein-998591.html

http://de.wikipedia.org/wiki/Wardriving

http://www.kismetwireless.net/

http://ettercap.sourceforge.net/

http://de.wikipedia.org/wiki/Address_Resolution_Protocol

http://de.wikipedia.org/wiki/MAC-Adresse

http://www.pcwelt.de/start/dsl_voip/dsl/praxis/102792/kabelloses_netzwerk_einrichten/index15.html

http://code.google.com/p/pykismetkml/