Eidgenössische Technische Hochschule Zürich
Swiss Federal In

Institut für
Technische Informatik und
Kommunikationsnetze

Markus Frei
Adrian Gämperli

Historische Entwicklung der Sicherheit in Wireless Netzwerken

Gruppenarbeit
März 2011 bis Juli 2011

Tutors: David Gugelmann, Dominik Schatzmann
Supervisor: Prof. Dr. B. Plattner

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Kapitel 1

Einleitung

Die Problematik von unzureichend geschützten Wireless Netzwerken, die es einem Angreifer sehr einfach machen, Daten abzufangen oder das Netzwerk für unautorisierten Internetzugang zu verwenden, hat in den letzten Jahren einiges an Aufmerksamkeit erhalten.
Ziel dieser Arbeit ist es, zu evaluieren, ob die Prominenz dieses Themas auch tatsächlich dazu geführt hat, dass Wireless Netzwerke heutzutage sicherer konfiguriert sind, entweder durch den Hersteller oder den Benutzer, als vor einigen Jahren. Eine sichere Konfiguration in diesem Kontext heisst, dass WPA1 oder idealerweise WPA2 verwendet wird statt WEP oder gar keine Verschlüsselung. Ein zusätzlicher Aspekt, der bei dieser Untersuchung beachtet werden muss, sind unverschlüsselte WLANs, die von kommerziellen Anbietern (z.B. Monzoon oder Swisscom) als Public Wireless Access Points betrieben werden. Diese müssen für die Untersuchung von unverschlüsselten privaten Netzwerken unterschieden werden. Zudem werden Unterschiede zwischen Geschäftsviertel und Wohngegend in Bezug auf die verwendete Verschlüsselung vermutet.

1.1 Motivation

Beide Autoren interessieren sich für Sicherheit in Netzwerken. Es ist interessant zu erforschen, wie weit verbreitet das Wissen ist, wie ein sicheres WLAN zu betreiben ist, oder inwiefern die Hersteller ihre Kunden zwingen, eine sichere Konfiguration zu verwenden.

1.2 Aufgabenstellung

- Suche nach historischen Daten (in der Wardriving Szene).
- Entwicklung von Tools für das Erfassen von WLAN Netzwerken und zur Unterscheidung zwischen unverschlüsselten Netzwerken von kommerziellen Anbietern und privaten Netzwerken. Dabei ist zu beachten, dass keine widerrechtlichen Daten aufgezeichnet oder übermittelt werden.
- Erstellen einiger WLAN Traces und Vergleich mit historischen Daten.
- Verfassen eines Reports, der die geleisteten Arbeiten und Resultate beschreibt.

Kapitel 2

Software

Für die Erhebung der Daten kam eine eigens dafür entwickelte Software zum Einsatz. Diese wurde in Python mit einem objektorientierten Ansatz geschrieben. Das folgende Kapitel ist wie ein Manual gehalten und soll es dem Leser ermöglichen, dieses Tool zu benutzen und gegebenenfalls zu erweitern.

2.1 Aufsetzen

Die Software wurde in Python 2.6 geschrieben und wurde auf Ubuntu 10.10 getestet. Als Hardware wurde ein Lenovo T60 verwendet. Bei der Verwendung von anderer Hardware, im speziellen der WLAN-Karte, ist Vorsicht geboten, da eine gewisse Treiberabhängigkeit beobachtet werden konnte. Es wurde der NL-402u von NAVILOCK als GPS-Empfänger verwendet.

Abbildung 2.1: Eingesetzter Laptop und GPS-Empfänger

Vor der ersten Verwendung der Software sollten die zusätzlich benötigten Pakete installiert und das Betriebssystem konfiguriert werden. Die Software befindet sich mit allen Tools und Daten auf der beiliegenden CD. Vor der ersten Verwendung der Software führt man folgende Befehle im Terminal aus:

```
cd code/script
sudo ./requirements.sh
```

Im Homeverzeichnis muss der Ordner `traces` erstellt werden, da in ihm die Datenbank abgespeichert wird.
Achtung: Dieses Skript löscht unter anderem das Paket network-manager. Somit sollte dies nicht auf einem produktiv eingesetzten Rechner ausgeführt werden.

2.2 Daten sammeln

Der Datenbankpfad kann im Ordner `code/lib` in der Datei `WlanTester.py` mit der Variable `dbFile` geändert werden.
Es muss nicht für jeden Trace ein neuer Pfad eingetragen werden, sondern es ist möglich, mehrere Traces in einer Datei abzuspeichern. Zum Testen empfiehlt sich möglicherweise ein von der Zeit abhängiger Dateiname.
Achtung: Vor dem Starten sollten unbedingt die IP-Adressen (IPv4 und IPv6) in `ConnectivityTesting.py` überprüft werden.
Bevor die Software gestartet wird, sollte der GPS-Empfänger angeschlossen werden und der Lautsprecher nicht auf stumm geschaltet werden, da die Software akustische Hinweise an den Benutzer gibt. Nun kann die Software gestartet werden und der Trace beginnen.

```
cd code/lib
sudo python2.6 WlanTester.py
```

Hinweis: Das Skript benötigt root-Rechte, da unter anderem iwlist sonst keinen aktuellen Scan auslösen kann.
Beim Sammeln der Daten ist darauf zu achten, dass zu Beginn der GPS-Empfang hergestellt werden kann. Bis dies geschehen ist, kann nicht gescannt werden. Da zu jedem nicht verschlüsselten Access Point eine Verbindung hergestellt werden muss, gibt die Software das akustische Signal "wait testing", um dem Nutzer mitzuteilen, dass er stehenbleiben soll. Falls eine Landingpage vorhanden ist, warnt die Software mit dem akkustischen Signal "Firefox". Der Nutzer muss nun die Landingpage im Firefox behandeln und diesen wieder schliessen. Um den Trace zu beenden, muss Ctrl-c gedrückt werden (eventuell mehrmals). Die Software sollte während dem Scanvorgang beendet werden, da es sonst unter gewissen Umständen zu einer Verfälschung einiger Daten führen könnte. Die Daten sind in der Datenbank im Ordner `traces` im Homeverzeichnis abgespeichert.
Unter gewissen Umständen ist es nötig, die Software zu killen. Dies kann bei GPS-Problemen nötig werden, im Speziellen, wenn kein GPS-Empfänger angeschlossen ist oder kein Empfang besteht.

```
sudo killall python2.6
sudo killall gpsd
```

Wenn kein Scannen möglich ist, sollte Folgendes ausgeführt werden:

```
sudo ifconfig <interface> down
sudo ifconfig <interface> up
```

Daten importieren

Das Datenset (Jahr) wird über den Dateinamen bestimmt. Es werden nur Daten importiert, bei denen das Format auch WPA Netzwerke unterstützt. Beim Import der historischen Daten wurden Annahmen getroffen (siehe 3.2). Da diese Annahmen nicht zwingend zutreffen müssen, ist bei diesem Tool etwas Vorsicht geboten. Zudem unterscheiden die historischen Daten nicht zwischen WPA1 und WPA2. Die Höhe über Meer ist bei den Access Points fehlerhaft (siehe auch 3.2).

```
cd code/lib
python2.6 kismet.py
```

Die historischen Rohdaten befinden sich in `data/import`.

2.3 Daten auswerten

Die finale Datenbank `final.db` ist im Ordner `data` zu finden. Mit folgenden Schritten kann man die Auswertung erstellen:

```
cd analysis
python2.6 generate.py
python2.6 analyzeMaxDistance.py
```

Im Ordner `data` befindet sich auch die Datenbank `raw-fs11.db`, welche nur die Daten aus dem Frühjahrssemester 2011 enthält.
Hinweis: Beim Auswertungscode wird mehrmals davon ausgegangen, dass die Bitmasken (siehe 2.5) den vordefinierten Werten entsprechen! Die Auswertung der Daten wurde in Ubuntu 11.04 erstellt.

Dataviewer

Es wurde zusätzlich ein kleines Programm mit einem GUI geschrieben, welches einige Eigenschaften der WLANs auflistet. Man kann auch die Access Points auf der Karte anzeigen lassen mit verschiedenen Symbolen für die schwächste Verschlüsselung des Access Points. Ausserdem lässt sich auch die Route eines Traces auf der Karte einzeichnen.

```
cd dataviewer
python2.6 dataviewer.py
```

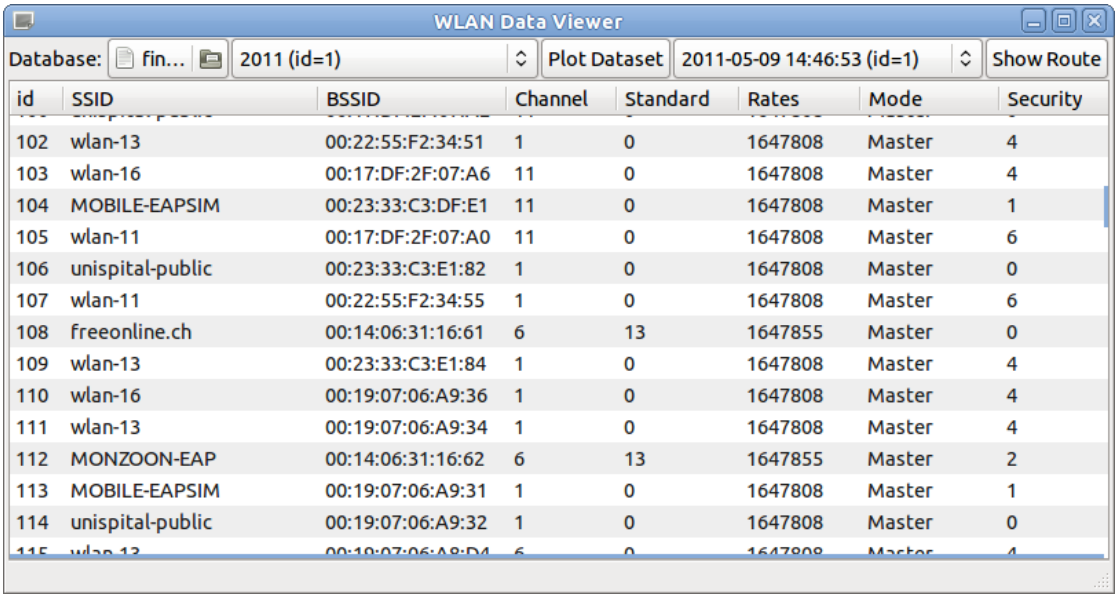

Abbildung 2.2: Screenshot des Dataviewers

2.4 Programmstruktur

Die Dateien sind im Ordner `code/lib` zu finden.

2.4.1 WlanTester.py

In dieser Datei wird das Scaninterface in der Variable `networkInterface` geändert. Dieses muss gegebenenfalls geändert werden, um mit dem gewünschten Device zu scannen. Die Datenbankparameter werden in den Variabeln `dbOptions` und `dbFile` geändert.
Der Ablauf kann in Pseudocode wie folgt beschrieben werden:

```
Initialisierung
while True:
  Scannen
  GPS-Koordinaten setzen
  unverschlüsselte WLANs testen und
    alle WLANs in die Datenbank schreiben
```

Das Scannen wird von `WlanScanner.py` übernommen. Die GPS-Koordinaten werden von `GPSPosition.py` gelesen und die unverschlüsselten WLANs werden von `ConnectivityTesting.py` getestet. Zudem werden alle Access Points in dieser Datei in die Datenbank geschrieben. Zwei WLANs sind dann unterschiedlich, wenn das Tupel bestehend aus BSSID und ESSID unterschiedlich ist.

2.4.2 WlanScanner.py

Um nach verfügbaren Access Points zu scannen, wird das in Linux integrierte Tool iwlist verwendet.

```
sudo iwlist <interface> scan
```

Dieser Output wird mit `wrappers/iwlist.py` geparsed, damit alle relevanten Informationen in einem Dictionary vorliegen. Nun wird für jeden Access Point eine Net-Instanz erstellt (definiert in `wlan.py`). Somit übergibt die Funktion `getWlanList()` eine Liste von Net-Instanzen.

2.4.3 GPSPosition.py

Die Positionsdaten werden mit Hilfe des Pakets gpsd gesucht.

```
GPSdaemon = gpsd(mode=WATCH_ENABLE|WATCH_NEWSTYLE)
report = GPSdaemon.next()
```

Damit wird das GPS initialisiert und mit `next()` wird der nächste GPS Report zurückgegeben. Diese Funktion ist blockierend.
Der obige Teil läuft in einem eigenen Thread. Es wird also permanent nach neuen GPS-Reports gesucht. Die Funktion `getCurrentPosition()` gibt die letzte Position in einer Position-Instanz zurück. Mit der Funktion `getWayPoints()` liest man die Wegpunkte als Liste von Position-Instanzen aus.
Um das Skript auch ohne GPS-Empfang zu testen, empfiehlt sich gpsfake. Zudem muss die Variable `maxGPSDelay` in der Datei `WlanTester.py` erhöht werden.

2.4.4 ConnectivityTesting.py

Die Funktion `testWlanList(wlanList)` hat als Eingabeparameter eine Liste von Net-Instanzen mit den GPS-Koordinaten. Zu jedem nicht verschlüsselten WLAN wird mit der Funktion `connectTo(wlan, timeout)` eine Verbindung aufgebaut. Anschliessend wird mit der Funktion `test(wlan, timeoutPerTest)` überprüft, ob DNS und HTTP über IPv4 (im Folgenden HTTP4) sowie IPv6 (im Folgenden HTTP6) funktioniert. Für den Fall, dass eine Landingpage existiert, wird der Firefox geöffnet und die Landingpage muss vom Nutzer behandelt werden. Die Software warnt in diesem Fall mit der Sprachausgabe "Firefox". Anschliessend muss Firefox wieder geschlossen werden. Nun werden die DNS- und HTTP-Tests erneut durchgeführt. Schlussendlich werden alle WLANs in die Datenbank geschrieben.
Als Testergebnis wird zwischen PASS, SOFTFAIL und HARDFAIL unterschieden. SOFTFAIL ist beispielsweise, wenn man eine HTTP Antwort bekommt, diese aber nicht die erwartete ist (z.B. bei einer Landingpage). Ein HARDFAIL liegt vor, wenn eine Exception geworfen wird, beispielsweise, wenn IPv6 nicht eingerichtet ist.
In Pseudocode geschrieben sieht dieser Ablauf folgendermassen aus:

```
def testWlanList(self, wlanList):
  for wlan in wlanList:
    if wlan.isOpen():
```

```
    connectTo(wlan)
    test(wlan)
  wlan in Datenbank schreiben
```

2.4.5 db.py

Diese Datei enthält die Funktionen für alle Datenbankabfragen.

2.5 Datenbank

Der SQL-Befehl für die Erstellung der Datenbank befindet sich in `code/db/structure.sql`.

bitmasks

In dieser Tabelle werden alle Bitmasken der ganzen Datenbank gespeichert. Die Bitmasken werden dabei immer mit dem Spaltennamen zusammen gespeichert. Bitmasken werden für Folgendes verwendet:

- Access Point Standards
- Access Point Bitraten
- Access Point Sicherheitsstandards
- Verbindungstestsresultate

routes

In dieser Tabelle werden Wegpunkte des Traces gespeichert.

zones

Jeder Trace kann einer Zone zugeordnet werden. Eine Zone besteht aus der Stadt und einer Gebietsbezeichnung. Importe werden der Zone "other" zugeordnet.

datasets

Ein Dataset ist eine Ansammlung von Traces. Beispielsweise alle Access Points von 2003.

connectivitytests

In dieser Tabelle werden die Verbindungstestergebnisse gespeichert.

condetails

In condetails werden zusätzliche Informationen, zum Beispiel Fehlermeldungen, der connectivitytests gespeichert.

traces

Ein Trace fasst die Daten vom Programmstart bis zum Abbruch des Scanvorgangs zusammen.

signalposition

Diese Tabelle speichert Informationen (GPS, Zeit, Signaleigenschaften) zu den Access Points (wlans).

wlans

In dieser Tabelle werden alle Access Points gespeichert.

Kapitel 3

Resultate

Bei der Auswertung unterscheidet sich ein Access Point von einem anderen, wenn die BSSID unterschiedlich ist.
Mit *voll offen* werden im folgenden Access Points bezeichnet, die einerseits keine Verschlüsselung aktiviert haben und andererseits ein direkter Internetzugriff möglich (HTTP4 erfolgreich) ist ohne Landingpage oder sonstige Interaktion.
Offene Access Points sind Access Points, die keine Verschlüsselung aktiviert haben, also sowohl öffentliche Hotspots als auch voll offene Access Points.

3.1 Vorverarbeitung der Messdaten

Es wird vermutet, dass sich durch nicht n-Standard kompatible Hardware einige Fehler in die Resultate eingeschlichen haben, deshalb werden alle bei der Auswertung als a-Standard erkannten Netzwerke aus der Auswertung ausgeschlossen. Es wurden dabei 348 Einträge gelöscht. Zudem wurde festgestellt, dass die Scans nicht komplett sein müssen, weshalb einige WLANs fälschlicherweise als WEP anstelle von WPA erkannt wurden (siehe 4.2). Dadurch mussten 18 WLANs gelöscht werden. Insgesamt wurden durch diese beiden Löschvorgänge 365 WLANs gelöscht (eine Überschneidung). Ausserdem wurden 111 WLANs gelöscht, die unerklärliche iwlist-Outputs hatten.

```
sqlite> delete from wlans where wlan_standard = 2;
sqlite> delete from wlans where wlan_raw not like '%Extra:%';
sqlite> delete from wlans where wlan_raw like '%Cell %Cell %' or
  wlan_raw like '%ESSID:%ESSID:%' or wlan_raw like '%Unknown/bug%';
```

Ausserdem mussten aufgrund einer falschen Variable die IPv6 HTTP-Tests für ungültig erklärt werden.

3.2 Historische Daten

Es wurden historische Daten von Zürich und Basel gefunden. Herr Christoph Weber von wardriving.ch hat freundlichweise die Daten von Zürich zur Verfügung gestellt. Die Daten von Basel, welche leider aus zeitlichen Gründen nicht analysiert werden konnten, stammen von Herrn Markus Forrer von der Webseite wardriving.agssucks.com.
Beim Import der Zürcher Daten (neueres Kismet Format) wurden bei der Verschlüsselung folgende Annahmen getroffen:

- Kommt in der Verschlüsselungszeichenkette "WPA" vor, dann wird der Access Point als WPA1 erkannt.
- Kommt "WEP" vor, wird der Access Point als WEP erkannt.
- Trifft beides nicht zu, wird dem Access Point keine Verschlüsselung zugeordnet.

Da auch Daten in einem älteren Format vorlagen, diese jedoch bereits vom Format her kein WPA anzeigen konnten, wurde auf den Import dieser Daten verzichtet. Auch 2006 wurden noch Daten in diesem Format aufgezeichnet. Zudem sind bei den importierten Access Points die Höhenangaben fehlerhaft. In der Wohngegend im Jahr 2006 gibt es Access Points auf einer Höhe von über 1000 Metern, was nicht stimmen kann. Da aber die horizontalen Koordinaten zu stimmen scheinen (die Access Points liegen genau auf den Strassen), wurden diese nicht gelöscht.

3.3 Gebiete

Die Daten wurden in zwei verschiedenen Gebieten gesammelt. Zum einen im Geschäftviertel von Zürich und zum anderen in einer Wohngegend. Die untenstehenden Grafiken stellen jeweils die schwächste Verschlüsselung dar. Für das Wohngebiet wurden zusätzlich noch Daten aus dem Jahr 2006 ausgewertet.

★	Keine Verschlüsselung
★	WEP
★	WPA1
★	WPA2

Tabelle 3.1: Legende zu den Karten

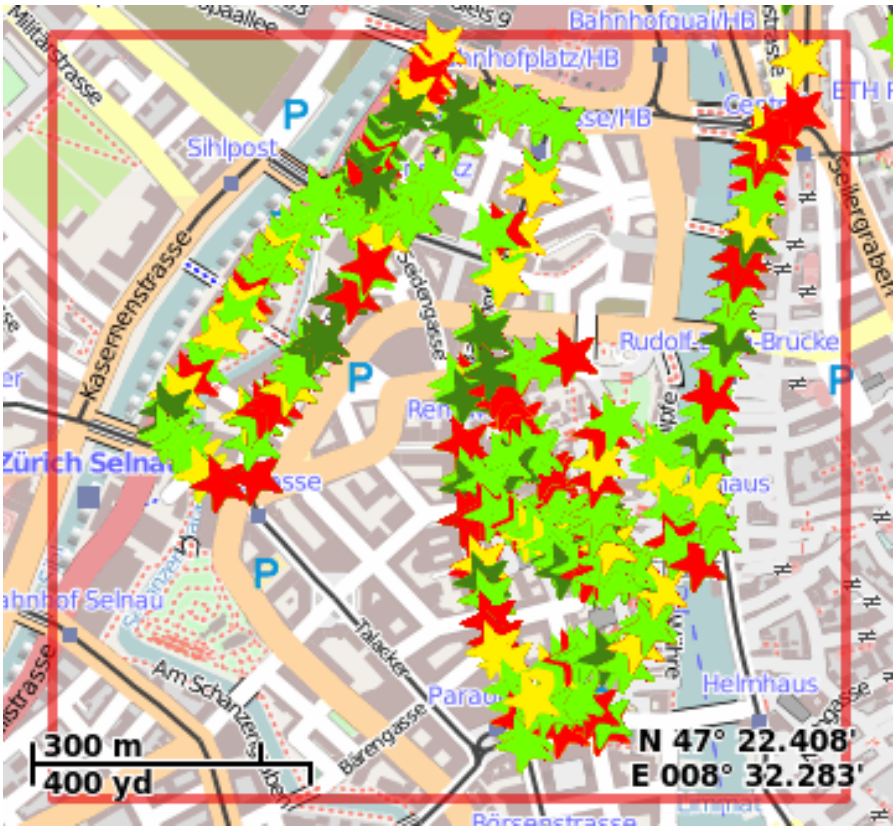

Abbildung 3.1: Karte schwächste Verschlüsselung Geschäftsviertel 2011; Breitengrad 47.3689-47.3779 Längengrad 8.5312-8.5449; basiert auf OpenStreetMap [1] [2]

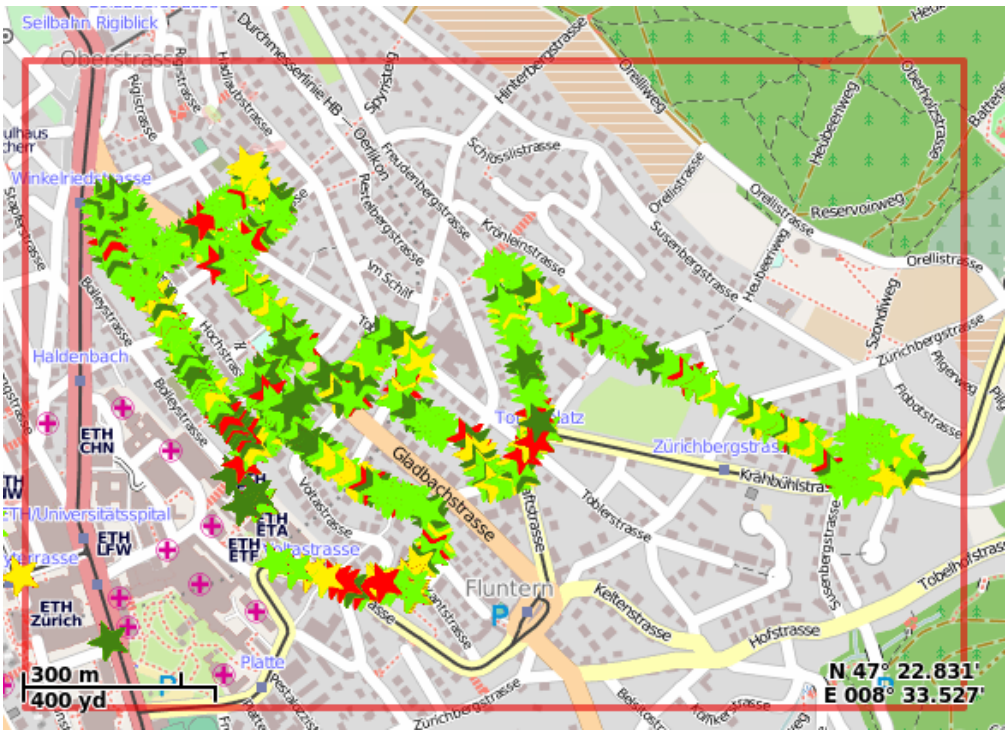

Abbildung 3.2: Karte schwächste Verschlüsselung Wohngegend 2011; Breitengrad 47.3747-47.3857 Längengrad 8.5468-8.5703; basiert auf OpenStreetMap [1] [2]

Abbildung 3.3: Karte schwächste Verschlüsselung Wohngegend 2006; Breitengrad 47.3747-47.3857 Längengrad 8.5468-8.5703; basiert auf OpenStreetMap [1] [2]

In der Wohngegend wurden im Jahr 2011 1478 Access Points gefunden. Im Geschäftsviertel sind es im Jahr 2011 1815 Access Points und in der Wohngegend im Jahr 2006 597 Access

Points.

3.4 Analyse der GPS-Koordinaten

Es ist möglich, dass zu einer BSSID mehrere GPS-Koordinaten gemessen wurden. In der Grafik 3.4 wird der maximale Abstand der Fundorte einer BSSID aus dem Jahr 2011 aufgezeigt. Erwartungsgemäss ist eine Art exponentieller Abfall zu beobachten. Die Grafik 3.5 zeigt nur die Access Points von Monzoon. Diese überschreiten die theoretisch mögliche Distanz von einigen hundert Metern Reichweite zum Teil deutlich. Bei den meisten dieser Access Points liess sich die OUI keinem Hersteller zuordnen. Es wird daher vermutet, dass die Access Points von Monzoon nicht alle verschiedene BSSIDs besitzen. Da dieser Effekt quantitativ eher gering ist, wird trotzdem angenommen, dass jeder Access Point eine andere BSSID besitzt.

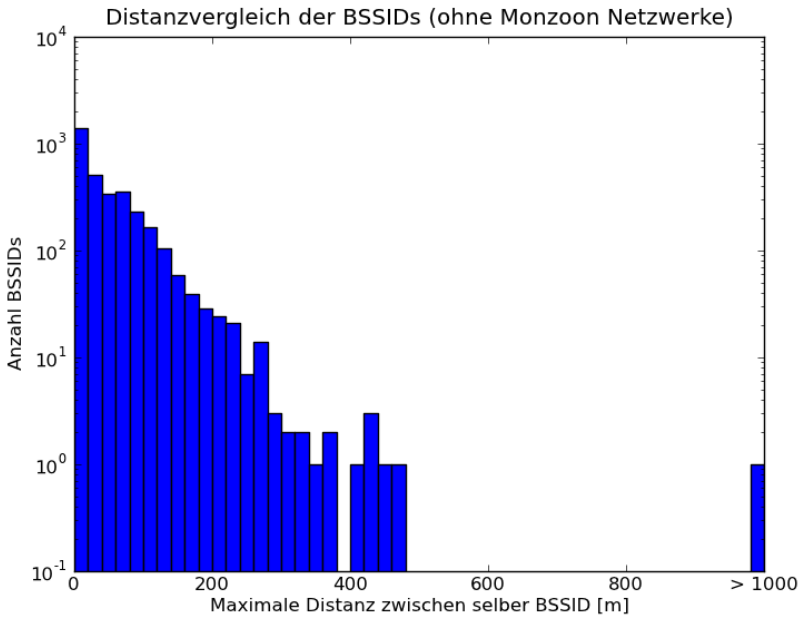

Abbildung 3.4: Vergleich der maximalen Distanz zwischen zwei Fundorten einer BSSID aus dem Jahr 2011; Access Points mit ESSID "MONZOON-EAP", "freeonline.ch" und "MONZOON" ausgeschlossen

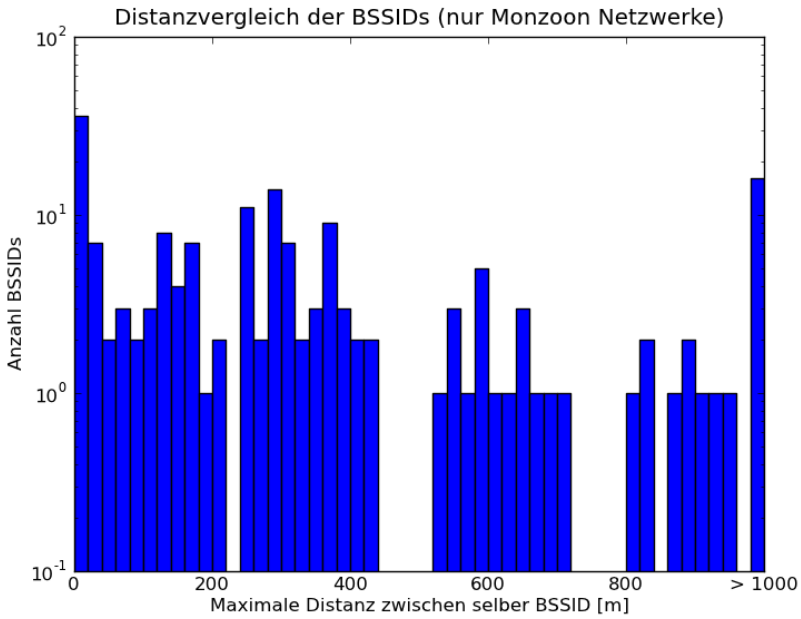

Abbildung 3.5: Vergleich der maximalen Distanz zwischen zwei Fundorten einer BSSID aus dem Jahr 2011; nur Access Points mit ESSID "MONZOON-EAP", "freeonline.ch" oder "MONZOON"

3.5 Übersicht

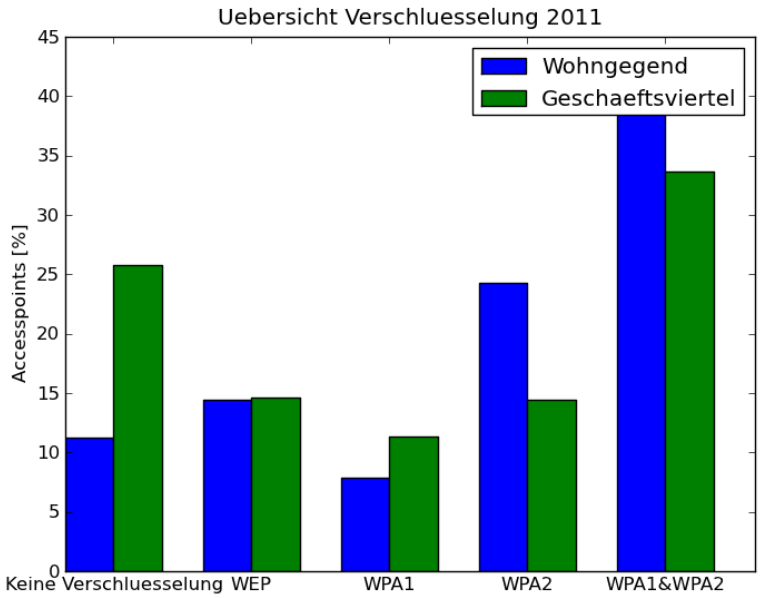

Abbildung 3.6: Vergleich der Verschlüsselung der Gebiete

In dieser Grafik werden die verschiedenen Verschlüsselungen der beiden Gebiete im Jahr 2011 miteinander verglichen. Sofort sticht hervor, dass im Geschäftsviertel jeder vierte Access Point unverschlüsselt ist, während in der Wohngegend fast nur jeder zehnte Access Point unver-

schlüsselt ist. Es wird vermutet, dass viele dieser Access Points beabsichtigte Hotspots sind, die auf einen Zugang per Landingpage setzen. Somit sind diese Netze zwar unverschlüsselt, aber nicht zwangsläufig voll offen.
In beiden Gebieten sind praktisch gleich viele Access Points mit WEP verschlüsselt. Absolut sind dies 479 Access Points, wobei 182 Access Points zu Swisscom (ESSID: "MOBILE-EAPSIM") gehören. Es wurde von Swisscom bestätigt, dass es sich hierbei wirklich um eine WEP-Verschlüsselung handelt.
Etwa 24% aller Access Points in der Wohngegend sind mit WPA2 verschlüsselt. Im Geschäftsviertel sind dies ungefähr 14%.

3.6 Schwächste Verschlüsselung

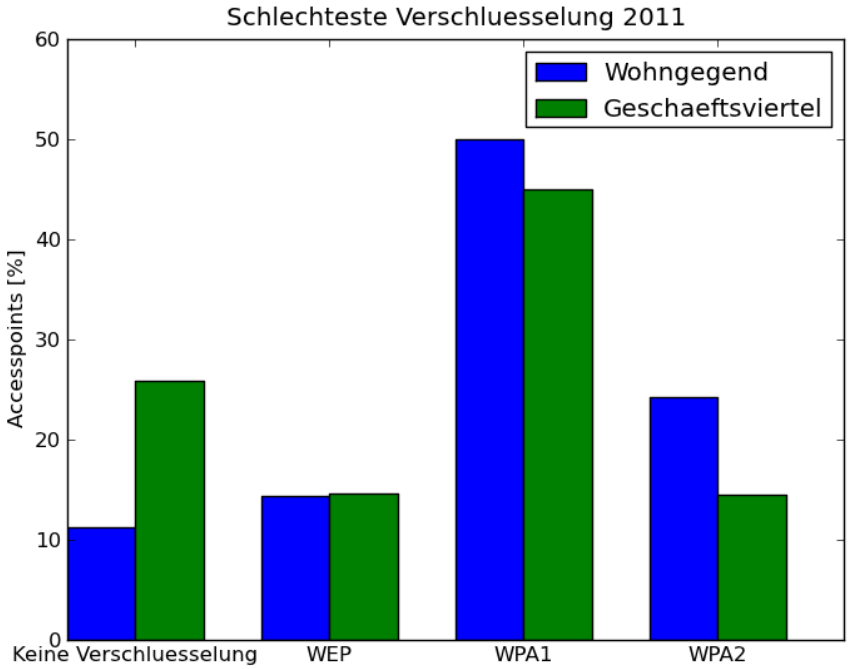

Abbildung 3.7: Vergleich der schwächsten Verschlüsselung der Gebiete

In der obigen Grafik sind die Access Points in vier Kategorien unterteilt worden: keine Verschlüsselung, WEP, WPA1 und WPA2. Diejenigen Access Points, welche WPA1 und WPA2 unterstützen, wurden nun zur Kategorie mit WPA1 gezählt.
Heutzutage sind ca. 26% der Access Points in der Wohngegend und ca. 40% der Access Points im Geschäftsviertel nicht oder nur unzureichend verschlüsselt. Wobei durch die Landingpages im Geschäftsviertel nicht jeder unverschlüsselte Access Point auch automatisch voll offen ist. Umgekehrt sind also ca. 74% der Access Points in der Wohngegend und ca. 60% der Access Points im Geschäftsviertel hinreichend verschlüsselt. Als unzureichend verschlüsselt wird keine Verschlüsselung und WEP gezählt.

3.7 Historischer Vergleich

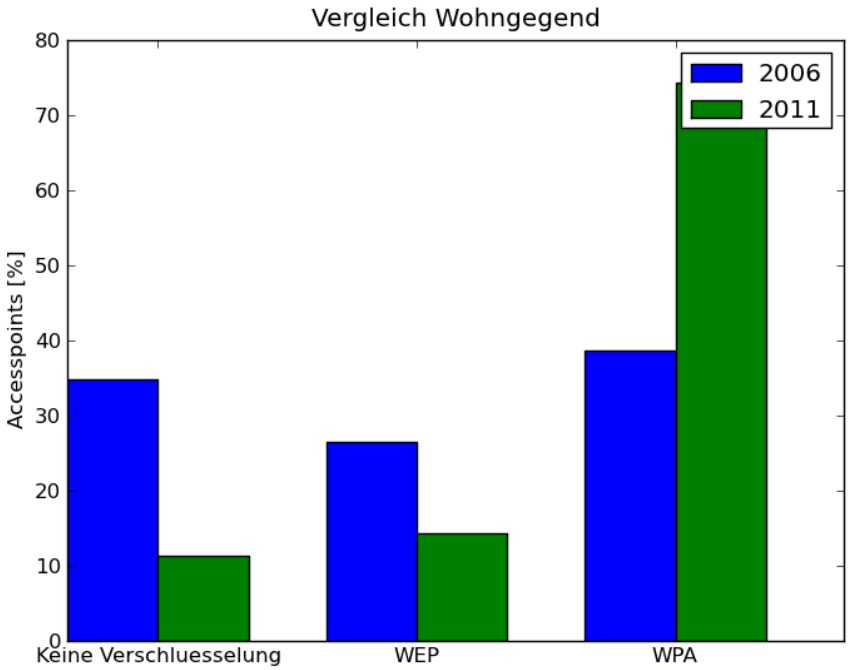

Abbildung 3.8: Vergleich der Verschlüsselung der Wohngegend

Aufgrund fehlender historischer Daten im Geschäftsviertel wird nur die Veränderung in der Wohngegend betrachtet. Die historischen Daten lassen nur die Unterscheidungen keine Verschlüsselung, WEP und WPA zu. Deshalb wurden bei den Daten die Kategorien WPA1 und WPA2 zu WPA zusammengefasst.
Im Jahr 2006 war ein Drittel der Access Points unverschlüsselt. Dies hat sich in den letzten fünf Jahren erheblich verbessert, da nun nur noch jeder zehnte Access Point unverschlüsselt ist.
Der Anteil an WEP verschlüsselten Access Points hat sich in den letzten fünf Jahren fast halbiert und liegt heute bei knapp 14%.
Erfreulicherweise hat sich der Anteil der mit WPA verschlüsselten Access Points innerhalb der letzten fünf Jahre annähernd verdoppelt und liegt heute bei ca. 74%.
Im Jahre 2006 waren ca. 61% der Access Points nicht oder nur unzureichend verschlüsselt. Dieser Anteil ist heute mit ca. 26% erheblich kleiner.

3.8 Veränderung einzelner Access Points

Insgesamt wurden 63 Access Points mit derselben BSSID in mehreren Jahren gefunden. Da bei den Access Points mit den ESSIDs "eth" und "MOBILE" von Mess- oder Importfehlern ausgegangen wird, werden sie nicht weiter beachtet. Nun bleiben noch 55 Access Points. Bei 20 von diesen hat sich die Verschlüsselung verändert, bei 35 ist die Verschlüsselung gleich geblieben. Im folgenden werden einige interessante Fälle genauer betrachtet. In den historischen Daten lässt sich WPA1 und WPA2 nicht voneinander unterscheiden. Somit wurden WPA1 und WPA2 zur Kategorie WPA zusammengefasst. 19 Access Points, bei denen sich die Verschlüsselung verändert hat, wurden nur zweimal gefunden. Ein Access Point wurde mehr als zweimal gefunden. Dieser eine Fall wird gesondert betrachtet.
Bei 10 von diesen Access Points hat sich die Verschlüsselung verbessert. Bei 8 von diesen Access Points wird heute WPA verwendet, bei den zwei anderen WEP.

Bei 9 Access Points hat sich die Verschlüsselung verschlechtert. Bei einigen erscheint dies plausibel, da auch die ESSID geändert hat. Doch bei den Restlichen entspricht dies nicht den Erwartungen und könnte von fehlerhaften oder falsch interpretierten historischen Daten stammen.
Der untenstehende Access Point ist ein Beispiel für die WLANs, bei denen sich die Verschlüsselung verbessert hat.

```
2011: ESSID = wohnraum; WEP
2006: ESSID = gesund & glcklich; WPA
```

Folgender Access Point steht stellvertretend für 9 Access Points, deren Verschlüsselung sich verschlechtert hat.

```
2011: ESSID = rotblau; WPA
2006: ESSID = WLAN02; WEP
```

Der folgende Access Point ist der einzige, welcher mehr als zweimal gefunden wurde. Mit Hilfe dieses Datensatzes lassen sich einige Vermutungen anstellen. Im Jahr 2006 war der Access Point mit WPA verschlüsselt. Im darauffolgenden Jahr einmal mit WPA und einmal mit WEP. Zudem lässt sich eine Namensänderung auf "linksys" feststellen, was ein Standardname eines Herstellers ist. Im Jahr 2011 ist wieder eine Namensänderung zu sehen, doch diesmal hat die Verschlüsselung nicht geändert. Es könnte sein, dass die historischen Daten zu wenig genau sind oder sich Fehler durch iwlist eingeschlichen haben. Der Wechsel von WPA zu WEP ist speziell, da die Zeitstempel ergeben, dass der Wechsel innerhalb von wenigen Minuten zwischen dem ersten Scan und dem zweiten Scan im Jahr 2007 hätte passieren müssen.

```
2011: ESSID = AP4; WEP
2007: ESSID = linksys; WEP
2007: ESSID = linksys; WPA
2006: ESSID = LTH; WPA
```

3.9 Organizationally Unique Identifier

Die ersten 24 Bit einer BSSID (und MAC Adresse) entsprechen der OUI (Organizationally Unique Identifier). Somit lässt sich aus der BSSID der Hersteller der Netzwerkkarte ermitteln. Es werden jeweils die zehn häufigsten OUIs für das Geschäftsviertel und die Wohngegend vom Jahr 2011 sowie für die Wohngegend vom Jahr 2006 aufgelistet. Die dazugehörigen Firmen liessen sich mit Hilfe der Registrierungsdatenbank finden [3].

#AP	OUI	Unternehmen
110	00:03:52	Colubris Networks
66	00:A0:C5	ZYXEL COMMUNICATION
59	00:0F:CC	Netopia, Inc.
29	00:00:C5	FARALLON COMPUTING/NETOPIA
28	00:11:24	Apple Computer
26	00:09:5B	Netgear, Inc.
19	00:01:E3	Siemens AG
18	00:0F:B5	NETGEAR Inc
16	00:13:49	ZyXEL Communications Corporation
14	00:13:46	D-Link Corporation

Tabelle 3.2: Zehn meist verbreitete OUIs Wohngegend 2006

#AP	OUI	Unternehmen
81	00:24:6C	ARUBA NETWORKS, INC.
78	00:26:99	Cisco Systems
70	00:0F:CC	Netopia, Inc.
68	00:24:37	Motorola - BSG
59	00:14:06	Go Networks
51	02:0C:42	*nicht registriert*
39	40:4A:03	ZyXEL Communications Corporation
38	00:24:C8	Broadband Solutions Group
38	00:24:C9	Broadband Solutions Group
34	00:03:52	Colubris Networks

Tabelle 3.3: Zehn meist verbreitete OUIs Geschäftsviertel 2011

#AP	OUI	Unternehmen
121	00:03:52	Colubris Networks
104	00:0F:61	Hewlett-Packard Company
71	00:0F:CC	Netopia, Inc.
69	00:19:A9	Cisco Systems
45	00:24:37	Motorola - BSG
44	00:24:C9	Broadband Solutions Group
42	00:02:CF	ZyGate Communications, Inc.
42	00:23:33	Cisco Systems
36	00:24:6C	ARUBA NETWORKS, INC.
35	00:22:55	Cisco Systems

Tabelle 3.4: Zehn meist verbreitete OUIs Wohngegend 2011

Verschlüsselung pro OUI

Im folgenden Kapitel wird die Verschlüsselung einiger OUIs genauer betrachtet. Es wird eine Auswahl getroffen und diese näher beschrieben.

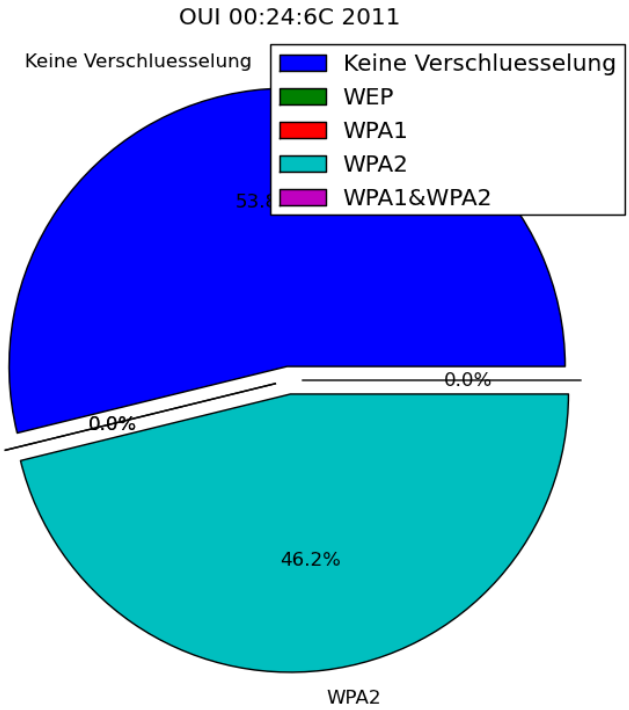

Abbildung 3.9: Verschlüsselung der OUI 00:24:6C (ARUBA NETWORKS, INC.) im Jahr 2011

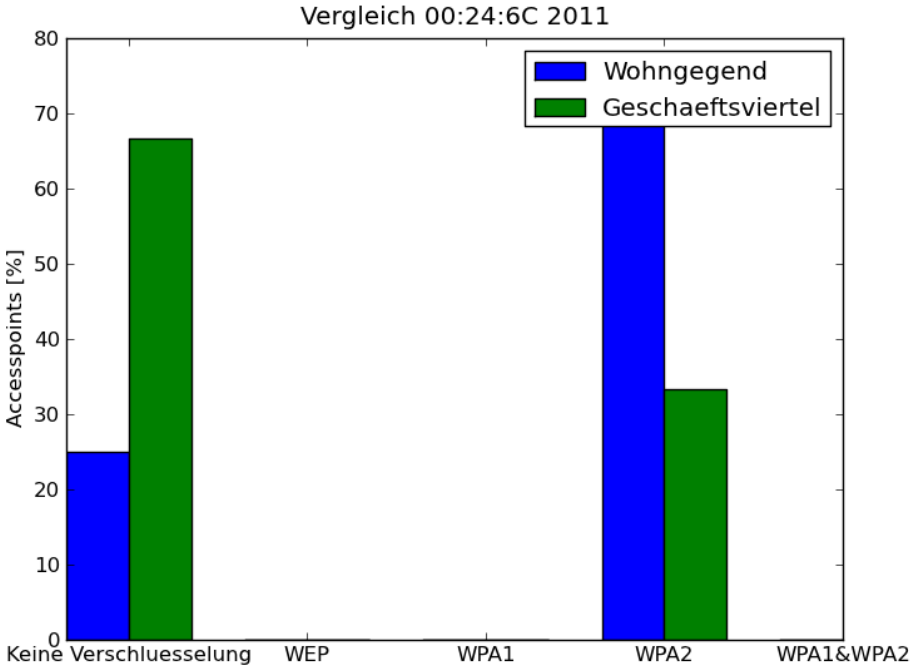

Abbildung 3.10: Verschlüsselung der OUI 00:24:6C (ARUBA NETWORKS, INC.) im Jahr 2011 im Vergleich von Wohn- und Geschäftsviertel

Diese OUI wurde im Geschäftsviertel 81 Mal und in der Wohngegend im Jahr 2011 36 Mal ge-

funden. Es ist sehr auffällig, dass nur WPA2 und keine Verschlüsselung vorkommt. Dies kommt daher, dass die meisten Access Points im Geschäftsviertel von der UBS betrieben werden. Dies erkennt man an den ESSIDs "UBS Employee" (WPA2), "UBS Guest" (keine Verschlüsselung) und "UBS VPN" (keine Verschlüsselung).
Es wird vermutet, dass es in der Wohngegend ein Unternehmen gibt, welches Access Points mit dieser OUI verwendet. Denn auch in der Wohngegend wurden Netze mit mehreren Access Points gefunden. Die Netze heissen "guest", "mitarbeiter", "rtls" und "voice".

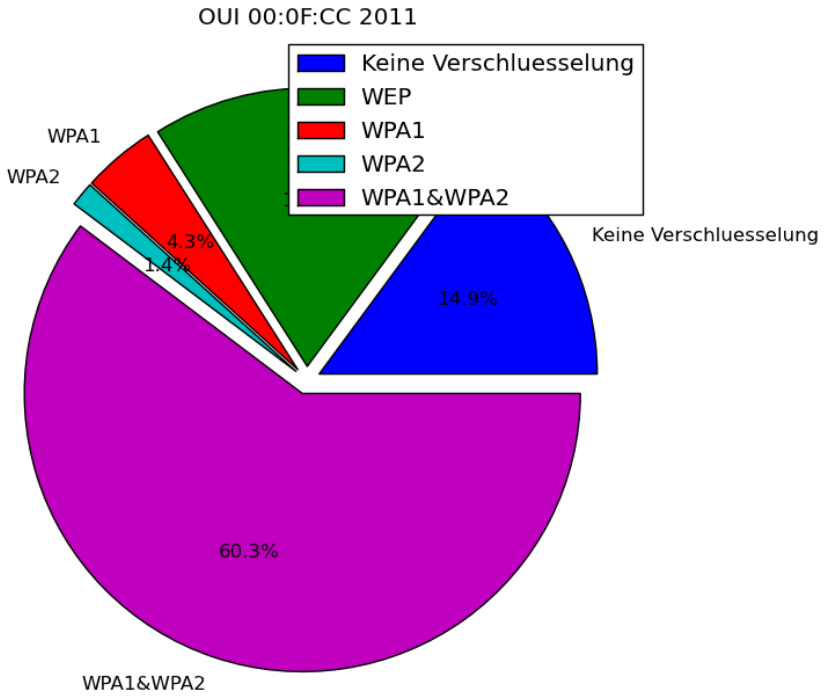

Abbildung 3.11: Verschlüsselung der OUI 00:0F:CC (Netopia, Inc.) im Jahr 2011

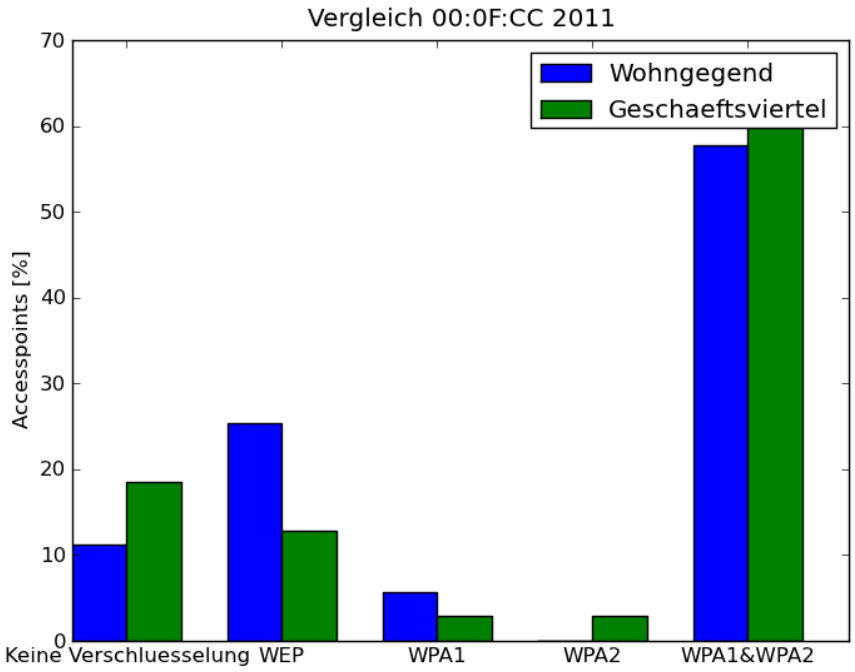

Abbildung 3.12: Verschlüsselung der OUI 00:0F:CC (Netopia, Inc.) im Jahr 2011 im Vergleich von Wohn- und Geschäftsviertel

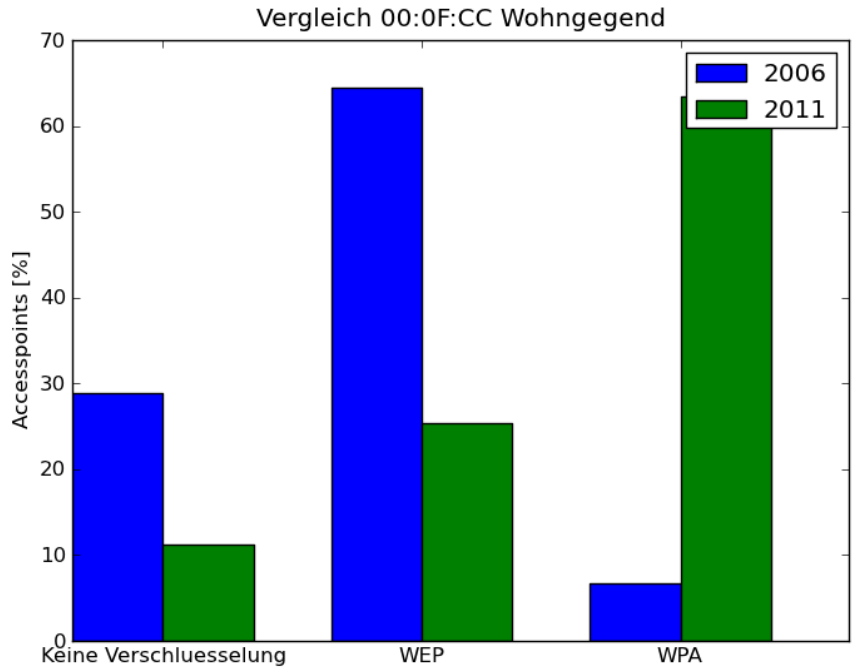

Abbildung 3.13: Verschlüsselung der OUI 00:0F:CC (Netopia, Inc.) im Vergleich der Jahre 2006 und 2011

Diese OUI kann dem Unternehmen Netopia, Inc. zugeordnet werden. Diese OUI ist in beiden

Gebieten und auch im Jahr 2006 die Dritthäufigste. Wenn man die ESSIDs betrachtet, fällt auf, dass annähernd jede BSSID eine andere ESSID besitzt. Somit kann davon ausgegangen werden, dass es sich eher um private oder von kleinen Firmen genutzte Access Points handelt. Auffallend in Abbildung 3.11 ist der grosse WPA1 & WPA2 Anteil. Etwa ein Drittel dieser Access Points ist im Jahr 2011 nicht oder nur unzureichend verschlüsselt.
Im Vergleich von Wohngegend und Geschäftsviertel fällt auf, dass in der Wohngegend der Anteil der nicht verschlüsselten Access Points geringer ist, dafür ist der Anteil mit WEP verschlüsselten Access Points grösser. In der Wohngegend sind ca. 37% der Access Points unzureichend verschlüsselt, während dies im Geschäftsviertel nur ca. 31% sind. Somit ist dieser Anteil im Wohngebiet grösser und im Geschäftsviertel kleiner als der Durchschnitt aller Access Points vom Jahr 2011.
Der Vergleich mit dem Jahr 2006 widerspiegelt den Trend zu sichereren WLAN-Netzen. Im Jahr 2006 ist der Anteil an unzureichend verschlüsselten Access Points bei ca. 93%. Über 60% aller Access Points benutzten WEP, während WPA sehr selten konfiguriert war. Trotzdem ist der Anteil an mit WEP verschlüsselten Access Points im Jahr 2011 mit ca. 25% noch sehr hoch und über dem Durchschnitt des Wohngebietes.

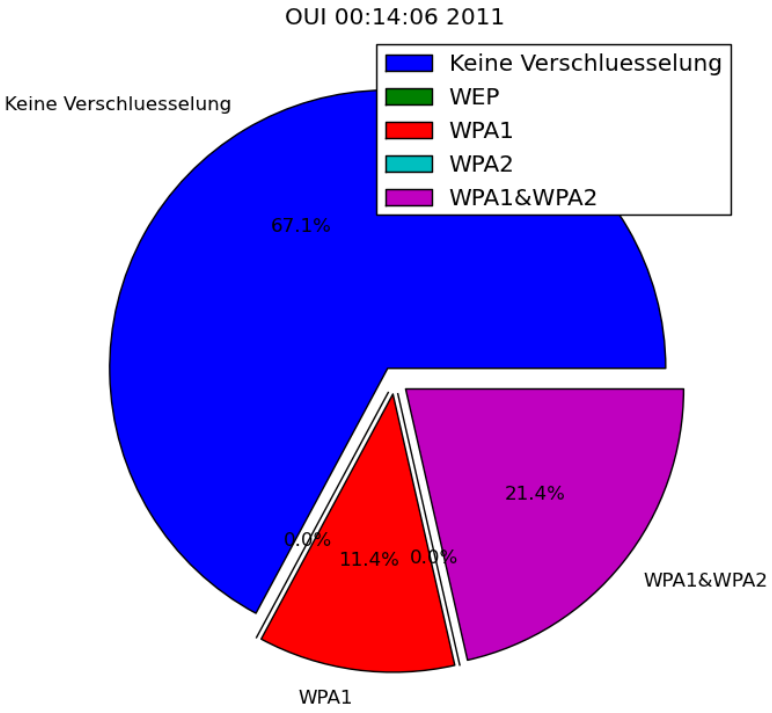

Abbildung 3.14: Verschlüsselung der OUI 00:14:06 (Go Networks) im Jahr 2011

Im Geschäftsviertel wurde diese OUI 59 Mal gefunden. Diese Access Points haben die Namen "MONZOON", "MONZOON-EAP", "freeonline.ch" und "metrozone.ch". Es handelt sich also um Hotspots. Diese haben Landingpages oder sind mit WPA verschlüsselt, sind also nicht voll offen.

3.10 Verbindungstests

Beim Verbindungstest hat das Script versucht, eine WLAN Verbindung zu den nicht verschlüsselten Netzwerken herzustellen. Wenn dies geklappt hat, wurde überprüft, ob DNS und HTTP über IPv4 sowie IPv6 funktioniert. Da bei den importierten Daten keine Verbindungstests durchgeführt wurden, beschränkt sich die Auswertung auf den Datenbestand von 2011.
Im nachhinein musste festgestellt werden, dass der HTTP6-Test fehlerhaft ist. Dadurch lässt sich nichts über IPv6 aussagen. Bei 61 Access Points wurden die Tests erfolgreich durchgeführt. 11 von den HTTP4-Verbindungen wurden als HARDFAIL gemessen. Bei 19 von diesen

Access Points funktionierte die HTTP4-Abfrage und es wurde die erwartete HTTP4-Antwort zurückgegeben. Bei insgesamt 31 Access Points wurde eine Landingpage gefunden. Bei einer grossen Zahl von nicht verschlüsselten Access Points konnte keine Verbindung hergestellt werden.
Aufgrund der sehr tiefen Zahl von erfolgreichen Verbindungsversuchen, wird auf eine genauere Analyse verzichtet. Mit den Verbindungstests ist es also nicht möglich, Hotspots zuverlässig von privaten unverschlüsselten Netzwerken zu unterscheiden.

Kapitel 4

Ausblick

Es könnte spannend sein, in einigen Jahren diese Untersuchung zu wiederholen. Somit könnte dies der Beginn einer längerfristigen Untersuchung sein. Da die Software leider auch zum jetzigen Zeitpunkt immer noch Probleme beinhaltet, wird diese im folgenden Kapitel niedergeschrieben, um die Benutzung und Erweiterung der Software zu erleichtern.

4.1 Verbindungtests bei offenen Netzwerken

Es wird empfohlen, die Verbindungstests in Zukunft nicht mehr durchzuführen, da die Verbindungsversuche nur bei einem kleinen Teil der offenen Netzwerke funktionierte und sehr viel Zeit (Bugsuche und Verbindungszeit) beanspruchte. Ein noch wichtigerer Punkt ist, dass auf gewissen Access Points keine Verbindung möglich ist (aus verschiedenen Gründen), egal wie lange man wartet. Wenn nun der Versuch aufgrund des Timeouts abgebrochen wird, wird das Netzwerk nicht als bereits getestet gespeichert, denn vielleicht hat man ja zu einem späteren Zeitpunkt besseren Empfang und dann könnte der Versuch funktionieren. Nun muss man stehen bleiben, bis alle Tests abgeschlossen sind. Wenn jetzt ein solches Timeout auftritt, und ein neuer Durchlauf beginnt, muss man sehr schnell wieder stehen bleiben und man kommt kaum vorwärts. Aus diesen Gründen wird zukünftigen Gruppen empfohlen, diesen Teil aus der Applikation zu löschen.

4.2 iwlist

Das Scannen der Access Points wird von `iwlist` übernommen. Es musste festgestellt werden, dass diese Scans nicht immer komplett sind. Dies kann das Erkennen der richtigen Verschlüsselung verunmöglichen, falls der "WPA-Tag" fehlt. Da dieses Problem erst spät erkannt wurde, ist die Software nicht optimal darauf ausgelegt. Im Moment werden nur die neu gefundenen Access Points in die Datenbank geschrieben, diejenigen, welche schon früher gefunden wurden, werden gar nicht mehr behandelt (ausser Verbinungstest und Standortinformationen). Um das Problem des nicht kompletten iwlist-Scans zu minimieren, wird empfohlen, jedes Mal alle Informationen mit der Datenbank abzugleichen, um so möglichst alle Informationen zu bekommen.

4.3 n Standard

Es wird vermutet, dass die n-Standard Netzwerke von der Hardware falsch erkannt wurden. Bei einer zukünftigen Arbeit sollte man sicher n-kompatible Hardware verwenden und wohl auch auf die falschen Datensätze dieser Arbeit achten. Sie werden fäschlicherweise als a-Standard erkannt, da der Treiber die Bitraten auch nur bis 54 Mb/s ausgibt und das gleiche Frequenzband nutzt.

4.4 Steuerung

Eine Suche beendet man beim verwendeten Programm mit Ctrl-c. Dies kann Probleme verursachen, wenn man diese Tastenkombination genau dann drückt, wenn das Programm beispielsweise in einem Verbindungstest steckt. Denn ein Ctrl-c wirft eine Exception (KeyboardInterrupt) und diese wird während eines Verbindungstests gefangen und als hardfail gewertet, was zu einer Verfälschung der Ergebnisse führen kann.

4.5 GPS

Um die Genauigkeit zu erhöhen, könnte eine Routine eingebaut werden, welche den Ort der Access Points besser berechnet. Zum jetzigen Zeitpunkt wird die Position an derjenigen Stelle angenommen, an der der Access Point die beste Signalstärke lieferte. Es wäre aber möglich, mit Hilfe der Signalstärke an verschiedenen Positionen den Ort des Access Points genauer abzuschätzen.

4.6 Datenbank

Da die importierten Traces nicht nur in einer Gegend sind (z.B. Geschäftsviertel und Wohngegend), kann die anfangs eingerichtete Struktur nicht vollständig genutzt werden, da vorgesehen war, einen Trace einer Gegend zuzuordnen. Aus diesen Grund mussten für die Auswertung die GPS Koordinaten verwendet werden und man konnte sich nicht auf die Datenbank verlassen. Es wird empfohlen, sich für etwas zu entscheiden und die Datenbank entsprechend anzupassen.

4.7 Auswertung

Den Dataviewer könnte man noch dahingehend verbessern, dass man Filteroptionen einstellen kann. So würde die Auswertung der Daten erheblich vereinfacht.

Literaturverzeichnis

[1] OpenStreetMap,
OpenStreetMap Foundation,
http://www.openstreetmap.org/,
Abgerufen am: 04.07.2011

[2] osm-gps-map,
John Stowers, Till Harbaum, Alberto Mardegan, Mark Cottrell und Marcus Bauer,
http://nzjrs.github.com/osm-gps-map/,
Abgerufen am: 04.07.2011

[3] OUI PUBLIC LISTING: PUBLIC OUI AND 'COMPANY_ID' ASSIGNMENTS,
IEEE Registration Authority,
http://standards.ieee.org/develop/regauth/oui/public.html,
Abgerufen am: 22.06.2011