

WEP - Probleme und Risiken

Alexander Nägele, Matr.Nr. 215441, alex@societys-pet.de

Tobias Walter, Matr.Nr. 215438, tobias@zahrun.net

Benjamin Bratkus, Matr.Nr. 215180, benscho@benscho.org

Dozent:

Mirko Dziadzka

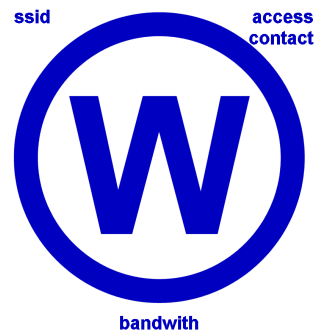
WPV Angewandte Netzwerksecurity

FH Furtwangen

Sommersemester 2004

Powered by L^AT_EX

27. Juni 2004



Inhaltsverzeichnis

1	Vorwort	3
2	WLAN - ein Überblick	4
2.1	Technische Funktion von WLAN	4
2.2	Standards	5
2.3	Frameformat von 802.11 oder 'Wie die Daten durch die Luft fliegen'	7
3	WEP	10
3.1	Wie wird verschlüsselt?	10
3.2	Wie wird authentisiert?	11
4	Warum WEP scheisse ist	12
5	Möglichkeiten, WEP zu knacken	14
5.1	FMS-Attacke	14
5.2	Das Problem von XOR	14
5.3	Brute Force	15
5.4	Dictionary Attack	15
6	Tools	15
6.1	tcpdump und Ethereal	16
6.2	Kismet	17
6.3	Wellenreiter	18
6.4	Airsnort	18
6.5	WepCrack	18
7	Wie macht man WLAN sicherer?	19
7.1	Konfiguration und Administration der Funkkomponenten	19
7.2	Zusätzliche technische Maßnahmen	20
7.3	Organisatorische Maßnahmen	20
7.4	Ausblick	21
8	Fazit	22
9	Referenzen	23

1 Vorwort

In der heutigen Zeit schießen drahtlose Netzwerke gar pilzartig aus dem Boden. Für Firmen und vor allem auch für Privatpersonen werden sie zunehmend erschwinglicher. Hinzu kommt neben den günstigen Preisen noch die einfache Konfiguration, um sich ein solches Netzwerk aufzubauen.

Im Vergleich zu verkabelten Netzen, auf die nur durch direkten Anschluss per Kabel zugegriffen werden kann, halten sich WLAN-Netze nicht an Gebäudegrenzen. Somit wird es für Angreifer einfacher, bspw. ausserhalb eines Firmengeländes auf ein internes Netzwerk Zugriff zu erlangen. Der Angriff auf ein kabelloses Netzwerk wird also immens vereinfacht, da keine physikalische Verbindung mehr benötigt wird.

Nichtsdestotrotz besteht die Möglichkeit, mit Hilfe von WEP¹ zu verschlüsseln. Hierbei zeigt sich allerdings, daß dies vielen Privatanwendern oft nicht bekannt ist oder aus Leichtsinne einfach übersehen wird. Hinzu kommt die meist deaktivierte WEP-Verschlüsselung durch die Hersteller bei der Auslieferung ihrer Endgeräte. Ausserdem ist zu beachten, dass die WEP-Verschlüsselung an sich nur ein gewisses Maß an Sicherheit bietet, die durch unterschiedliche Attacken und das Ausnutzen von Verschlüsselungsschwachstellen ausgehebelt werden kann.

Diese Ausarbeitung soll zuallererst einen allgemeinen Überblick über WLAN verschaffen und dessen technische Funktion beleuchten. Nach einer Auseinandersetzung mit der WEP-Verschlüsselung wird dann näher auf die Risiken eingegangen, die sich daraus ergeben. Anschliessend werden unterschiedliche Möglichkeiten vorgestellt, mit denen WEP geknackt werden kann. Zu guter Letzt gibt die Ausarbeitung dann einen Ausblick darauf, wie man WLAN sicherer gestalten kann.

Dieses Dokument soll aber nicht als Anleitung zum Knacken von WLAN-Netzen, geschweige denn zur Verbesserung derer Sicherheit dienen. Das Ziel ist lediglich, einen Einblick in WLAN und WEP zu geben sowie die damit verbundenen Sicherheitsrisiken zu analysieren.

¹Wired Equivalent Privacy

2 WLAN - ein Überblick

Der folgende Abschnitt beschreibt die technische Funktion von WLAN in seinen Grundzügen und geht auf die einzelnen Standards ein. Anschliessend wird die verwendete Fragmentierung bei WLAN näher betrachtet.

2.1 Technische Funktion von WLAN

Das einfachste WLAN-Netz besteht aus mindestens zwei Kommunikationspartnern. Der Kommunikationsbereich dieser beiden Partner ist dabei durch die Reichweite der Funkwellen begrenzt. Dieser Bereich wird auch als Basic Service Set, kurz BSS, bezeichnet. Im BSS kann die Kommunikation auf zwei Arten erfolgen.

- **AdHoc**

Im AdHoc-Modus kommunizieren zwei oder mehr mobile Endgeräte, ausgestattet mit einer WLAN-Karte, direkt miteinander (Peer 2 Peer). Dabei besteht keine feste Verbindung zwischen den Clients, diese wird nur bei Bedarf hergestellt. In diesem Modus sind Access Points also überflüssig, da jeder mit jedem kommuniziert und somit keine zentrale Vermittlungsstelle notwendig ist. Die nachfolgende Abbildung verdeutlicht dies. Falls

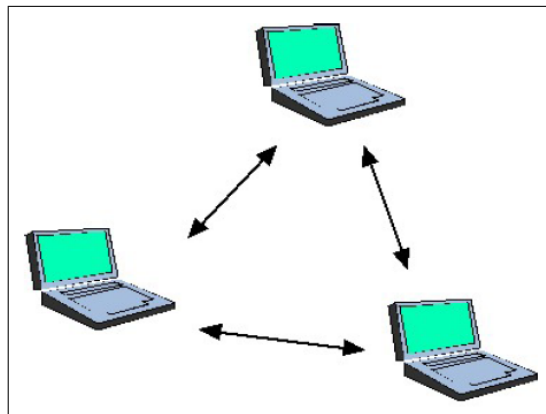


Abbildung 1: AdHoc-Modus

man plant, eine kleine Gruppe von Rechnern zu vernetzen, ist dies wohl die kostengünstigste Alternative, wobei die Access Point-Lösung natürlich mehr Komfort bietet.

- **Infrastructure**

Im Gegensatz zum AdHoc-Verfahren findet der Infrastructure-Modus die grösste Verwendung bei WLAN-Netzen. Hierbei befindet sich ein Access-Point im BSS, der mit mehreren Clients kommuniziert. Man findet hier eine Zellstruktur vor, in der jeder Access Point eine Zelle bedient. Folglich findet die Kommunikation zwischen den Clients über diesen Access Point statt.

Zusätzlich zur Client-IP und der Netzmaske wird eine SSID² verwendet,

²Service Set Identifier

die den Namen des Netzwerkes definiert. Die SSID, bestehend aus einer alphanumerischen Zeichenfolge, dient dazu Netze, selbst wenn sie auf dem gleichen Kanal überlappend arbeiten, eindeutig zu unterscheiden. Die eigentliche Unterscheidung der Netze findet allerdings auf der Basis der ESSID³ bzw. der BSSID⁴ statt. Da diese aber im MAC-Adressen-Format vorliegen, sind sie für den Anwender nur schwer zu merken.

Die wichtigsten Faktoren, um ein Infrastructure-Netzwerk zu betreiben sind also die SSID, die BSSID sowie der Kanal, auf dem das Netz arbeiten soll. Auf der folgenden Grafik ist eine Möglichkeit für ein Infrastructure-Netzwerk abgebildet. Wie daraus ersichtlich, kann ein Access Point eine

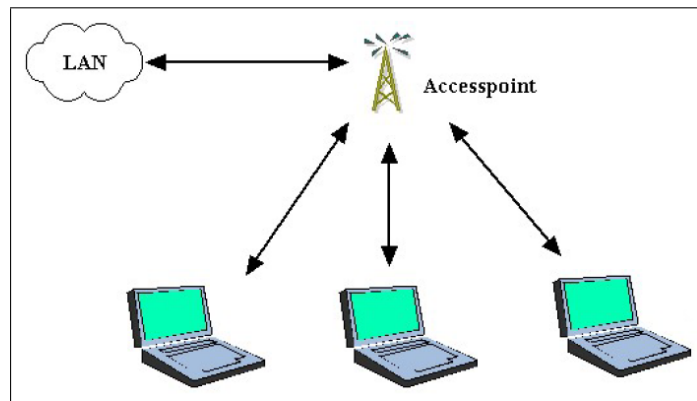


Abbildung 2: Infrastructure-Modus

Verbindung zu anderen Netzen bereitstellen, z.B. zu einem LAN. So könnten bspw. zwei Access Points, also zwei Funkzellen, über ein LAN verbunden werden. Ein anderer Vorteil, der sich bei der Verwendung mehrerer Access Points ergibt ist das Roaming. Hierbei wird beim Zellenwechsel von sich überlappenden Funkzellen die Verbindung aufrechterhalten, wodurch grosse Bereiche flächendeckend versorgt werden können.

2.2 Standards

Die folgende Tabelle bietet einen Überblick über die wichtigsten vom IEEE definierten WLAN-Standards.

Standard	Frequenzband	max. Datenrate	NOC	max. Reichweite innen/aussen
802.11	2,4 GHz	2MBit/s	3	100/300 Meter
802.11a	5 GHz	54 MBit/s	4	20/1500 Meter
802.11b	2,4 GHz	11 MBit/s	3	50/300 Meter
802.11g	2,4 GHz	54 MBit/s	3	50/300 Meter

³Extended Service Set Identifier

⁴Basic Service Set Identifier

Anmerkungen:

- Im Frequenzband direkt nebeneinander liegende Kanäle können sich überlappen. NOC (Non Overlapping Channels) gibt dabei die maximale Anzahl der sich nicht überlappenden Kanäle an.
- Bei den oben angegebenen Datenübertragungsraten werden nur ca. 50 Prozent im Praxiseinsatz erreicht.

802.11

Nach siebenjähriger Entwicklung wurde vom IEEE der 802.11 Standard verabschiedet. Dieser ermöglicht Datenübertragungsraten von 1 bis 2 MBit/s. Der Standard arbeitet auf einem Frequenzband von 2,4 GHz und erlaubt eine Reichweite von maximal 300 Metern im Aussenbereich und 100 Metern innerhalb von Gebäuden. Allerdings findet er heute kaum noch Verwendung und ist höchstens noch für AdHoc-Netze interessant.

802.11a

Der 802.11a Standard wurde 1999 definiert und erlaubt theoretisch Datenübertragungsraten von bis zu 54 MBit/s. Der Standard funkt im 5 GHz-Bereich mit einer sog. OFDM⁵ Modulation. Durch die Verwendung dieses Frequenzbereiches kann es allerdings zu Störungen mit anderen Geräten kommen, die auch diese Frequenz nutzen, z.B. Radar- oder Satellitenübertragungsgeräte. Desweiteren können Reichweiten von bis zu 1500 Meter im Aussenbereich, allerdings nur 20 Meter im Innenbereich, erreicht werden. Ausserdem ist die Nutzung von 802.11a in Deutschland nur auf Bereiche innerhalb von Gebäuden zugelassen.

802.11b

Definiert wurde der 802.11b Standard im Jahr 1999 und ist heute der am meisten verwendete Standard in Industrie und Home-Office. Ein Grund dafür sind die stark gesunkenen Preise. Auf einem Frequenzband von 2,4 GHz werden Datenraten von bis zu 11 MBit/s erreicht. Bedauerlicherweise wird diese Frequenz auch von Mikrowellen und Bluetooth-Geräten genutzt, was zu Störungen führen kann. Die Reichweite innerhalb von Gebäuden betrifft maximal 50 Meter, ausserhalb bis zu 300 Meter. In Deutschland darf der Standard im Aussen- sowie im Innenbereich eingesetzt werden.

802.11g

Der 802.11g Standard ist voll kompatibel zu 802.11b, bietet aber eine Datenübertragungsraten von 54 MBit/s. Der Standard wurde im Jahr 2003 definiert, arbeitet ebenfalls auf einem Frequenzband von 2,4 GHz und hat eine Reichweite von 50 Metern innerhalb sowie von 300 Metern ausserhalb von Gebäuden. In Deutschland ist der Einsatz inner- und ausserhalb von Gebäuden erlaubt und nicht zuletzt durch die Abwärtskompatibilität dürfte dieser Standard die Zukunft des WLANs sein.

802.11h

Der 802.11h Standard stellt eine Erweiterung des 802.11a Standards für den eu-

⁵Orthogonal Frequency Division Multiplexing

ropäischen Markt dar mit der Unterstützung für DFS⁶ und TPC⁷. Dabei wird nur die momentan benötigte Bandbreite genutzt, was zu einer Verringerung der Störanfälligkeit mit anderen Geräten führt.

Aus den IEEE-Spezifikationen lässt sich damit folgender Migrationspfad ableiten.

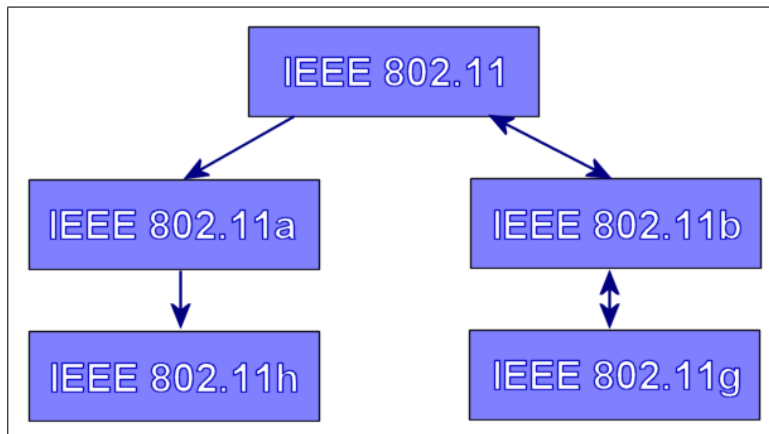


Abbildung 3: WLAN Migrationspfad

2.3 Frameformat von 802.11 oder 'Wie die Daten durch die Luft fliegen'

Frames, die in 802.11 verwendet werden, setzen sich aus dem MAC Header (30 Byte Länge), dem Framebody (0 bis 2312 Byte Länge) und der Frame Checksum (4 Byte Länge) zusammen. Die Frame Checksum wird dabei über den MAC Header und den Framebody gebildet.

Frame Control	Duration/ ID	Addr. 1	Addr. 2	Addr. 3	Sequence Control	Addr. 4	Frame Body	FCS
2	2	6	6	6	2	6	0-2312	4

in Byte

Protoc. Version	Type	Sub- type	To DS	From DS	MF	Retry	Power Manag.	More Data	WEP	Order
2	2	4	1	1	1	1	1	1	1	1

in Bit

⁶Dynamic Frequency Selection

⁷Transmission Power Control

Genauere Beschreibung der Frames und der Frame Control:

Frame Control

Das Frame Control Feld ist 2 Byte lang und setzt sich aus folgenden Komponenten zusammen:

- **Type**

Das Type Feld hat eine Länge von 2 Bit. Ein Paket kann drei verschiedene Funktionen übernehmen. Diese werden im Type Feld gesetzt.

- Daten-Type für Nutzdaten im Framebody
- Control-Type, z.B. für Power-Management
- Management-Type, z.B. zur Authentifizierung und Assoziierung

- **Subtype**

Dieses Feld ist 4 Bit lang und legt zusammen mit dem Type Feld die genaue Funktionalität eines Frames fest. Insgesamt gibt es 25 verschiedene Untertypen, die in der nachfolgenden Tabelle aufgeführt sind.

Type Value B3 B2	Type Description	Subtype Value B7 B6 B5 B4	Subtype
00	Management	0000	Association Request
00	Management	0001	Association Response
00	Management	0010	Reassociation Request
00	Management	0011	Reassociation Response
00	Management	0100	Probe Request
00	Management	0101	Probe Response
00	Management	0110-0111	Reserved
00	Management	1000	Beacon
00	Management	1001	ATIM
00	Management	1010	Dissassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication
00	Management	1101-1111	Reserved
01	Control	0000-1001	Reserved
01	Control	1010	Power Save Poll
01	Control	1011	Request To Send
01	Control	1100	Clear To Send
01	Control	1101	ACK
01	Control	1110	Condition Free End
01	Control	1111	CF-End + CF-ACK
10	Data	0000	Data
10	Data	0001	Data + CF-ACK
10	Data	0010	Data + CF-Poll
10	Data	0011	Data + CF-ACK + CF-Poll
10	Data	0100	Null Function
10	Data	0101	CF-ACK
10	Data	0110	CF-Poll
10	Data	0111	CF-ACK + CF-Poll
10	Data	1000-1111	Reserved
11	Reserved	0000-1111	Reserved

- **Protocol Version**

Das Protocol Version Feld hat eine Länge von 2 Bit und kennzeichnet die Version des verwendeten 802.11-Protokolls. Dieser Wert ist für alle Versionen von

802.11 identisch, nämlich 0. Andere Werte sind für neue Revisionen des Standards reserviert, die bei einer möglichen Inkompatibilität verwendet werden.

Wird ein Frame mit einer vom Empfänger nicht unterstützten Protocol Version empfangen, wird dieser verworfen. Dies wird dem Sender allerdings nicht mitgeteilt.

- **To DS**

Das To DS Feld (Distribution System) ist 1 Bit lang. Bei Paketen, die für ein DS bestimmt sind, also bei 2 oder mehr miteinander verbundenen Access Points, wird dieser Wert auf 1 gesetzt, bei allen anderen auf 0.

- **From DS**

Dieses Feld ist 1 Bit lang und wird für alle Datenpakete, die das DS verlassen, auf 1 gesetzt. Dies wird in der folgenden Tabelle ersichtlich.

To DS	From DS	Bedeutung
0	0	Direkte Datenpakete zwischen Stationen im gleichen WLAN (AdHoc), sowie auch Management- und Kontrollpakete
1	0	Datenpakete, welche für das DS bestimmt sind (Managed Modus)
0	1	Datenpakete, welche das DS verlassen (Übergang WLAN in Kabelnetzwerk)
1	1	Paket eines WDS, welches von einem Access Point zu einem anderen transportiert wird

- **MF**

Das More Fragments Feld ist ein Bit lang und wird bei verwendeter Fragmentierung auf 1 gesetzt, also wenn bei Daten- und Management-Paketen noch ein Fragment folgt.

- **Retry**

Das 1 Bit lange Retry Feld wird bei Daten- und Management-Paketen auf 1 gesetzt, wenn das Paket bereits mindestens einmal versendet wurde. Andernfalls enthält das Feld den wert 0. Dieses Feld dient dazu, mögliche Dubletten leichter zu eliminieren.

- **Power Management**

Dieses Feld mit einer Länge von 1 Bit zeigt den Stromsparmodus einer Station an. Hier wird der Modus der sendenden Station nach der Übertragung gekennzeichnet. Ist dabei das Feld auf 1 gesetzt, deutet dies daraufhin, dass der Sender in den Stromsparmodus wechselt, bei 0 ist dies nicht der Fall. Zwischen zwei Access Points ist dieses Feld immer auf 0 gesetzt.

- **More Data**

Das More Data Feld (1 Bit lang) teilt Stationen, die sich im Stromsparmodus befinden mit, dass weitere Pakete am Access Point für sie vorliegen (Wert auf 1). Dieses Feld wird bei Daten- und Management-Paketen verwendet.

- **WEP**

Das WEP Feld gibt an, ob die WEP-Verschlüsselung aktiviert ist oder nicht, d.h. ob der Inhalt des Framebodys verschlüsselt vorliegt.

- **Order**

Das 1 Bit lange Order Feld wird bei allen Datenpaketen, di nach Strictly Ordered Service Class⁸ transportiert werden, auf 1 gesetzt.

⁸vom IEEE definiert

Duration/ID

Das Duration/ID Feld ist 2 Byte lang. Bei Frames vom Typ Control (Subtype Power Save Poll) enthält das Feld die AID⁹ des Senders. Bei allen anderen enthält das Feld einen Wert, der zur Aktualisierung des NAV¹⁰ benötigt wird. Der NAV legt die Dauer der erlaubten Übertragungszeit fest. Sollte CFP¹¹, einer von 2 Übertragungsmodi im WLAN, verwendet werden, wird der Duration-Wert auf das Maximum gesetzt (32768).

Address 1-4

Beim WLAN-Framing existieren insgesamt 4 Adressfelder im MAC-Adress-Format. Sie werden benutzt, um die BSSID, die Source Address, die Destination Address, die Transmitting Station Address und die Receiving Station Address zu übermitteln. Je nach der Frame Control variiert dabei die Angabe der Adressen, so z.B. Address 1 für den endgültigen Empfänger, Address 2 für den endgültigen Sender, Address 3 für den nächsten Empfänger und Address 4 für den letzten Sender.

Sequence Control

Das 2 Byte lange Sequence Control Feld besteht aus den Elementen Sequenznummer (12Bit) und Fragmentnummer (4 Bit). Die Sequenznummer wird in jedem Paket verwendet und zusammen mit der Fragmentnummer kann ein Paket eindeutig gekennzeichnet werden. Die Sequenznummer beginnt bei 1 und wird dann um je 1 inkrementiert. Für das erste Fragment einer Fragmentierung und für unfragmentierte Pakete wird die Fragmentnummer 0 vergeben, die sich auch bei erneutem Senden des Paketes nicht ändert.

Frame Body

Der Frame Body hat eine variable Länge von 0 bis 2312 Byte. Wird die WEP-Verschlüsselung verwendet, erweitert sich die Länge, da die ICV¹² und der IV¹³ mit je 4 Byte hinzukommen.

FCS

Die Frame Check Sequence ist eine CRC32-Checksum, die über den Header und den Framebody gebildet wird. Das Feld hat eine Länge von 4 Byte.

3 WEP

Bei der WEP-Verschlüsselung (Wired Encryption Privacy) benötigt jede Station und jeder Access Point einen identischen Schlüssel, einen sog. Shared Key. Dieser hat eine Länge von 40 oder 104 Bit. Zusätzlich muss im MAC Header das WEP-Bit entsprechend gesetzt werden.

3.1 Wie wird verschlüsselt?

In diesem Abschnitt soll erläutert werden, wie mit Hilfe von WEP verschlüsselt wird. Dazu wird der RC4-Algorithmus benutzt, der im folgenden näher betrachtet wird.

Um mit WEP zu verschlüsseln, wird ein 40 oder 104 Bit langer Schlüssel (Shared Key) benötigt. Dieser muss jedem teilnehmenden Kommunikationspartner, also bspw. Client und Access Point, bekannt sein.

Zusätzlich wird vom Sender ein 24 Bit langer Initialisierungsvektor gewählt. Dieser

⁹Association Identity

¹⁰Network Allocation Vectors

¹¹Contention Free Period

¹²Integrity Check Value

¹³Initialisierungsvektor

wird dazu genutzt, gleiche Datenpakete nach der Verschlüsselung unterschiedlich aussehen zu lassen. Die Übertragung des IV ist unverschlüsselt. Nach der Generierung des IV wird dieser zwischen Header und Body eingefügt.

Aus dem IV und dem Shared Key wird dann ein pseudozufälliger Bitstrom erzeugt. Anschliessend wird über die zu sendenden Daten anhand des CRC32-Algorithmus eine Prüfsumme über die Daten gebildet. Diese Prüfsumme wird Integrity Check Value, kurz ICV, genannt.

Nun können die Daten verschlüsselt werden. Dazu wird der Bitstrom mit den Daten und der dazugehörigen ICV über XOR verknüpft. Hierdurch erhält man die verschlüsselten Daten.

Zusammen mit dem IV werden die verschlüsselten Daten in ein WLAN-Paket verbaut, was durch Anhängen des Headers und der Frame Check Sequence geschieht. Dieses Paket kann nun gesendet werden. Auf Empfängerseite werden der IV und die ver-

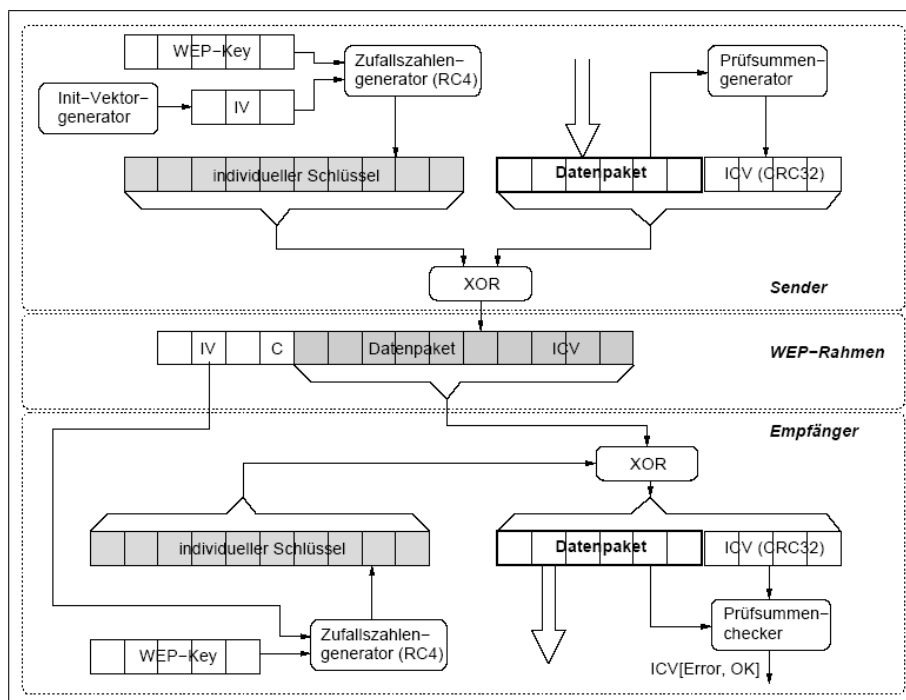


Abbildung 4: Verschlüsselung mit WEP

schlüsselten Daten aus dem Paket extrahiert. Mit Hilfe des Shared Keys und des IV als Klartext wird derselbe Bitstrom wie beim Sender generiert. Um den Klartext der verschlüsselten Daten zu erhalten, werden diese erneut mit dem generierten Bitstrom XOR verknüpft. Über die erhaltenen Daten wird nun eine CRC32-Prüfsumme gebildet und mit der empfangenen ICV des Paketes verglichen. Bei einer Übereinstimmung beider ICV kann also davon ausgegangen werden, dass die Daten fehlerfrei übertragen wurden.

Anmerkung: Für jedes zu sendende Paket wird ein anderer IV gewählt, um einen konstanten Bitstrom zu vermeiden.

3.2 Wie wird authentisiert?

Zur Authentisierung in WLAN-Netzen gibt es zwei Möglichkeiten: die Open System und die Shared Key Authentifizierung. Bei der Open System Authentifizierung han-

delt es sich um kein richtiges Authentifizierungsverfahren. Der Access Point gleicht höchstens die Sender MAC-Adresse mit einer black- bzw. white-list ab. Die Shared

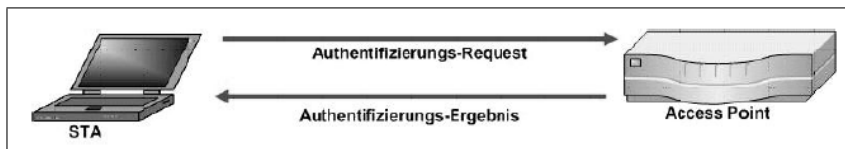


Abbildung 5: Open System Authentifizierung

Key Authentifizierung hingegen verwendet ein Challenge-Response Verfahren. Dabei schickt der Access Point einen zufällig generierten, 128 Bit langen Text an den Client. Dieser verschlüsselt die Challenge mit einem Bitstrom, der aus dem beidseitig bekannten Shared Key und dem Initialisierungsvektor generiert wurde (Verfahren wie bei WEP).

Die verschlüsselten Daten schickt der Client wiederum an den Access Point, welcher die Daten entschlüsselt und das entsprechende Authentifizierungsergebnis zurück an den Client schickt. Der Authentisierungsprozess läuft dabei einseitig ab, der Access Point muss sich also nicht beim Client authentisieren.

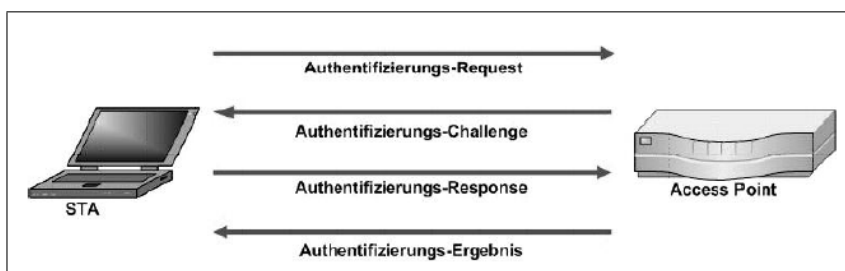


Abbildung 6: Shared Key Authentifizierung

4 Warum WEP scheisse ist

In diesem Kapitel sollen die Schwachstellen der WEP-Verschlüsselung aufgezeigt werden.

Zu kurze Schlüssel

Die erste Implementierung von WEP verfügte nur über einen 40 Bit langen Schlüssel. Die mit dieser Keylänge verschlüsselte Nachricht kann selbst mit handelsüblichen PCs innerhalb weniger Tage durch Schlüsseldurchprobieren entschlüsselt werden. Eine Länge von 104 Bit ist dagegen ausreichend, um sich auch vor versierten Angreifern mit solch einer Attacke zu schützen.

Schwachstellen im RC4-Design

Gewisse Schwachstellen im RC4-Design sind seit dem Jahr 2001 bekannt. Im Internet erhältliche Tools erlauben es auch weniger versierten Anwendern, einen Angriff auf das WEP-Protokoll durchzuführen.

Durch das Sammeln einer bestimmten Anzahl von Paketen mit den dazugehörigen Initialisierungsvektoren lässt sich mit Hilfe von statistischen Methoden der gesamte Schlüssel bestimmen. Da für Angreifer Pakete mit schwachen Initialisierungsvektoren

recht selten sind, muss dieser entsprechend viele Pakete mitsniffen. Sollte der IV immer um 1 inkrementiert werden, würde man z.B. etwa 4 Millionen Pakete benötigen. Durch aktuelle Verbesserungen des Angriffs werden lässt sich diese Anzahl aber auf ca. 1 Million beschränken.

Die für den Angreifer benötigte Zeit hängt stark von der durchschnittlichen Paketgrösse und der durchschnittlichen Übertragungsrate, also der Auslastung des Access Points ab. Die folgenden zwei Tabellen sollen dies verdeutlichen.

Benötigte Datenmenge in Abhängigkeit von der durchschnittlichen Paketgrösse und der Anzahl der Pakete.

Anzahl Pakete	Paket mit 512 Byte	Paket mit 1024 Byte	Paket mit 2048 Byte
2 000 000	0,95 GB	1,91 GB	3,81 GB
4 000 000	1,91 GB	3,81 GB	7,63 GB
6 000 000	2,86 GB	5,72 GB	11,44 GB
8 000 000	3,81 GB	7,63 GB	15,26 GB

Benötigte Zeit in Abhängigkeit von der Datenmenge und der durchschnittlichen Auslastung des Access Points für 802.11b Systeme

Datenmenge	Auslastung 5 MBit/s	Auslastung 1 MBit/s	Auslastung 0,1 MBit/s
0,95 GB	25 min	2,11 h	21,11 h
1,91 GB	50 min	4,24 h	42,22 h
2,86 GB	1,27 h	6,36 h	2,65 Tage
3,81 GB	1,70 h	8,47 h	3,53 Tage
5,72 GB	2,54 h	12,71 h	5,30 Tage
7,63 GB	3,39 h	16,96 h	7,06 Tage
11,44 GB	5,08 h	25,42 h	10,59 Tage
15,26 GB	6,78 h	33,91 h	14,13 Tage

Wiederverwendung des IV

Der WEP-Standard erlaubt die Wiederverwendung des Initialisierungsvektors (IV). Dadurch wird es für Angreifer einfacher, da immer wieder die gleiche Verschlüsselung komprimiert werden muss. Der IV hat einen Wertebereich von 2^{24} . Dies ist viel zu wenig. Ein Stromchiffrialgorithmus kann nur dann sicher sein, wenn der generierte Bitstrom für zwei Datenpakete immer unterschiedlich ist oder sich erst nach unendlich langer Zeit wiederholt. Diese Problematik betrifft sowohl die Verschlüsselung mit 40, sowie mit 104 Bit

Zur Verdeutlichung ein kleines Beispiel: ein Access Point tauscht mit einem Host 1500 Byte grosse Pakete bei einer Übertragungsrate von 11 MBit/s aus. Durch die Rechnung $1500 \times 8 / 11 \times 10^6 \times 2^{24} = 18000$ Sekunden erhält man eine Zeitspanne, nach der sich der IV wiederholt. In der Praxis ist dieser Wert eher etwas kleiner und liegt bei ca. 5 Stunden.

Initialisierung von WLAN-Karten

Einige WLAN-Karten setzen den Initialisierungsvektor beim Initialisieren der Karte auf null und inkrementieren anschliessend um 1. Dadurch werden niedere IVs öfter verwendet, sodass vermehrt Pakete mit einem niedrigen, identischen IV auftauchen.

Austauschen des Shared Keys

Der WEP-Standard bietet keine Methode, Keys automatisch auszutauschen. Dies muss

manuell erledigt werden. Diese Art des Schlüsselmanagement führt in der Praxis oft dazu, dass der Shared zu selten oder gar nicht gewechselt wird.

Authentifizierungsproblem

Bei der Authentifizierung wird der Text verschlüsselt und unverschlüsselt übertragen. Dadurch kann der zu einem IV zugehörige Bitstrom errechnet werden.

Verwendung einfacher Passphrasen

Oft werden einfachste Keyphrasen als Shared Keys verwendet, die leicht mit Dictionary Attacken zu knacken sind.

5 Möglichkeiten, WEP zu knacken

5.1 FMS-Attacke

Die FMS-Attacke (Fluhrer, Martin, Shamir) ist eine wirkungsvolle, aber auch recht komplizierte Möglichkeit, WEP zu knacken. Diese Methode nutzt eine Schwäche im Key-Scheduling-Algorithmus aus.

Durch diesen Implementierungsfehler werden schwache Initialisierungsvektoren erzeugt, die den Schlüsselfestlegungsalgorithmus in einen bestimmten Zustand versetzen, sodaß Rückschlüsse auf den gesuchten Schlüssel gezogen werden können. Je mehr Pakete mit schwachen IVs zur Verfügung stehen, desto mehr Schlüsselbytes können geschätzt werden. Bei genügend mitgeschnittenen Paketen wird die Auswahl an möglichen bishin zum endgültigen Schlüssel eingeeengt.

Im Gegensatz zum Mitschniffen der Pakete, benötigt dann das Berechnen des Keys weniger als eine Minute.

Die Tools Aircrack-ng und Wepcrack verwenden bspw. diese Methode, bei der Wepcrack ca. 5 bis 10 Millionen Pakete mitschniff und Aircrack-ng einen Netzverkehr von 100 bis 1000 MB benötigt.

Anmerkung zu den schwachen Initialisierungsvektoren: Interessant sind für den Angreifer Pakete, deren erste Bytes des IV zwischen 13 und 15 liegen und im zweiten Byte den Wert 255 haben. Hierbei werden für jeden Wert zwischen 3 und 15 ca. 60 Initialisierungsvektoren benötigt. Von den zugehörigen Chiffredaten ist nur das erste Byte erforderlich.

Da ein unverschlüsseltes Paket immer mit demselben Byte (AA) beginnt, kann aus dem ersten Chiffrebyte das erste Byte des Schlüssels ermittelt werden.

5.2 Das Problem von XOR

Der folgende Abschnitt beschreibt, wie man anhand einer verschlüsselten Nachricht und deren unverschlüsselten Klartextes auf den Bitstrom schliessen kann. Mit dessen Hilfe besteht dann die Möglichkeit, in das Netzwerk einzudringen und Schindluder zu treiben.

Das Problem der RC4-Verschlüsselung besteht darin, dass die XOR-Verknüpfung einer verschlüsselten Nachricht mit deren Klartext den Bitstrom ergibt, der zur Verschlüsselung verwendet wurde.

Dies soll an folgendem Beispiel verdeutlicht werden.

- Verschlüsselung anhand des Klartextes und dem Bitstrom:

Nachricht	01101011
Bitstrom	10111001
verschl. Nachricht über XOR	11010010

- Herausfinden des Bitstroms anhand der verschlüsselten Nachricht und deren Klartextes:

Nachricht	01101011
verschl. Nachricht	11010010
Bitsrom über XOR	10111001

Nun besitzt man für einen Initialisierungsvektor den dazugehörigen Bitstrom, mit dem man sich nun am Access Point authentisieren und Nachrichten ins Netz einschleusen kann. Ausserdem lassen sich alle Nachrichten, deren verschlüsselter Bitstrom genau mit diesem IV erzeugt wurde, entschlüsseln.

Möglichkeiten, um an eine verschlüsselte Nachricht und deren Klartext zu gelangen besteht bspw. darin, eine Shared-Key-Authentifizierung zwischen einem Client und einem Access Point abzuhehren. Eine andere Möglichkeit besteht darin, Pakete von ausserhalb zu einem Client ins WLAN-Netz zu schicken und die vom Access Point verschlüsselte Nachricht abzuhehren.

5.3 Brute Force

Bei der Brute Force Attacke werden alle möglichen Schlüsselvarianten durchprobiert. Allerdings ist dies keine realisierbare Lösung, da extrem hohe Rechenzeiten entstehen, was an zwei kleinen Beispielen verdeutlicht werden soll. Es wird davon ausgegangen, das pro Sekunde ca 25000 Wörter berechnet werden können (Pentium4 mit 1,8 GHz)

- **64 Bit Schlüssel (40 Bit Schlüssel + 24 Bit IV)**
 $2^{\text{hoch } 40} \text{ mögliche Schlüssel} / 25000 \text{ Schlüssel/s} = 43980465,11104 \text{ Sekunden}$
 Dies entspricht ungefähr 1,4 Jahren
- **128 Bit Schlüssel (104 Bit Schlüssel + 24 Bit IV)**
 $2^{\text{hoch } 104} \text{ mögliche Schlüssel} / 25000 \text{ Schlüssel/s}$
 $= 811296384146066816957890051,44064 \text{ Sekunden}$
 Dies entspricht ungefähr 25 726 039 578 452 144 119 Jahren

Es besteht allerdings die Möglichkeit, eine Brute Force Attacke entsprechend einzuschränken. Dies könnte der Fall sein, wenn ein Teil des Shared-Keys bekannt ist. Eine Einschränkung ist ausserdem dadurch möglich, da bekannterweise nicht alle ASCII-Zeichen mit der Tastatur eingegeben werden können. Kann man davon ausgehen, dass nur Buchstaben, nur Zahlen oder nur Klein- bzw. Grossbuchstaben im Shared Key verwendet werden, dann würde dies einen idealen Ausgangspunkt für die Brute Force Attacke darstellen.

5.4 Dictionary Attack

Die Dictionary Attack basiert auf der Annahme, daß für den Shared-Key eine einfache Passphrase gewählt wurde. Anhand einer Wortliste werden die darin enthaltenen Wörter durchprobiert. Mit der Rechenleistung heutiger Prozessoren lassen sich dabei mehrere tausend Wörter pro Sekunde testen.

6 Tools

Hier sollen kurz einige Tools vorgestellt werden, mit deren Hilfe die WEP-Verschlüsselung ausgehebelt werden kann. Es handelt sich hierbei um

- tcpdump und Ethereal
- Kismet
- Wellenreiter
- Aircsnort
- WepCrack

6.1 tcpdump und Ethereal

tcpdump ist ein Softwarepaket, das es erlaubt, den Datenverkehr eines Interface zu überwachen. Dabei werden alle Pakete abgehört, die das entsprechende Interface passieren. Die Ergebnisse können wahlweise in eine Datei umgeleitet werden. Die Grösse des Dumps kann dabei eingestellt werden, der Default-Wert liegt bei 64 Byte pro Paket.

Mit tcpdump ist es bspw. möglich, die Quell- und Ziel-MAC, den Ethernet-Type, das Längenfeld und Teile der Nutzdaten auszulesen. Durch die Dekodierung des Ethernet-Type Feldes kann das verwendete Protokoll im Datenteil herausgefunden werden.

tcpdump beschränkt sich allerdings nicht nur auf den IP-Verkehr, da zusätzlich entsprechende Filteroptionen mitgegeben werden können. Um Daten mitzuspionieren, muss sich die Karte selbst im Promiscuous Modus befinden.

Zur graphischen Aufbereitung und Auswertung der Daten von tcpdump-Logs empfiehlt sich das Tool Ethereal.

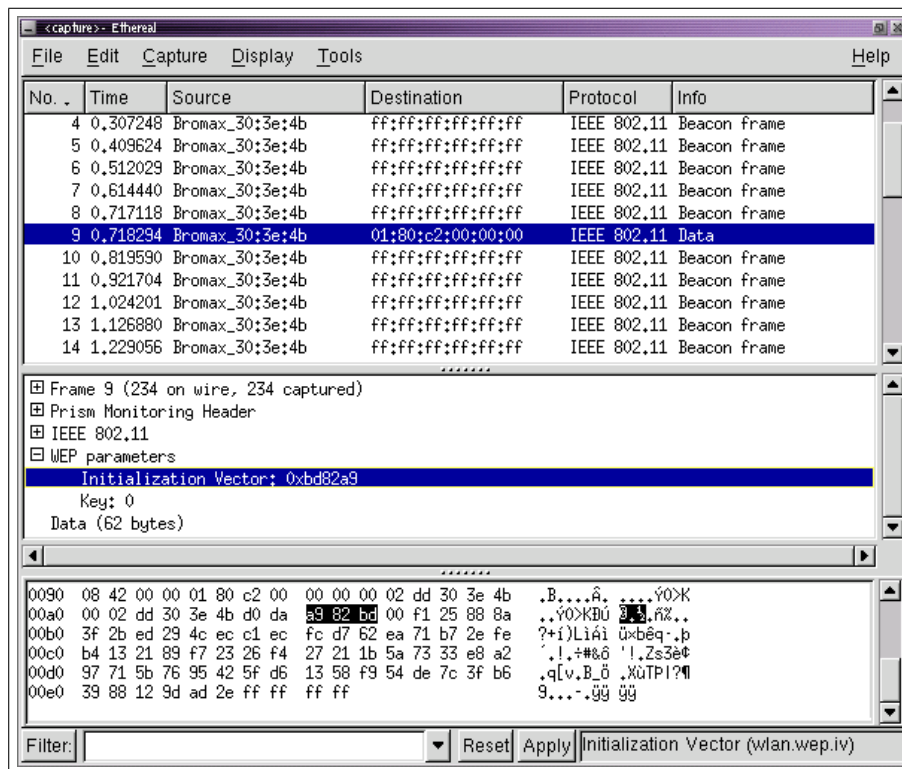
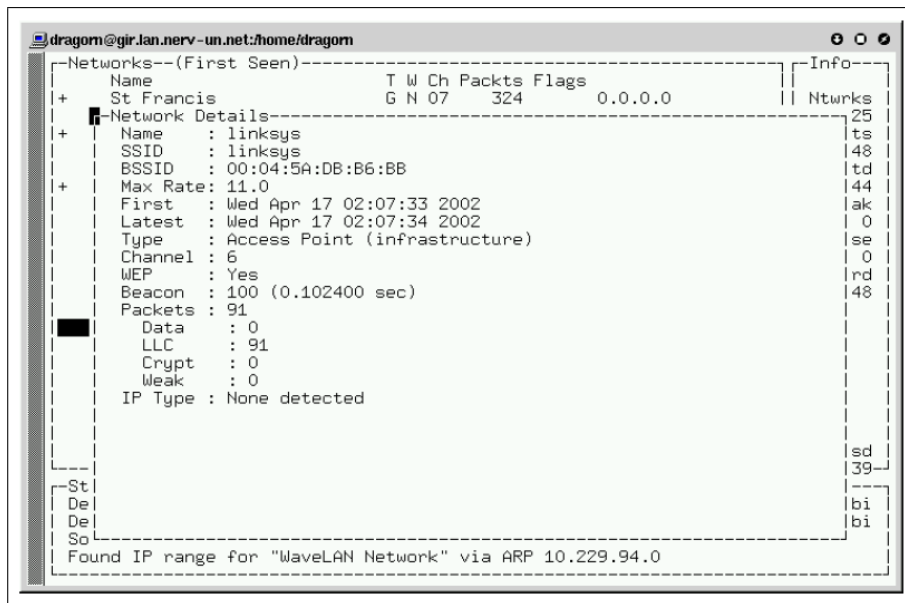


Abbildung 7: Screenshot Ethereal

6.2 Kismet

Ursprünglich wurde das Tool Kismet als Netzwerksniffer entwickelt, findet heute aber hauptsächlich als WLAN-Scanner Verwendung. Dabei können mitgeloggte Daten in verschiedenen Formaten gespeichert werden. Das Tool gibt Netzwerkinfos (SSID, Kanal) und unterschiedliche Statistiken zur Weiterverwendung in anderen Programmen aus.

Bei Kismet kommt die sogenannte Hopper-Funktion zum Einsatz. Dies bedeutet, dass ständig der Kanal gewechselt wird. Dadurch können bequem auf jedem Kanal die Aktivitäten mitverfolgt werden.



```
dragom@gir.lan.nerv-un.net:/home/dragom
--Networks--(First Seen)-----Info-
+ Name          T W Ch Packts Flags      Ntwrks
+ St Francis    G N 07   324   0.0.0.0
+ [Network Details]-----
+ Name       : linksys          ts
+ SSID       : linksys          48
+ BSSID      : 00:04:5A:DB:B6:BB td
+ Max Rate   : 11.0             44
+ First      : Wed Apr 17 02:07:33 2002 ak
+ Latest     : Wed Apr 17 02:07:34 2002 0
+ Type       : Access Point (infrastructure) se
+ Channel    : 6                 0
+ WEP        : Yes                rd
+ Beacon     : 100 (0.102400 sec) 48
+ Packets    : 91
+ Data       : 0
+ LLC        : 91
+ Crypt      : 0
+ Weak       : 0
+ IP Type    : None detected
+
+ St
+ Del
+ Del
+ So
+ Found IP range for "WaveLAN Network" via ARP 10.229.94.0
+
+ sd
+ 39
+ bi
+ bi
```

Abbildung 8: Screenshot Kismet

6.3 Wellenreiter

Wellenreiter ist ein WLAN-Erkennungs- und Überprüfungstool für Linux. Es arbeitet mit weit verbreiteten Prins2-, Lucent- und Cisco-Karten. Das Tool ist einfach zu benutzen und benötigt keine Konfiguration der WLAN-Karte. Es können Netze sowie die ESSID von Broadcast- und nicht-Broadcast-Netzen erkannt werden. Mitgeschnittene Daten werden im tcpdump-Format gespeichert.

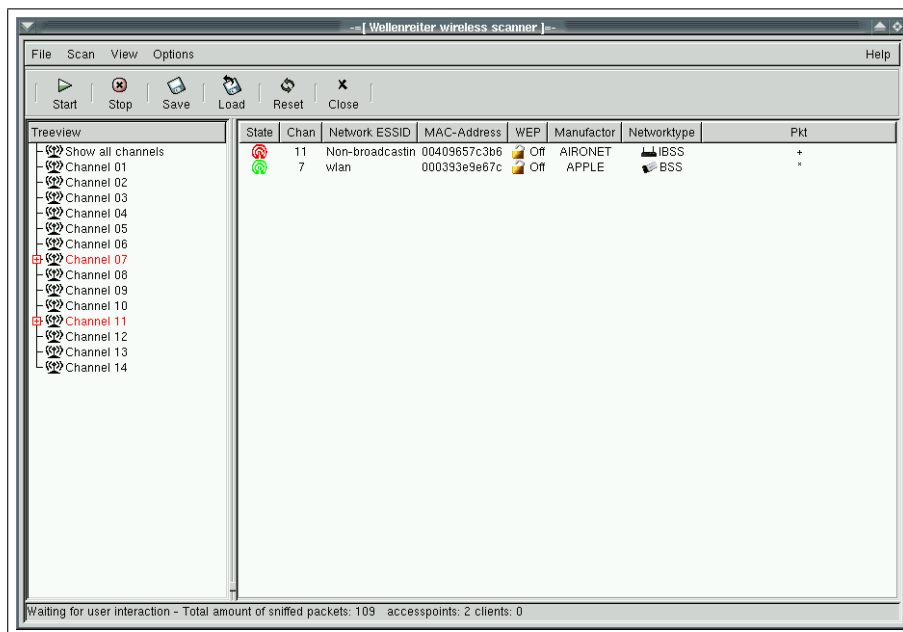


Abbildung 9: Screenshot Wellenreiter

6.4 Aircrort

Aircrort ist ein Tool für passive Attacken. Dabei werden Schwächen im WEP-Algorithmus ausgenutzt (Weak IV). Das unter LINUX arbeitende Programm benötigt ca 100 bis 1000 MB Traffic, um den Schlüssel anschliessend passiv zu rekonstruieren. Wurde ausreichend Traffic abgehört, kann der Schlüssel in kurzer Zeit berechnet werden. Mit dem Zusatztool Decrypt können verschlüsselte Dumpfiles (pcap-Format) anhand der SSID und des Shared Keys entschlüsselt werden. Allerdings unterstützt Aircrort nur die Prism2-Karten.

6.5 WepCrack

WepCrack arbeitet mit der gleichen Attacke wie Aircrort. Für das auf Perl-Skripten arbeitende Tool ist keine spezielle Konfiguration notwendig. Ein Nachteil besteht darin, dass für das Capturen von Daten ein eigenständiges Tool, z.B. Prism-Dump (Tool für Prism2-Karten), verwendet werden muss.

Die URLs zu den einzelnen Tools finden sich in den Referenzen am Ende dieser Ausarbeitung.

7 Wie macht man WLAN sicherer?

Um die Sicherheit von WLAN-Netzen zu erhöhen sind vom Einsatzszenario und dem Schutzbedarf der Informationen abhängig, mehrere Maßnahmen erforderlich. Diese lassen sich in drei Kategorien unterteilen:

- Konfiguration und Administration der Funkkomponenten
- Zusätzliche technische Maßnahmen
- Organisatorische Maßnahmen

Diese Punkte sollen im Folgenden näher erläutert werden.

7.1 Konfiguration und Administration der Funkkomponenten

Diese Basisschutzmaßnahmen sollten trotz bekannter Unzulänglichkeiten aktiviert werden, um Angriffe von einigen frei verfügbaren Tools abzuwehren.

Aktivieren der Basisschutzmaßnahmen

- Passwortvorgaben ändern. Dies betrifft die SSID am Access Point und bei allen Clients, die keine Rückschlüsse auf Firma oder Netzwerk zulassen sollte. Ausserdem sollte das Standard-Passwort zur Konfiguration des Access Points geändert werden.
- SSID-Broadcast am Access Point sollte deaktiviert werden, falls dies technisch möglich ist.
- Aktivieren der MAC-Adressen-Filterung am Access Point.
- 128 Bit WEP-Verschlüsselung aktivieren.
- Sollte die WEP-Verschlüsselung aktiviert sein, ist die Authentisierungsmethode Open zu wählen, da die Sicherheitsmethode Shared Key zusätzliche Risiken birgt.

Periodisches Wechseln des WEP-Schlüssel

Der WEP-Schlüssel sollte in regelmässigen Abständen gewechselt werden. Dabei sollte der Key nach entsprechend anerkannten Passwortgestaltungsregeln so gewählt werden, dass er einen möglichst wirksamen Schutz gegen Angreifer bietet.

Optimieren des Aufstellungsorts und der Antennencharakteristik eines Access Points

Der Access Point sollte so aufgestellt werden, das möglichst nur das gewünschte Gebiet funktechnisch versorgt wird. Es sollte dabei nicht übersehen werden, dass sich Funkwellen horizontal sowie auch vertikal ausbreiten.

Optimierung der Access Point Sendeleistung

Die Sendeleistung sollte soweit reduziert werden, dass nur das gewünschte Gebiet funktechnisch versorgt wird. Allerdings muss zur Gewährleistung der maximalen Datenübertragungsrate ein bestimmtes Signal-Rausch-Verhältnis vorhanden sein.

Deaktivieren des DHCP-Servers im Access Point

Der DHCP-Server im Access Point sollte, sofern vorhanden und möglich, deaktiviert werden. Folglich sollten statische IP-Adressen vergeben und der IP-Adressraum möglichst klein gehalten werden.

Durchführen von Firmware-Upgrades

Die Firmware der Komponenten sollte regelmässig auf erweiterte Sicherheitsstandards

aktualisiert werden. Diese Möglichkeit bieten viele Hersteller an. Hierbei ist zu beachten, dass diese Erweiterungen oft herstellerspezifisch sind. Daher ist die Verwendung dieser Mechanismen meist auf den gleichen Hersteller beschränkt.

Überlappungsfreie Frequenzkanäle

Werden mehrere Access Points eingesetzt, dann sind die benutzten Frequenzkanäle benachbarter Access Points möglichst überlappungsfrei zu wählen.

Funkkomponenten nur bei Gebrauch aktivieren

Sollten Komponenten nicht benutzt werden, dann sollten sie auch deaktiviert werden. Dies gilt für Access Points sowie auch für Clients, bei diesen insbesondere für den AdHoc Modus.

Access Point Konfiguration nur über sichere Kanäle

Die Konfiguration und Administration von Access Points sollte nur über sichere Kanäle, also drahtgebundene Netze erfolgen. Außerdem sollten sichere Protokolle wie SSL/TLS oder SNMPv3 benutzt werden. Zusätzlich sollten nur autorisierte Personen physischen Zugriff zu den Access Points haben.

7.2 Zusätzliche technische Maßnahmen

Die oben genannten Maßnahmen wehren zwar einige Angriffe ab, die mit frei verfügbaren Tools durchführbar sind, das Netz bleibt aber dennoch leicht angreifbar. Folglich sind weitere technische Maßnahmen zur Erhöhung der Sicherheit notwendig.

Verwendung einer zusätzlichen Sicherheitslösung

Das Ziel dieser Sicherheitslösung ist, nur berechnete Clients und Access Points in einem Virtual Private Network, kurz VPN, miteinander kommunizieren zu lassen, sowie diese Kommunikation vertraulich und integritätsgeschützt zu halten. Folglich sollte eine zusätzliche Sicherheitslösung die drei Bausteine Authentisierung, Verschlüsselung und Integritätssicherung sinnvoll miteinander kombinieren.

Hierfür wird hinter dem Access Point ein VPN-Gateway installiert. Beim Verbindungsaufbau wird ein kryptographischer Tunnel (bspw. basierend auf IPSEC oder SSL Version3/TLS) zwischen dem Client und dem VPN-Gateway aufgebaut. Da es sich bei IPSEC und SSL um Standards handelt, können alle marktgängigen Produkte, die diesen Standard erfüllen, verwendet werden. Es sind mittlerweile auch Produkte erhältlich, die die VPN-Funktionalität bereits im Access Point integriert haben.

Abschottung des drahtgebundenen Netzes durch Firewall und IDS

Das drahtgebundene Netz sollte durch eine Firewall mit Intrusion Detection System gegen die Access Points des Funknetzes abgeschottet werden. Mittlerweile sind auch auch funkbasierte IDS auf dem Markt, die das Funk-LAN überwachen und sicherheitsrelevante Anomalien entdecken. Der Einsatz dieser IDS ist als Alternative bzw. Ergänzung in bestimmten Szenarien denkbar.

Absicherung der Clients

Bei mobilen Clients sollten weitere Schutzmaßnahmen implementiert werden. Dies betrifft den Zugriffsschutz, die Benutzerauthentisierung, Virenschutz, Personal Firewall, Datei- und Ressourcen-Freigabe, lokale Verschlüsselung, etc.

7.3 Organisatorische Maßnahmen

In Kombination mit den beiden oben erwähnten Maßnahmen dienen die organisatorischen Maßnahmen zur Anhebung des Sicherheitsniveaus.

Sicherheitsrichtlinien aufstellen

Für den Einsatz von Funk-LAN-Komponenten sollten individuelle Sicherheitsrichtlinien aufgestellt werden. Diese sollten konform zum generellen Sicherheitskonzept der betroffenen Institution sein und regelmässig geprüft und ggf. aktualisiert werden. Zusätzlich sollten die Nutzer des WLAN-Netzes auf die Gefährdungen hingewiesen werden.

Einhaltung der Sicherheitsrichtlinien

Die Einhaltung der Richtlinien sollte ständig kontrolliert werden. Dies wäre über regelmässige Kontrollen der Access Points und Clients per Sniffer und Analyser oder durch die Auswertung der Log-Files des Access Points möglich.

Schutz personenbezogener Daten

Als Nutzer von öffentlich zugänglichen WLAN-Netzen sollte man sich vergewissern, dass der Anbieter datenschutzkonform mit den personenbezogenen Daten umgeht.

Nach Verabschiedung des Standards 802.11i soll eine robustere Sicherheitsarchitektur verfügbar sein. Diese Architektur gliedert sich in zwei Teile:

- Vertraulichkeit und Integrität
Hier wird ein neues auf AES (Advanced Encryption Standard) basierendes Protokoll angeboten, sowie eine auf WEP basierende Kompatibilitätslösung namens TKIP (Temporal Key Integrity Protocol).
- Authentisierung und Schlüsselmanagement
Diese Protokolle werden auf dem Standard IEEE 802.1X basieren

7.4 Ausblick

Basierend auf den Drafts von IEEE 802.11i sollte TKIP und 802.11X von der Wifi-Alliance unterstützt werden. Dies geschah unter dem Namen Wifi Protected Access, kurz WPA. WPA ist eine zu 802.11i aufwärtskompatible Zwischenlösung. Zur Behebung der grossen Schwächen wurden neue sicherheitsrelevante Lösungen eingeführt. Diese sind ein erweiterter Initialisierungsvektor, eine dynamische Schlüsselerzeugung pro Datenpaket und ein kryptographischer Message Integrity Check, kurz MIC namens Michael, der zusätzlich zur Integritätssicherung eingesetzt wird.

Allerdings sind auch bei WPA bereits neue Schwachstellen bekannt geworden. Entdeckt der Access Point bspw. einen Angriff in Form von gefälschten Paketen, werden alle Verbindungen getrennt und der Access Point versetzt sich für eine Minute in einen inaktiven Modus. Dadurch steht die Tür für DOS-Attacken mit Hilfe von gefälschten Paketen offen.

Eine weitere Schwachstelle von WPA ist der Kompatibilitätsbetrieb eines Access Points mit WPA und WEP. Alle WPA Clients kommunizieren zwar über WPA mit dem Access Point, allerdings werden Multi- und Broadcast-Nachrichten grundsätzlich über WEP verschlüsselt. Da nicht-WPA-fähige Clients in der Regel auch nicht 802.1X kompatibel sind, kann die Authentisierung und der dynamische Schlüsselwechsel umgangen werden. Aus diesem Grund sollte der Kompatibilitätsmodus deaktiviert werden.

Nichtsdestotrotz ist das Sicherheitsniveau von WPA um einiges höher einzustufen als das von WEP.

8 Fazit

Im momentanen Status ist WLAN in Verbindung mit WEP keine sichere Lösung. Die erschreckenden Sicherheitslücken sind vor allem für Firmen inakzeptabel. Der 1999 verabschiedete Standard wurde schon zwei Jahre später über eine FMS-Attacke geknackt, und das vor dem eigentlichen Einsatz in der breiten Masse. Der Grund für die Lücken ist vermutlich die in Bezug auf Sicherheit blauäugige Implementierung, da der Focus mehr auf Einfachheit und Performanz gerichtet war.

Eine sinnvolle Verbesserung der Sicherheit wäre eine Ausweichung auf die im vorigen Kapitel angesprochenen Lösungen, also bspw. Tunneling. Allerdings sind solche Lösungen für den Home-Office-Bereich noch zu teuer und teilweise auch zu komplex zu installieren.

Ein weiterer Punkt ist, dass es jedem halbweg versierten User möglich ist, anhand im Internet erhältlicher Tools einen Angriff auf ein WLAN-Netz zu starten.

Eines der Hauptprobleme liegt aber immer noch an dem auch in Firmen weit verbreiteten Glauben, dass die WEP-Verschlüsselung vor Datenspionen ausreichend Schutz bieten würde.

9 Referenzen

zum Nachlesen:

- WLAN-Standard - <http://grouper.ieee.org/groups/802/11/>
- 'Weakness in the key scheduling algorithm of RC4' von Fluhrer, Martin und Shamir - <http://downloads.securityfocus.com/library/>
- Bundesamt für Sicherheit in der Informationstechnik - www.bsi.de
- comp.security.misc
- comp.os.linux.networking
- comp.security.firewalls

Tools:

- Kismet - www.kismetwireless.net
- Wellenreiter - www.wellenreiter.net
- Aircrack-ng - aircrack-ng.org
- WepCrack - sourceforge.net/projects/wepcrack