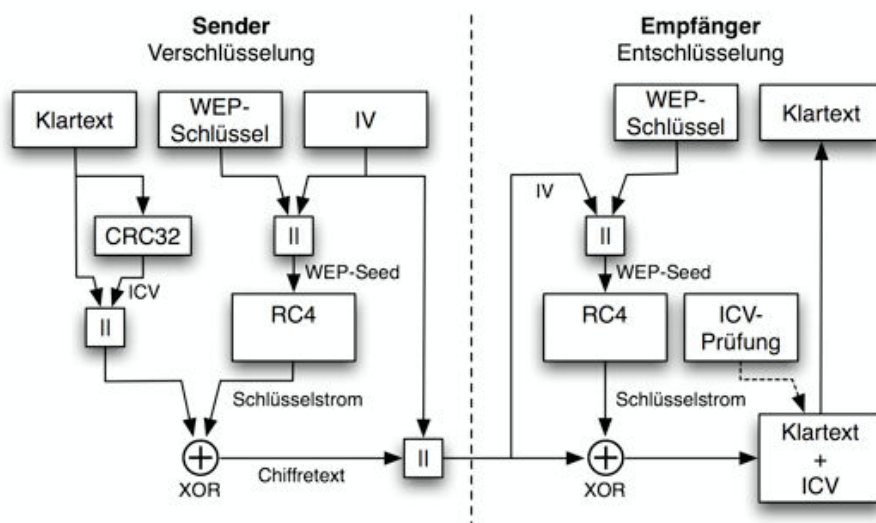




Handout Kryptographie

WEP-Verschlüsselung



Modul: TeKRYP		Datum: 19. Mai 2010
	Name:	E-Mail:
Verfasser:	Marco Costa	marco.costa@tet.htwchur.ch
Dozent:	Hermann Knoll	hermann.knoll@htwchur.ch
 HTW Chur Hochschule für Technik und Wirtschaft  Fachhochschule Ostschweiz University of Applied Sciences		

Inhaltsverzeichnis

1 Einleitung	3
2 WLAN.....	4
2.1 WLAN-Typen	4
2.2 Sicherheitsanforderung an Netzwerke	5
2.3 Verschlüsselungsmethoden.....	7
3 WEP-Algorithmus	9
3.1 CRC-32	9
3.2 RC4	10
3.3 Kryptographische Aspekte.....	11
3.4 Sicherheitsmängel	12
Abbildungsverzeichnis.....	
Quellenverzeichnis	

1 Einleitung

„Heutzutage gibt es viele Technologien, welche die Übertragung von Daten per Funk ermöglichen. Eine der wichtigsten und bekanntesten ist das Wireless Local Area Network (WLAN). Die Verbindung zwischen mehreren Rechnern, welche über ein Drahtlosnetzwerk miteinander verbunden sind, wird normalerweise verschlüsselt. Damit verhindert man, dass Drittpersonen über persönliche Daten, wie Passwörter oder wichtige Dokumente, zugreifen können. Grundsätzlich gibt es zwei Methoden um den Datenverkehr zu verschlüsseln: WEP und WPA.“ [1]

Diese Arbeit basiert auf der Studienarbeit drei „Angriffe auf WLANs mit Aircrack-ng“, die ich im dritten Semester an der HTW Chur geschrieben habe. Die Ziele für die Studienarbeit drei waren: Die Funktionsweise eines WLAN verstehen, das Programm Aircrack-ng Suite unter Linux-Umgebung bedienen können und wie man ein WLAN richtig konfiguriert. Aus Zeitgründen konnte ich die Funktionsweise des WEP-Algorithmus nicht unter die Lupe nehmen. Somit ist diese Arbeit als eine Ergänzung zur Studienarbeit drei zu verstehen, bei der ich spezifisch die mathematischen Grundlagen der WEP-Verschlüsselung erkläre.

Im ersten Teil dieser Arbeit wird das Wichtigste von der Studienarbeit 3 zusammengefasst und im 3. Kapitel wird das Thema WEP-Verschlüsselung vertieft.

Die Ziele dieser Arbeit sind:

- Die kryptografische Seite der WEP-Verschlüsselung zu verstehen
- Funktionsweise der CRC-32 und RC4 Algorithmen verstehen
- Schwachstellen von WEP erläutern

2 WLAN

Die WLAN Technologie ist eine der am meist verwendeten Funktechniken um Daten zu übertragen. Heute wird es immer stärker in der Industrie und in privaten Haushalten eingesetzt. Eine drahtlose Verbindung muss gewisse Anforderungen haben, um die Sicherheit der Netzwerke zu gewährleisten. Diese sind im Sicherheitsmanagement eines Netzwerkes definiert. Das Sicherheitsmanagement soll fünf Ziele erfüllen. Das sind die Datenintegrität, die Verfügbarkeit, die Vertraulichkeit, die Verbindlichkeit und die Authentizität. Diese Begriffe werden unter dem Kapitel 2.2 erläutert.

2.1 WLAN-Typen

Die WLAN-Technik für drahtlose Übertragung von Daten wurde vom „*Institute of Electrical and Electornics Engineers IEEE*“ im Standard 802.11 definiert. „Bis heute gibt es fünf verschiedene Haupt-WLAN-Typen:

IEEE-802.11 Ist im Jahr 1997 entstanden. Der Datentransfer liegt zwischen 1 und 2 MBit/s und arbeitet auf den Frequenzen von 2,400 bis 2,485 GHz. Es gibt 13 verschiedene Kanäle in Europa, die auf dem Frequenzbereich verteilt sind. Zum Beispiel arbeitet der Kanal sechs auf der Frequenz 2,437 GHz. Ein wesentlicher Anteil ist der Frequenzbereich, da auch andere Geräte wie Bluetooth auf den gleichen Frequenzen angesiedelt sind und das zu Störungen führen kann.

IEEE-802.11a WLAN Standard vom Jahr 1999 arbeiteten im 5 GHz (5,180 bis 5,835 GHz) Bereich. Die Reichweite liegt zwischen 10-25 Metern bei einem maximalen Datentransfer von 54 MBit/s. Aber in der Praxis läuft die netto Geschwindigkeit nur rund 20-22 MBit/s.

IEEE-802.11b Wurde im gleichen Jahr wie das IEEE-802.11a standardisiert aber arbeitet im Bereich von 2,4 GHz (2,400 bis 2,4835 GHz) und hat eine geringe Übertragungsrate von 11 MBit/s (netto 5-6MBit/s). Die Vorteile dieses Standards sind seine höhere Reichweite von bis zu

250-300 Metern (Outdoor) und seine Kompatibilität zum IEEE-802.11g. Dieser Standard hat den gleichen Nachteil wie der IEEE-802.11. Trotzdem ist seine Nutzung heutzutage noch ziemlich verbreitet.

IEEE-802.11g Nach vier Jahren (2003) wurde ein neuer Standard erlassen, der auf dem gleichen Frequenzband wie sein Vorgänger arbeitet aber mit einem höheren Datentransfer von 54 MBit/s (netto 20-22 MBit/s). Heutzutage ist dieser WLAN-Typ am weitesten verbreitet. Die Reichweite ist gleich wie die des IEEE-802.11b. Der Vorteil ist, dass er mit dem Vorgänger Standard kompatibel ist, d.h. die Netzwerkkarten von Typ IEEE-802.11b können problemlos mit einem Access Point IEEE-802.11g kommunizieren.

IEEE-802.11n Wurde schon im Jahr 2006 in verschiedenen Geräten eingebaut aber wurde nicht als IEEE-Standard angenommen. Erst am 11. September 2009 wurde dieser Standard ratifiziert. Der Datentransfer liegt auf 600 MBit/s (netto 100-120 MBit/s) und arbeitet auf dem Frequenzband von 2,400 bis 2,485 GHz und optional kann es auch auf 5 GHz als zusätzliches Band arbeiten.

Zusätzlich gibt es noch Variationen von diesen IEEE-Standards. Zum Beispiel existiert auch der IEEE-802.11h Standard, wo die Reichweite vom IEEE-802.11a verbessert wurde.“ [1]

2.2 Sicherheitsanforderung an Netze

Datenintegrität: Während der Übertragung von Daten auf einem Trägersignal passiert oft, dass äussere Störungen den Bitstrom beeinflussen oder die Pakete werden durch einen Angreifer manipuliert. Folglich ist das Datenpaket unbrauchbar. Das Sicherheitsmanagement muss die Integrität der Datenpakete gewährleisten und das wird durch eine Prüfsumme erreicht. In der WEP-Verschlüsselung wird das „Cyclic Redundancy Check 32“ (CRC-32) Verfahren angewendet. Dieses Verfahren wird im

Kapitel 3.1 erklärt. Für eine grössere Sicherheit werden auch Hash-Funktionen als Prüfsumme verwendet.

Verfügbarkeit: Als Verfügbarkeit wird die Zeit wenn ein System online ist bezeichnet. Die Verfügbarkeit eines Systems wird folglich berechnet: $(\text{Gesamtzeit} - \text{Gesamtausfallzeit}) / \text{Gesamtzeit}$. Sie wird vermindert durch Angriffe wie DOS (Denial-of-Service) z.B: Ein Angreifer sendet ein starkes Störsignal auf den Frequenzbereich des Funknetzes. Dadurch entsteht eine Überlagerung zwischen dem Störsignal und dem Nutzsignal. Somit ist das Nutzsignal beim Empfangen nicht rekonstruierbar.

Vertraulichkeit: Ein WLAN-Gerät strahlt in jede Richtung bis zu 300 Meter. So hat jede Person die Möglichkeit die Daten, die zwischen zwei Teilnehmer vertauscht werden, zu empfangen. Das Sicherheitsmanagement muss an Dritte keine Informationen aus den Paketen gewinnen können und das wird realisiert durch die Verschlüsselung der Pakete, die über das Trägersignal geschickt werden. In der Praxis werden das WEP- und WPA-Algorithmus eingesetzt.

Authentizität: Unter diesem Begriff versteht man, dass die Identität der Teilnehmer eines Funknetzes sichergestellt wird. Bei WEP-Verschlüsselung gibt es zwei Arten von Authentifizierung und zwar *Open System Authentication* und *Shared Key Authentication*. Mehr Informationen darüber finden Sie im Kapitel 2.1 meiner Studienarbeit 3 (<http://www.hitech-blog.com/htw/angriffe-auf-wlans-mit-aircrack-ng-tutorial/>). In Kürze muss der Teilnehmer sich mit dem WEP-Schlüssel am Funknetz anmelden.

Verbindlichkeit: Die Steigerung der Forderung nach Authentizität wird durch die Verbindlichkeit erweitert. Hier wird nicht nur die Identität des Teilnehmers sichergestellt, sondern der Teilnehmer kann auch das Senden von übertragenen Daten nicht verheimlichen. [2]

2.3 Verschlüsselungsmethoden

„Durch Verwendung der Verschlüsselung des WLANs wird verhindert, dass externe Personen auf private Daten zugreifen. Normalerweise unterstützt ein WLAN-Gerät zwei Verschlüsselungsmethoden: WEP und WPA/WPA2.

WEP (Wired Equivalent Privacy):

Funktionsweise:

WEP verwendet ein symmetrisches Verschlüsselungsverfahren d.h. der gleiche Schlüssel wird zur Verschlüsselung und Entschlüsselung verwendet. Der Schlüssel kann 40 Bit oder 104 Bit sein. Je höher, desto sicherer ist er. Wenn man von WEP-Verschlüsselung spricht, muss man sich vorstellen, dass die Daten durch einen Bitstrom übertragen werden.

Verschlüsselung: Ein WEP-Datenpaket besteht immer aus zwei Teilen. Der erste Teil ist der Initialisierungsvektor (IV) von 24 Bit und der zweite der chiffrierte Text. Der chiffrierte Text stammt aus einer XOR-Verknüpfung von zwei Eingängen. Der IV mit dem WEP-Key (40 oder 104 Bit) werden durch den Algorithmus RC4 durchgelaufen und seine Ausgabe dient als erster Eingang für die XOR-Verknüpfung. Als zweiter Eingang wird aus dem Klartext und einem 32 Bit Checksumme (IC) zusammengesetzt. Jetzt kann die XOR-Verknüpfung bitweise arbeiten und ihr wird der chiffrierte Text zurückgegeben. Nachher wird das Paket über eine Funkverbindung geschickt.

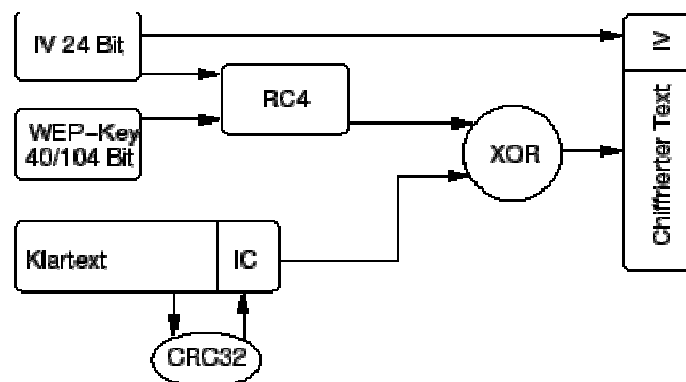


Abb. 1: Funktionsweise von WEP – Verschlüsselung (Quelle: <http://www.schorschi.org/dipl/img9.png>)

Entschlüsselung: Hier kommt das verschlüsselte Paket an und muss entschlüsselt werden. Zuerst braucht man den 24 Bit Initialisierungsvektor und den WEP-Key, wo der IV aus dem ersten Teil des Pakets herauslesen kann. Nachher werden sie wieder den RC4 durchlaufen und an die XOR-Verknüpfung geschickt. Hier wird der chiffrierte Text und die Ausgabe des RC4s bitweise verknüpft und als Ergebnis erhalten wird der Klartext mit dem Checksumme.

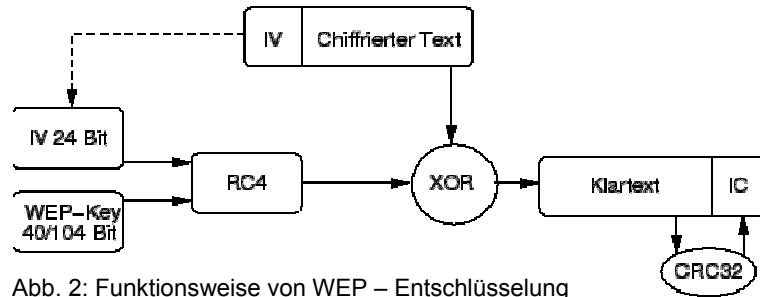


Abb. 2: Funktionsweise von WEP – Entschlüsselung
(Quelle: <http://www.schorschi.org/dipl/img10.png>)

Aufbau eines WEP-Paketes

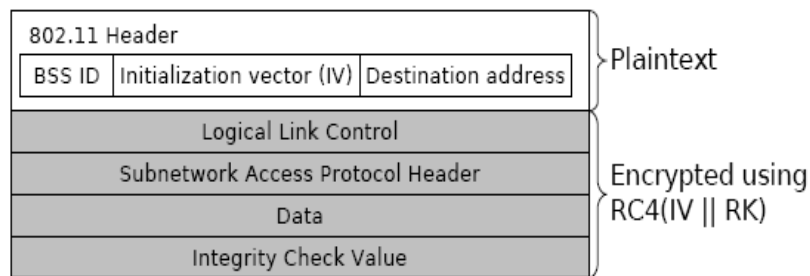


Abb. 3: Aufbau eines WEP-Paketes (Quelle: <http://eprint.iacr.org/2007/120.pdf>)

WPA/WPA2 (Wi-Fi Protected Access) enthält die gleiche Architektur von WEP. WEP-Verschlüsselung verwendet das TKIP Protokoll (Temporal Key Integrity Protocol), welches das WEP mit einem stärkeren Verschlüsselungsalgorithmus ersetzt: Neben dem IV wird auch Per-Packet-Key-Mixing-Funktion, einen Re-Keying-Mechanismus sowie einen Message Integrity Check (MIC) benutzt. Advanced Encryption Standard (AES) wird von WPA2 unterstützt und das ermöglicht eine höhere Sicherheit des WLANs.“ [1]

Heutzutage wird die WEP-Verschlüsselung wegen ihrer Schwachstelle nie eingesetzt und sie wird in den neuen Access Points nicht mehr implementiert (z.B. Airport Extreme von Apple). Hingegen ist die WPA-Verschlüsselung noch heute als eine sichere Verschlüsselung eingestuft. Aircrack ist fähig nur mit einer Brute Force Attacke den WPA-Schlüssel herauszufinden aber dieser Art von Attacke dauert zu lang.

3 WEP-Algorithmus

In diesem Kapitel sind am Anfang zwei andere Algorithmen zu finden, die eine wesentliche Rolle für die WEP-Verschlüsselung spielen. Danach wird in den Unterkapiteln 3.3 und 3.4 wieder die Funktionsweise der WEP-Verschlüsselung unter die Lupe genommen, aber dieses Mal unter dem kryptografischen Aspekt.

3.1 CRC-32 (Cyclic Redundancy Check 32)

„Cyclic Redundancy Check“ (CRC) oder auf Deutsch „zyklische Redundanzprüfung“ ist ein Fehlerprüfverfahren und es wird in der WEP-Verschlüsselung eingesetzt um die Integrität der Datenpakete zu gewährleisten. Die Version CRC-32 bedeutet, dass für die Erzeugung der Prüfsumme dem Datenblock bitweise mit dem Modulo Polynom 32. Grades ($x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$, 10000'0100'1100'0001'0001'1101'1011'0111) dividiert wird, wobei ein Rest bleibt. Mit diesem Verfahren können Bitfehlern erkannt aber nicht korrigiert werden.

Funktionsweise:

Erzeugung der Prüfsumme: Der Datenblock (Bitfolge) wird am Anfang um n-Bits (n=Grades des Polynoms) ergänzt. Danach wird die Bitfolge mit mod(Polynom) dividiert. Das wird realisiert durch eine XOR Verknüpfung.

Beispiel:

- Datenblock: 11011
- Polynom 5. Grades: $x^5 + x^4 + 1x^2 + 1 = 110101$

```

1101100000
110101
-----
0000110000
   110101
   -----
      101 (Rest / Prüfsumme)

```

Beim Übertragen der Information wird dem Datenblock der Rest angehängt. In diesem Beispiel wird die Bitfolge 1101100101 übertragen.

Kontrolle auf Integrität des Datenblocks beim Empfangen:

Hier wird die Bitfolge mit dem gleichen Polynom dividiert. Wenn der Rest gleich null ist, bedeutet, dass die Daten richtig übermittelt wurden.

Empfangene Bitfolge: 1101100101

```

1101100101
110101
-----
      110101
      110101
      -----
          000000
    
```

Eine Schwäche von CRC ist seine Linearität, deshalb ist es nicht verwendbar für kryptographische Zwecke: $CRC(M1)+CRC(M2) = CRC(M1 +M2)$. [5,6]

3.2 RC4 (Ron's Code 4)

RC4-Algorithmus ist ein einfacher Stromchiffre und er dient als Kern für die WEP- und WPA-Verschlüsselung. RC4 wird auch für die Protokolle HTTPS und SSH-1 verwendet. „RC4 wurde 1987 von Ronald L. Rivest entwickelt, ist eine Marke von RSA Security und offiziell geheim (Security by Obscurity). ARC4 (Alleged RC4) oder Arcfour geht auf eine anonyme Veröffentlichung von Quelltext im Jahr 1994 zurück und ist Open Source.“ [7]

RC4-Algorithmus generiert eine Bitfolge (Keystream) und das wird mit den Daten XOR verknüpft, so erhält man den Ciphertext. Um den Keystream zu generieren braucht der Algorithmus einen Schlüssel als Parameter $RC4(\text{WEP-Schlüssel} || \text{IV})$ und dieser Schlüssel kann maximal 128 Bit (WEP-Schlüssel + IV) Wortbreite haben. [7]

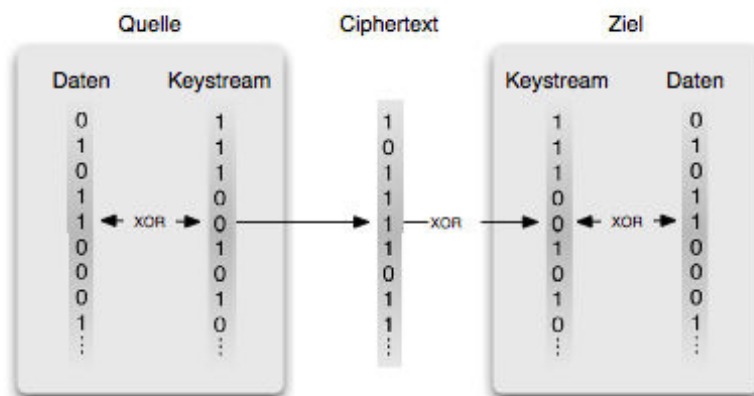


Abb. 3: RC4 (Quelle: http://sarwiki.informatik.huberlin.de/Image:RC4_grob.png)

3.3 Kryptographische Aspekte

Ablauf der WEP-Verschlüsselung:

1. WEP-Schlüssel $KBBS$ (*Key Bulletin Board System*¹) muss bekannt sein
2. Die Prüfsumme vom Datenblock M wird generiert und angehängt: $M' = M \parallel CRC(M)$,
 $M' = ICV$ (Integrity Check Value)
3. Der Keystream K wird durch WEP PRNG (pseudo random number generator - PRNG) erzeugt: $K = RC4(KBBS')$ wobei $KBBS' = KBBS \parallel IV^2$. Initialisierungsvektor (IV) wird immer zufällig gewählt.³
4. Datenblock wird verschlüsselt: C (Ciphertext) = $M' \text{ XOR } K$
5. Übertragung per Funk: $IV \parallel C$

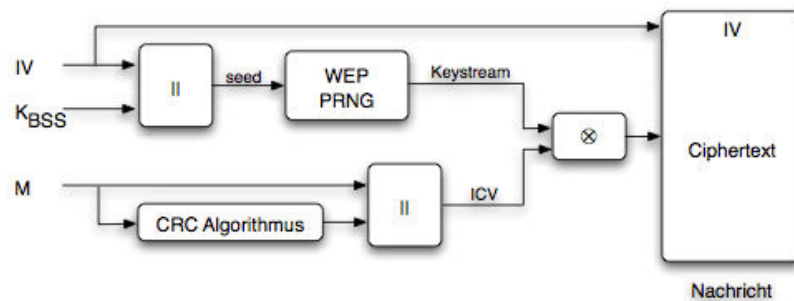


Abb. 4: WEP – Verschlüsselung (Quelle http://sarwiki.informatik.hu-berlin.de/Image:WEP_Kodierung.png)

Ablauf der WEP-Entschlüsselung:

1. Der Keystream K wird erzeugt. IV wird immer im Klartext übertragen und $KBBS$ ist bekannt: $K = RC4(KBBS')$ wobei $KBBS' = KBBS \parallel IV$
2. Der Chipertext wird entschlüsselt: $M' = C \text{ XOR } RC4(KBBS')$
3. Integrität des Datenblocks wird geprüft. [4]

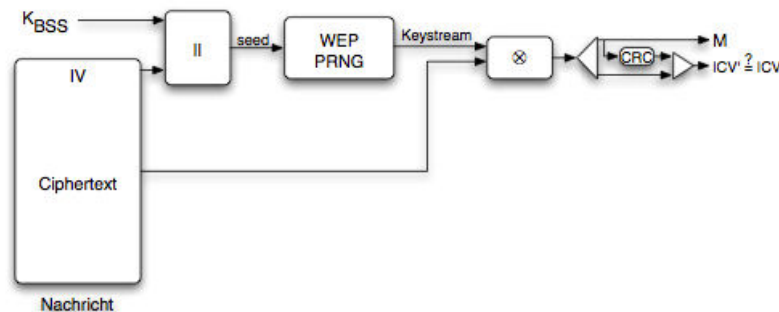


Abb. 5: WEP – Entschlüsselung (Quelle: http://sarwiki.informatik.hu-berlin.de/Image:WEP_Dekodierung.png)

¹ BBS ist der Access Point

² Das Symbol || bedeutet die Zusammensetzung von zwei Elementen: $111 \parallel 101 = 111101$

³ IVs werden anhand eines feststehenden Algorithmus generiert. Normalerweise werden sie um 1 inkrementiert

3.4 Sicherheitsmängel

„Beim Einsatz des WEP-Verschlüsselungsalgorithmus bei drahtlosen Netzwerken dachte man, dass es unknackbar sei. Aber in den letzten Jahren haben viele WLAN-Forscher bewiesen, dass diese Verschlüsselungsmethode Schwachstellen enthält. Beim Mitschneiden von chiffrierten Datenpaketen ist es möglich, den WEP-Schlüssel zu berechnen.“ [1]

Gründe dafür sind:

- Linearität des RC4 Algorithmus
- Den gleichen WEP-Schlüssel wird für alle Teilnehmer verwendet
- WEP-Schlüssel ist zu kurz
- IVs sind zu kurz
- RC4 ist ein lineares System

Eine Nachricht $M1$ wird mittels RC4 verschlüsselt und geschickt: $C1 = M1 \text{ XOR } RC4(KBBS+IV)$. Danach wird eine weitere Nachricht $M2$ mit dem gleichen WEP-Schlüssel verschlüsselt und gesendet: $C2 = M2 \text{ XOR } RC4(KBBS+IV)$. Ein Angreifer ist im Besitz von $C2$, $C1$ und $M1$. Wegen der Linearität des RC4 kann er $M2$ berechnen und zwar: $M2 = (C1 \text{ XOR } C2) \text{ XOR } M1$. [3,4]

```

M1=1100          C1=1100 XOR 0101 = 1001
M2=1000          C2=1000 XOR 0101 = 1101
Keystream=0101

M2= (1001 XOR 1101) XOR 1100 = 1000

```

In der Studienarbeit 3 „Angriffe auf WLANs mit Aircrack-ng“ verwendet das Tool Aircrack eine andere Attacke. Diese Attacke heisst PTW und der Angreifer muss nur 40'000 Pakete für eine Erfolgswahrscheinlichkeit von 50% empfangen, somit kann der PTW-Algorithmus den WEP-Schlüssel berechnen. Dieses Verfahren wird in dieser PDF-Datei (<http://eprint.iacr.org/2007/120.pdf>) gut geklärt. In Kürze nützt die PTW-Attacke (Andrei Pyshkin, Erik Tews and Ralf-Philipp Weinmann) die Schwachstelle (Korrelationen zwischen Keystream und WEP-Schlüssel) von RC4 aus.

Abbildungsverzeichnis

Abb. 1: Funktionsweise von WEP – Verschlüsselung	7
Abb. 2: Funktionsweise von WEP – Entschlüsselung.....	8
Abb. 3: RC4.....	10
Abb. 4: WEP – Verschlüsselung.....	11
Abb. 5: WEP – Entschlüsselung.....	11

Quellenverzeichnis

- [1] Marco Costa: Angriffe auf WLANs mit Aircrack-ng, 2009 [<http://www.hitech-blog.com/htw/angriffe-auf-wlans-mit-aircrack-ng-tutorial/>]
- [2] Wikipedia: Wireless Local Area Network, gefunden am 20. April 2010 [<http://de.wikipedia.org/wiki/Wlan>]
- [3] Jörg Hedrich: Seminar Net Security, Sicherheit im WLAN, gefunden am 20. April 2010 [<http://www.uni-koblenz.de/~steigner/seminar-net-sec/sem8.pdf>]
- [4] Humboldt Universität Berlin Informatik, Wireless Risk Potential Scenario: WEP, gefunden am 21. April 2010 [http://sarwiki.informatik.hu-berlin.de/Wireless_Risk_Potential_Scenario:_WEP]
- [5] Wikipedia: Zyklische Redundanzprüfung, gefunden am 21. April 2010 [<http://de.wikipedia.org/wiki/CRC-32>]
- [6] Bruno Wenk, Arbeitsblatt: Cyclic Redundancy Code CRC (DKP), Version 1.1, 2010, HTW-Chur
- [7] Wikipedia, RC4, gefunden am 21. April 2010 [<http://de.wikipedia.org/wiki/Rc4>]