A.3 – The Final Nail in WEP`s Coffin

Alexander Lichti
(alexlichti@gmail.com)

Seminar “Internet Sicherheit”,
Technische Universität Berlin

WS 2006/2007 (Version vom 03.02.2007)

Zusammenfassung

Konzeptionelle Sicherheitsmängel beim Einsatz von 802.11’s optionalem Verschlüsselungsstandard *Wired Equivalent Privacy* (WEP) werden seit Jahren diskutiert. Diese Seminararbeit behandelt einen neu entwickelten Ansatz, um WEP verschlüsselte Netzwerke mit nur einem abgehörten Paket zu kompromittieren. Dies bedeutet, unbefugt Daten in das Netz zu senden sowie verschlüsselte Daten zu dekodieren. Unter speziellen Voraussetzungen ist es sogar möglich, verschlüsselte Datenpakete in Echtzeit zu dekodieren. Es soll verdeutlicht werden, dass WEP unsicher ist und die Anstrengungen verstärkt werden müssen, den Einsatz von WEP als Basisverschlüsselung in den meisten Netzwerken zu beenden. Das vorliegende Dokument bezieht sich in erster Linie auf den Aufsatz „The Final Nail in WEP`s Coffin“ von Bittau, Handley und Lackey [1]. In den Fällen, wo weitere Quellen verwendet wurden, ist dies explizit gekennzeichnet.

1. Einleitung

WEP ist trotz aller Sicherheitsmängel und einer breiten öffentlichen Diskussion darüber immer noch der de-facto Standard für verschlüsselte Funknetzwerke. Insbesondere im privaten Bereich wird er als ausreichende Sicherheitstechnik angesehen. Tabelle 1 gibt einen beispielhaften Überblick der prozentualen Verbreitung von WEP gegenüber anderen Technologien im Großraum London und Seattle.

Region	WEP	WPA	802.11i
London	76	20	4
Seattle region	85	14	1

Tabelle 1: Verbreitung von WEP im Großraum London und Seattle (in %)

Eine theoretische Einführung in die Grundlagen von WEP wird in Kapitel 2 gegeben. Damit soll dem Leser ohne entsprechende Vorkenntnisse die Möglichkeit gegeben werden, die danach vorgestellten Konzepte zu verstehen und einzuordnen.

Die erkennbaren Schwachstellen von WEP wurden bisher als nicht so bedeutsam aufgefasst, da nur eine Minderheit in der Lage war, die Verschlüsselung in der Praxis auch wirklich zu knacken. Dies ist auf die langen Wartezeiten zurückzuführen, die mit den herkömmlichen

Methoden benötigt wurden. Diese sogenannten *Keystream Based Attacks,* die auf eine Dekodierung den WEP-Keys abzielen, werden in Kapitel 3 vorgestellt.

Die von [1] entwickelten *fragmentation attacks* verkürzen die Zeit für einen erfolgreichen Angriff auf ein Funknetz auf Minuten und brauchen teilweise nur ein einziges Paket mitlesen. Sie bilden den Schwerpunkt dieser Seminararbeit und werden in Kapitel 4 beschrieben. Es geht hierbei um die theoretischen Konzepte und nicht um die bereits vorhandene technische Implementierung.

Kapitel 5 bietet eine Zusammenfassung der Ergebnisse.

2. Funktionsweise von WEP

Ziel von WEP ist es, ein Funknetzwerk auf Basis von IEEE 802.11 genauso sicher zu machen wie ein kabelgebundenes Netzwerk. WEP stellt dafür Funktionen für die Paketverschlüsselung und die Authentifizierung bereit. Dieses Kapitel beschreibt erst das Verschlüsselungsprinzip für Datenpakete und geht dann auf die Authentifizierungsverfahren ein.

2.1 WEP Verschlüsselung

Grundlage der Kodierung ist das RC4 Verfahren, siehe [3]. Hierbei wird eine Pseudozufallsbitfolge genutzt, um einen sogenannten *keystream* zu erzeugen. Mittels dieses Keystreams wird ein Ausgangstext (Plain text) in einen Ciphertext umgewandelt. Dieser Ciphertext kann nun übertragen werden. Um den Ausgangstext wieder herzustellen, muss der Empfänger den Ciphertext mit dem Keystream verknüpfen. Abbildung 1 aus [2] zeigt den Ablauf der Datenübermittlung.

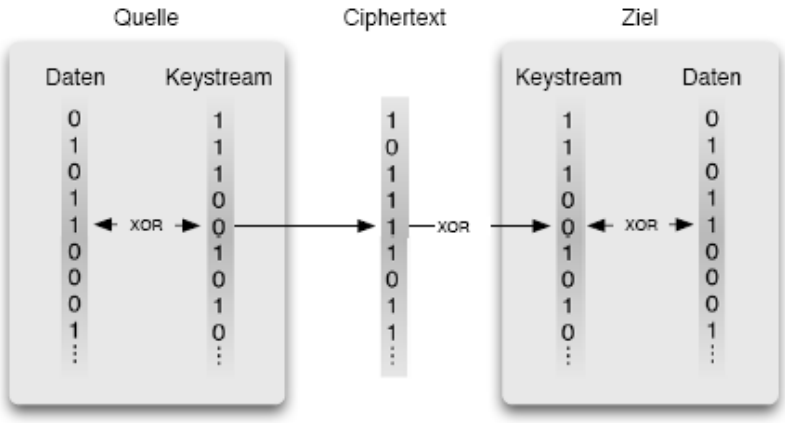

Abbildung 1: Übermittlung von Daten von der Quelle zum Ziel

2.2 Keystream

In WEP wird der Keystream anhand einer Wurzel (seed) gebildet, die aus einem *pre-shared-key* und einem Initialisierungsvektor (IV) besteht.

Der Key ist laut Standard ein 40-bit Vektor, allerdings werden heute üblicherweise 104-bit benutzt. Der Key ändert sich über die Zeit hinweg nicht, ist geheim und muss der Quelle sowie dem Ziel vor Beginn der Kommunikation bekannt sein.
Der IV dagegen ist öffentlich und wird in Klarschrift übertragen. Er ist 24-bit lang und wird zur Erzeugung des Keystreams dem Key vorangestellt, siehe Abbildung 2:

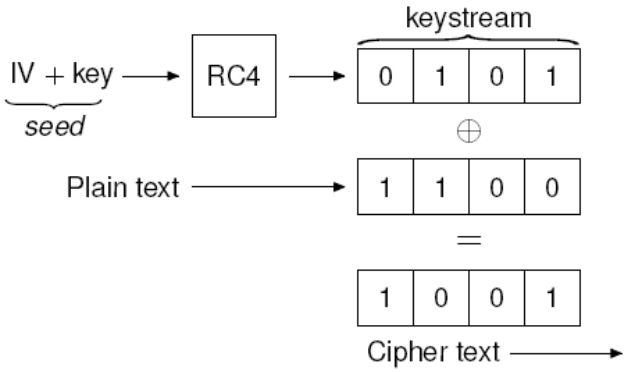

Abbildung 2: Erzeugen des Ciphertext mittels Keystream und Plaintext

Der Keystream sei im Folgenden auch mit RC4(IV, K) bezeichnet. Jeder neue, unterschiedliche IV produziert einen anderen Keystream, da sich die Wurzel für RC4 ändert. Daher können mit einem Key insgesamt 2^{24} verschiedene Keystreams erzeugt werden. Wie bereits gezeigt, wird der Keystream zusammen mit dem zu verschlüsselnden Klartext P benutzt, um den Ciphertext C mittels bitweiser XOR ($\oplus$) Verknüpfung zu erzeugen:

(1) $C = P \oplus RC4(IV, K)$

Umgekehrt kann der Klartext P durch eine Verknüpfung des Ciphtertext C mit dem Keystream RC(IV, K) ermittelt werden:

(2) $P = C \oplus RC(IV, K)$

Entscheidend für die Berechnung von RC(IV, K) ist es, den Klartext einer Nachricht zu kennen.

(3) $RC(IV, K) = P \oplus C$

Für die Verschlüsselung kann ein beliebiger Keystream verwendet werden, für die Entschlüsselung nur der über den IV spezifizierte Keystream.

Prinzipiell ist es möglich, denselben Keystream RC(IV, K) mit derselben IV für die Verschlüsselung mehrerer Pakete zu benutzen. Das ist allerdings nicht ratsam, da ein Angreifer dann sämtliche so kodierte Pakete mit nur einem entzifferten Keystream entschlüsseln kann.

2.3. Authentifizierungsverfahren

Die Authenifizierung unterscheidet zwei Verfahren:

- Die *Open System Authentification* ist die Standard-Authentifizierung. Damit ist das Funknetz für alle Clients offen und es gibt keine weitere Authentifizierung. Allerdings kann ein verbundener Netzwerkteilnehmer nur mit Kenntnis eines gültigen WEP-Schlüssels eine Kommunikation mit dem Access Point (AS) aufbauen.
- Die *Shared Key Authentification* ist die vermeintlich sichere Variante. Die Authentifizierung erfolgt über die Challenge-Response-Authentifizierung mit einem geheimen Schlüssel. Abbildung 3 aus [4] zeigt den Ablauf. Das Problem ist hier, dass das gesamte Verfahren auf WEP basiert, und der Key K entblößt wird. Darauf wird in Abschnitt 3.3 eingegangen.

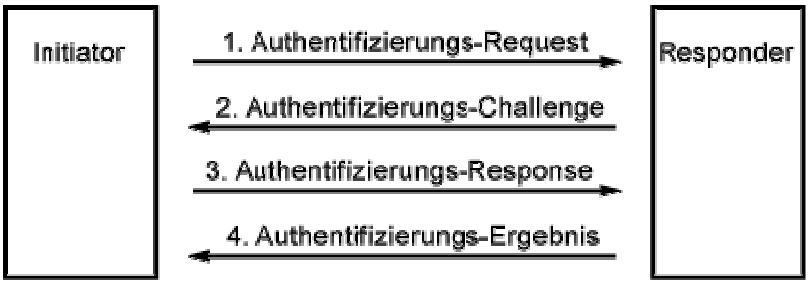

Abbildung 3: Handshaking bei der Shared Key Authentification

3. Basisverfahren zum Angriff auf WEP

In diesem Kapitel werden die Basisverfahren geschildert, die bislang in der einen oder anderen Form genutzt wurden, um WEP verschlüsselte Netze zu attackieren. Grundsätzlich geht es dabei darum, die im Netzwerk gesendeten Daten zu entschlüsseln oder auch unbefugt Daten in das Netz zu senden.

3.1. Brute-Force-Attacke

Die einfachste und gebräuchlichste Möglichkeit eines Angriffs auf ein WEP verschlüsseltes Netz ist die *Brute-Force-Attacke*. Diese versucht anhand bekannter Informationen den Schlüssel K zu berechnen. Grundvoraussetzung ist, das der Klartext der Nachricht bekannt ist. Dann kann mit dem Ciphertext anhand Formel (3) aus Abschnitt 2.2 der Schlüssel K berechnet werden, indem einfach alle möglichen Kombinationen durchprobiert werden.
Den im Standard spezifizierten 40-bit WEP Schlüssel zu knacken, ist in angemessener Zeit möglich. Die Verwendung von 104-bit Schlüsseln ist allerdings ein effektiver Schutz gegen Brute-Force-Attacken.

3.2 Keystream re-use

Eine Möglichkeit, einen Keystream verlässlich zu entdecken und Daten in das Netzwerk zu senden ist ein Angriff auf die *Shared Key Authentification.* Hierbei nutzt man einen konzeptionellen Fehler im Verfahren aus.

Wie gezeigt, funktioniert die Authentifizierung folgendermaßen:
- Der Server sendet dem Peer eine Klartext Anfrage (clear-text challenge)
- Der Peer antwortet, indem er die verschlüsselte Version der Anfrage zurücksendet

Wenn man als Angreifer die Kommunikation mithört (snooping), bekommt man damit den Ciphertext mit dem dazugehörigen Klartext. Nun kann mittels Formel (3) der Keystream ermittelt werden.
802.11 kennt dieses Szenario und rät dazu, bereits benutzte IVs für das hand-shaking (siehe Abbildung 3) nicht mehr zu benutzen. Allerdings ist es möglich, mit dem IV und dem zugehörigen Keystream beliebige Pakete ins Netz zu senden (Keystream re-use).

3.3 Weak IV Attacks

Frühe Studien über WEP zeigten bereits, dass der Schlüssel K berechnet werden kann. Für diesen Angriff benötigt man ungefähr 1.000.000 Pakete, bei denen Einige sogenannte „weak" IVs benutzen. Ein einziger *weak* IV enthüllt ein korrektes Schlüsselbyte mit ungefähr 5% Wahrscheinlichkeit. Indem man eine hohe Anzahl von IVs sammelt, kann der wahrscheinlichste Schlüssel berechnet werden. Mit dieser Möglichkeit können automatisierte Tools einen Key entschlüsseln. Allerdings ist dieser Angriff sehr aufwendig und führt nur unter speziellen Umständen zum Ziel [1].

4. Erweiterte Angriffsverfahren

Im letzten Kapitel wurden die traditionellen Möglichkeiten gezeigt, ein WEP Netz zu attackieren. Diese Verfahren zeigen zwar Schwachstellen von WEP, stellen diese Verschlüsselungstechnik jedoch nicht grundsätzlich in Frage.
Mit den jetzt vorgestellten „Layer 2 Fragmentation Attacks" sieht das anders aus. Sie zeigen den fundamentalen Designfehler in WEP: Der IEEE Standard 802.11 selbst kann gegen WEP genutzt werden! Der konzeptionelle Fehler liegt hierbei in der Fragmentierung von Datenpaketen wie in 802.11 spezifiziert:

4.1 Fragmentation in 802.11

802.11 spezifiziert die Fragmentierung von Paketen auf dem MAC-Layer so, dass jedes Fragment unabhängig verschlüsselt wird. Dabei ist es möglich, mehrere Fragmente (bis zu 16) mit demselben Keystream zu kodieren, siehe Abbildung 4.

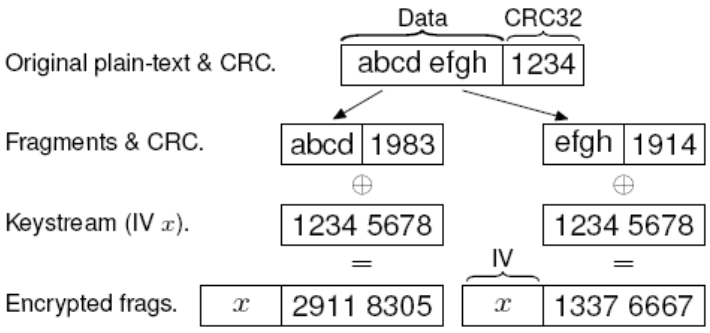

Abbildung 4: Fragmentierung eines Datenpakets

Was bringt diese Möglichkeit der Fragmentierung dem Angreifer? Nun, kennt er einen Teil des Keystreams, so kann er diesen nutzen, um schnell den kompletten Keystream zu dekodieren, wie später gezeigt. Der benötigte Teil des Keystreams kann dabei über bekannten Klartext in Paketen extrahiert werden:

4.2 Known Plain-text in Packets

802.11 *data frames* haben einen LLC/SNAP Header wie in Abbildung 4 dargestellt:

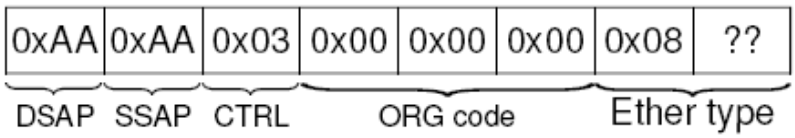

Abbildung 4: LLC/SNAP Header

Dieser ist praktisch immer gleich und beansprucht die ersten 8 Bytes eines Pakets. Das Feld für *Ethertype* ist entweder ARP oder IP. Da ein ARP Paket per Definition immer 36 Bytes hat, lässt sich leicht herausfinden, welches Protokoll benutzt wird. Somit sind die ersten 8 Byte bekannt.
Beim Mitlesen eines Datenpakets sind somit die ersten 8 Byte des Klartexts und des dazugehörigen Ciphertexts bekannt. Mit Formel (3) aus Abschnitt 2.2 wird leicht der Keystream ermittelt. Mit diesem Keystream kann man nun 8 Byte Daten senden. Die Nutzdaten setzen sich dabei aus 4 Byte Daten und 4 Byte Redundanzcheck (CRC32) zusammen.

Mittels dieser gewonnenen Informationen kann nun ein so genannter Pure Fragmentation Attack durchgeführt werden:

4.3. Pure Fragmentation Attack

Für ein Pure Fragmentation Attack muss das Netzwerk an das Internet angeschlossen sein. Darüber hinaus werden die MAC Adresse des Routers und die IP Adresse der Quelle benötigt. Siehe [1] für Techniken um diese leicht zu bekommen.
Wie gezeigt wird nun ein 8 Byte großer Keystream entschlüsselt.
Mit dieser Information können nun IP Header in jeweils 4 Byte großen Fragmenten erstellt werden. Diese werden dann zusammen mit dem abgehörten und benutzten Datenpaket ins Netz eingespeist, und zwar so, dass der Header vor das Paket „gesetzt“ wird.
Der Access Point (AP) sammelt nun die Fragmente, dekomprimiert diese und setzt sie zu einem neuen Datenpaket zusammen. Dann sendet der AP das Paket an die spezifizierte Internet Adresse in Klartext, da nur die Funkverbindung verschlüsselt ist. Kontrolliert der Angreifer das Ziel, kann er das Paket in Klartext lesen. Abbildung 5 verdeutlicht das Prinzip.

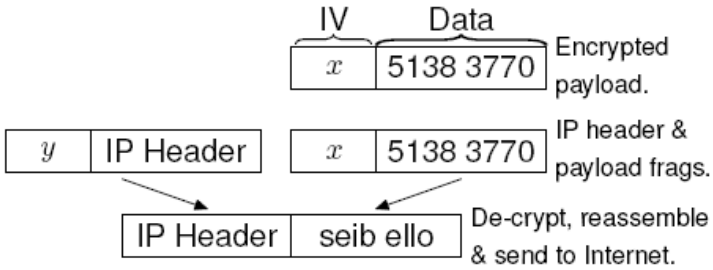

Abbildung 5: Entschlüsselung, in dem der AP genutzt wird, um das Datenpaket in Klartext in das Internet zu senden

In [1] werden noch verschiedene Möglichkeiten durchgespielt, wenn die mitgelesenen Datenpakete zu groß sind, um einfach eine IP-Adresse voranzustellen (Redirecting Maximum Transmission Units (MTU)). Ohne weiter DARAUF einzugehen, sei darauf hingewiesen, dass auch dies ohne großen Aufwand möglich ist.

4.4 Erweiterte Keystream Based Attacks

Dieser Abschnitt zeigt Erweiterungen der bisherigen Keystream Based Attacks durch die Nutzung der Fragmentierung.

4.4.1 Discovering Keystreams

Es ist auf einfache Art möglich einen vollständigen, 1500 Byte großen Keystream zu erzeugen.
Grundprinzip hierbei ist es, *Broadcast Frames* in kleinen Fragmenten zu senden.
Der AP dekodiert die frames, setzt die Fragmente wieder zusammen und kodiert sie in ein größeres Paket. Kennt man die frames, aus denen das neue Paket zusammengesetzt ist, so kennt man den Klartext und kann daraus den Keystream berechnen.

Ein Beispiel:
Wie gezeigt können 64 Bytes Nutzdaten in 16 8-Byte Fragmenten (4 Byte Nutzdate + 4 Byte CRC32) versendet werden. Der AP setzt diese Fragmente zu einem Paket der Größe 68 Byte zusammen (64 Byte + 4 Byte CRC32). Da der Klartext bekannt ist, können nun 64 Bytes in 16 Fragmenten gesendet werden, was in einem neuen Paket von 1028 Byte resultiert usw.
Somit kann fast sofort ein vollständiger Keystream aus einem einzigen Datenpaket produziert werden.
Um weitere vollständige Keystreams zu erzeugen, kann der Angreifer nun einfach Pakete unfragmentiert senden und die wiedergegebenen Pakete mitlesen. Dadurch kann recht schnell ein komplettes IV Dictionary erstellt werden, welches alle benutzen Keystreams beinhaltet. Theoretisch werden dazu etwa 2^{24} (16M) Pakete benötigt. In der praktischen Implementierung von WEP in den APs werden aber deutlich weniger Pakete benötigt.
Abbildung 6 zeigt das Prinzip:

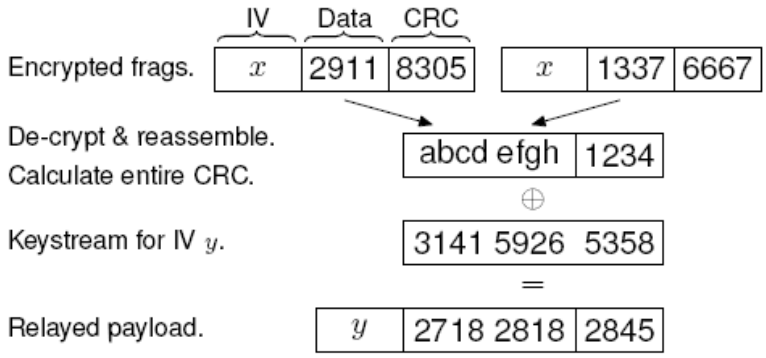

Abbildung 6: Entschlüsseln von Keystreams durch Fragmentierung und Broadcasting

4.4.2 Discovering a specific Keystream

Wenn ein Paket einen bekannten IV benutzt, so kann der Keystream über das IV Dictionary gefunden werden. Mit Formel (2) kann der Klartext gefunden werden.
Ist der Keystream nicht bekannt, so wird der Key für die ersten 8 Byte wie gezeigt ermittelt. Dann werden 256 Multicasts mit 9 Bytes gesendet, wobei das letzte Byte unterschiedlich ist. Dasjenige Paket, welches gültig ist, wird vom AP zurückgesendet. Damit kann das jeweils nächste Byte Schritt für Schritt ermittelt werden.

5. Zusammenfassung und Ausblick

Die in dieser Arbeit besprochenen Methoden zum Angriff auf ein WEP verschlüsseltes Netz zeigen eindeutig, dass WEP keinen effektiven Schutz vor Angriffen mehr bietet. Es zeigt, dass die Sicherheit eines Protokolls im Kontext eines Protokolls selbst designt werden muss. In diesem Fall ist es die Mehrfachverwendung von Keystreams (re-use) und die einfache, nicht geprüfte Fragmentierung von Paketen, die das gesamte Sicherheitskonzept obsolet werden lässt.
Durch das Ausnutzen der Fragmentierung, in Verbindung mit bekanntem Klartext von Paketen, kann ein Angreifer unter speziellen Umständen sämtlichen Verkehr in einem Netzwerk in Echtzeit entschlüsseln.
Darüber hinaus ist es ihm möglich, nicht nur einzelne Keystreams zu entschlüsseln sondern darüber hinaus auch komplette IV Dictionarys aufzubauen, mit denen verschlüsselte Pakete sofort anhand der übertragenenen IVs dekodiert werden können.
Im originalen Aufsatz von [1] wird auch die Implementierung und tatsächliche Ausführung der theoretischen Konzepte ausführlich besprochen. Es wird gezeigt, dass sämtliche Konzepte praxistauglich sind. So dauert es nach dem Mithören eines Paketes weniger als eine Minute, ein MTU-grosses Paket zu senden und die IP-Range für das lokale Subnetz zu kennen.

Literatur

[1] “The Final Nail in WEP`s Coffin“ von Bittau, Handley und Lackey

[2] http://www.uni-koblenz.de/~steigner/seminar-net-sec/sem8.pdf

[3] http://www.wisdom.weizmann.ac.il/~itsik/RC4/rc4.html

[4] http://www.elektronik-kompendium.de/sites/net/0905251.htm