

Wireless LAN (IEEE 802.11) Security Glossar

Bruno Blumenthal
wireless@blusk.net

15. Oktober 2003

Zusammenfassung

Dieses Dokument soll die gängigsten Begriffe zum Thema Security im Zusammenhang mit den IEEE 802.11 Wireless LAN Standards erklären. Es wurde verzichtet die Begriffe ins Detail zu erklären, der Glossar soll zusammenfassend und kurz gehalten sein.

Dieser Glossar erhebt keinerlei Anspruch auf Vollständigkeit und der Autor nimmt gerne Anregungen und Kommentare entgegen.

Inhaltsverzeichnis

1 WEP	3
1.1 RC4	3
2 Authentication	3
2.1 open system	3
2.2 shared-key	3
2.3 both	3
3 Angriffe auf WEP	4
3.1 IV-Reuse	4
3.2 FMS-Attacke	4
4 WEP Alternativen & Weiterentwicklungen	5
4.1 WPA & 802.11i	5
4.1.1 TKIP	5
4.1.2 802.1X (EAP)	5
5 SSID	6
5.1 SSID-Broadcast	6
5.1.1 BEACON-Frame	6
6 MAC-Adresse	6
6.1 MAC-Filter	6
7 Wireless Scanner/Sniffer	7
7.1 passiv	7
7.1.1 monitor-mode/promiscuous-mode	7
7.2 aktiv	7
A WEP	8
B RC4	9
C shared-key Authentication	9
D TKIP	10

1 WEP

Wired Equivalent Privacy; Wie der Name schon sagt soll WEP einen vergleichbaren Schutz gegen unerlaubtes Abhören bieten, wie dies bei einem kabelgebundenen Netzwerk der Fall ist. Da sich die Funkwellen frei ausbreiten, ist es mit geringem Aufwand möglich den Netzwerkverkehr abzuhören. Deshalb bietet der 802.11 Standard [6] mit WEP die Möglichkeit die Daten zu verschlüsseln. Leider hat das Design von WEP Fehler welche es ermöglichen die Verschlüsselung zu brechen, siehe dazu Abschnitt 3.

WEP ist gemäss Standard optional, wird aber heute in fast allen Geräten implementiert. WEP ist im Standard für eine Schlüssellänge von 40-Bit ausgelegt, heute stehen jedoch meist Versionen mit 40-Bit und 104-Bit, teilweise sogar 256-Bit, Schlüssellänge zur Verfügung. Die 104-Bit Variante wird meist mit 128-Bit bezeichnet, da für den RC4 Algorithmus 104-Bit Key + 24-Bit IV verwendet werden siehe Anhang A.

1.1 RC4

WEP basiert auf dem Verschlüsselungsalgorithmus RC4 [8] von Ron Rivest der RSA Data Security, Inc. Für die genaue Funktion von WEP und RC4 siehe Anhang A bzw. B

2 Authentication

IEEE 802.11 [6] bietet zwei Möglichkeiten zur Authentisierung der Clients *shared-key* und *open system*. Es besteht keine Möglichkeit um den AP zu authentisieren. Der Modus wird vom Client vorgeschlagen und der AP kann akzeptieren oder ablehnen. Die Authentisierung ist unabhängig von der Verschlüsselung.

2.1 open system

Open System ist das einfachere System, das keine Authentisierung vornimmt. d.h. jeder Client der sich anmelden will wird authentisiert und zugelassen.

2.2 shared-key

Für die shared-key Authentisierung muss eine WEP key definiert werden. Der Client wird mittels eines Challenge-Response Verfahrens, basierend auf dem WEP-Key authentisiert. siehe auch Anhang C

2.3 both

Einige AP erlauben den Modus 'both', dabei werden sowohl Clients zugelassen die sich mit open system wie auch shared-key anmelden wollen.

3 Angriffe auf WEP

Wie bereits erwähnt ist WEP leider mit einigen Fehlern entwickelt worden. WEP hat zwei grundlegende Schwächen welche es ermöglichen die Verschlüsselung zu knacken.

3.1 IV-Reuse

Weil RC4 als Stream-Cipher anfällig ist auf Synchronisationsfehler und bei einer Funkübertragung eine hohe Fehlerwahrscheinlichkeit herrscht, wurde entschieden, dass der Stream für jedes Paket neu initialisiert wird. Dieser "Missbrauch" von RC4 führt zu einem fatalen Problem. Das grundlegende Problem liegt darin, dass bei einer Stream-Cipher wie RC4 niemals derselbe Strom zweimal verwendet werden darf. Weil der Plaintext nur mit dem Schlüssel-Strom per XOR verknüpft wird und gilt

wenn:

$$C_1 = P_1 \oplus RC4(v, k)$$

$$C_2 = P_2 \oplus RC4(v, k)$$

dann gilt:

$$C_1 \oplus C_2 = (P_1 \oplus RC4(v, k)) \oplus (P_2 \oplus RC4(v, k)) = P_1 \oplus P_2$$

Da der Schlüssel statisch bleibt, unterscheiden sich die verschiedenen Schlüsselströme nur durch den IV. Da der IV Raum nur $2^{24} = 16777216$ beträgt, tritt jedoch relativ rasch eine Wiederholung des IV ein. Wenn der Angreifer nun zwei Pakete mit dem selben IV hat kann er einen Angriff starten. Dieser wird dadurch erleichtert, dass sich im Netzwerkverkehr viele bekannte Muster in den Paketen finden (z.B. Headerinformationen). Wenn ein Paket einmal entschlüsselt ist kann wiederum die entsprechende Schlüsselstrom-Folge ermittelt werden. Diese kann später verwendet werden um bei einem erneuten auftauchen des IV sofort das Paket zu entschlüsseln. [2]

Dieser Angriff ist zwar praktikabel jedoch sehr aufwändig.

Mit diesem Angriff ist es NICHT möglich den WEP-Key zu ermitteln.

3.2 FMS-Attacke

Diese Attacke ist viel wirkungsvoller, aber auch erheblich komplizierter zu verstehen, sie wurde von Scott Fluhrer, Itsik Mantin, and Adi Shamir entdeckt [3]. Sie nutzt eine Schwäche im Key Scheduling Algorithmus aus. Die Attacke basiert darauf, dass das erste word des Key-Streams überproportional vom Schlüssel abhängt. Es ist daher möglich eine statistische Aussage zu machen über den Schlüssel. Wenn wir genügend Pakete sammeln können wir die möglichen Schlüssel immer mehr einengen und letztendlich erhalten wird den Schlüssel. Das ganze ist sehr mathematisch und ich verzichte darauf es hier im Details zu erläutern.

WEPCrack und *AirSnort* basieren auf dieser Attacke und könne in verhältnismässig kurzer Zeit (5-10 Mio Pakete) den Schlüssel ermitteln. [9]

4 WEP Alternativen & Weiterentwicklungen

Wie bereits weiter oben erwähnt bietet WEP durch diverse Fehler beim Design Angriffspunkte, die es einem Angreifer ermöglichen die Verschlüsselung zu brechen, siehe Abschnitt 3. Aus diesem Grund wird bereits intensiv an Erweiterungen und Alternativen für WEP gearbeitet.

4.1 WPA & 802.11i

Wi-Fi Protected Access [11], soll die Schwächen von WEP beheben. Es wurde von der WiFi-Alliance entwickelt, einer Gruppe von verschiedenen Herstellern. Es basiert auf den Entwürfen zum IEEE Standard 802.11i. Die Idee ist schnellst möglich eine bessere Alternative zu WEP zu bieten und dabei den zukünftigen Standard vorzubereiten. WPA soll mit Firmware Updates auf bestehender Hardware funktionieren.

WPA kann in zwei Hauptelemente aufgeteilt werden zum einen TKIP welches die Verschlüsselung verbessern soll und zum anderen 802.1X [7] zur verbesserten Authentisierung.

4.1.1 TKIP

TKIP [10] steht für Temporal Key Integrity Protocol. TKIP ist ein Wrapper der WEP umschliesst und ist so ausgelegt, das es mit bestehender Hardware realisiert werden kann. Es ist als eine Art Bug-Fix, der die Schwächen von WEP beheben soll, zu verstehen.

1. *Michael*, ein Kryptografischer message authentication code, zur Verhinderung von gefälschten Paketen.
2. *IV Sequenz*, um replay Attacken zu verhindern
3. eine *Schlüssel Mix Funktion*, um einen neuen Schlüssel für jedes Packet zu generieren.
4. und *Re-Keying* Mechanismus, um regelmässig neue Schlüssel zu generieren.

Eine etwas ausführlichere Beschreibung der einzelnen Elemente finden Sie in Anhang D

TKIP ist auf eine starke Authentisierungslösung basierend auf 802.1X angewiesen.

4.1.2 802.1X (EAP)

Der IEEE 802.1X Standard [7] dient zur Authentisierung und zum Schlüsselmanagement. Der Standard wurde ursprünglich für Kabelgebundene IEEE 802 LANs entwickelt, als solches ist nicht festgeschrieben in welcher Form er für Drahtlose 802.11 Netzwerke eingesetzt werden kann. 802.1X basiert auf EAP (Extensible Authentication Protocol) [4] und definiert als solches keine feste Methode zur Authentisierung. EAP wurde für PPP Verbindungen entwickelt und bietet die Möglichkeit nachdem der Link steht die Authentisierung vorzunehmen. Als solches bildet es ein Framework, auf dem eine beliebige Authentisierung implementiert werden kann. Die gängigste Methode ist ein Implementierung mit RADIUS. Dabei bietet es eine sogenannte Port-Based Authentication d.h. der Port, in WLAN-Fall eine Assoziation mit dem AP, wird authentisiert, ist dies geschehen hat dieser Port vollen Zugang zum Netzwerk. (Port ist hier nicht mit einem TCP/IP-Port zu verwechseln)

LEAP [5] steht für Lightweight EAP und ist ein Cisco implementation von EAP mit RADIUS als Authentisierungsmechanismus, welche in den Cisco Aironet Access Point implementiert ist.

5 SSID

Die SSID ist der Service-Set-Identifizierer der eine Kennung des WLAN darstellt.

5.1 SSID-Broadcast

Dieser Begriff bezeichnet zwei verschiedene Vorgänge. Zum einen sendet ein Access Point in regelmäßigen Abständen ein *BEACON-Frame* mit seiner SSID und anderen Management Informationen an alle Clients die ihn empfangen können um so seine Existenz bekannt zu machen. Die SSID kann somit auch von unerwünschten Clients (z.B. Wardriver) empfangen werden. Mit Broadcast wird jedoch auch die Antwort auf ein *Probe Request* an die Broadcast SSID bezeichnet. Dabei sendet ein Client ein spezielles Paket, mit einer leeren SSID an alle die ihn hören können, alle APs antworten daraufhin mit ihrer SSID und weiteren Informationen.

Es ist unter Umständen sinnvoll den SSID-Broadcast auszuschalten. Die meisten AP haben eine solche Funktion die auch manchmal als *closed-* oder *secure-mode* bezeichnet wird. Dabei werden beide Broadcasts deaktiviert. So können dann nur noch Clients verbinden die die SSID bereits kennen. Es gibt jedoch auch so noch Möglichkeiten die SSID zu ermitteln siehe Abschnitt 7

5.1.1 BEACON-Frame

Das BEACON-Frame [6] ist ein Management-Frame welches diverse Informationen über das Netz enthält. Es wird von AP regelmäßig ausgesendet. Wenn der SSID Broadcast eingeschaltet ist, enthält das BEACON Frame auch die SSID.

6 MAC-Adresse

MAC steht für Media Access Control und ist ein Sublayer des Data Link Layers im OSI Modell. Die MAC-Adresse ist die eindeutige Hardwareadresse einer Netzwerkkarte. Dies gilt sowohl für Kabelgebundene wie Kabellose Netzwerkkarten.

6.1 MAC-Filter

Der MAC-Filter soll aufgrund der eindeutigen MAC-Adresse ein Client erkennen und autorisieren. Wireless Access Points verfügen häufig über Filter in denen alle zugelassenen MAC-Adressen definiert werden können. Es können dann nur noch diejenigen Clients mit diesem Access Point verbinden welche in der Filter-Regel definiert sind.

Vorsicht einige AP/Router-Kombinationen lassen zwei unterschiedliche MAC-Filter definieren, einen für den AP und einen für den Router. Bitte lesen die das Manuel aufmerksam durch.

7 Wireless Scanner/Sniffer

Wireless Scanner/Sniffer dienen dazu Wireless Netzwerke aufzuspüren und/oder abzuhören.

Beim Scannen geht es darum Wireless LANs zu entdecken und Informationen wie z.B. die SSID, WEP on/off oder auch den Hersteller des AP zu ermitteln. Sniffer hingegen zeichnen den kompletten Netzwerkverkehr auf und analysieren auch den Inhalt der Pakete. Man unterscheidet dabei zwei Ansätze wie dies geschehen kann.

7.1 passiv

Ein passiver Scanner hört nur zu d.h. er versendet nicht aktiv Pakete über die Wireless Schnittstelle. Der Passive Scanner liest alle Pakete und untersucht dabei die Pakete nach den gewünschten Informationen. Die SSID kann zum Beispiel im BEACON-Frame gefunden werden. Ist der SSID-Broadcast ausgeschaltet kann ein passiver Scanner immer noch die SSID bestimmen in dem er die Anmeldung eines legitimen Clients beobachtet, der dabei die SSID bekannt gibt. Um passiv Scannen zu können muss die Software die ganzen Pakete erhalten dazu muss die Netzwerkkarte im monitor-mode sein (siehe 7.1.1).

Ein Sniffer arbeitet ähnlich wie ein passiver Scanner nur das er dem User alle Pakete zur Verfügung stellt. Die meisten passiven Tools sind eine Kombination von Scannern und Sniffern. Einige Sniffer bieten auch die Möglichkeit die WEP-Verchlüsselung anzugreifen und so unbefugt auch verschlüsselte Pakete mitzulesen (*AirSnort*).

Passive Scanner/Sniffer sind zum Beispiel *Kismet*, *ISS Wireless Scanner* und *Wildpackets AiroPeek*

Einige dieser Produkte unterstützen ebenfalls Aktive Methoden um Informationen über ein WLAN zu erhalten.

7.1.1 monitor-mode/promiscuous-mode

Die meisten Wireless LAN Netzwerkkarten lassen sich in den sogenannten monitor-mode oder auch promiscuous-mode schalten. In diesem Modus reicht die Karte die gesamten Pakete die es empfängt an den Treiber weiter auch solche, die nicht direkt für diesem Client bestimmt sind. So lässt sich ein Wireless LAN unbemerkt überwachen und mitschneiden. Dabei ist jedoch in der Regel der normale Netzwerkverkehr der Wireless Karte behindert oder unterbrochen.

7.2 aktiv

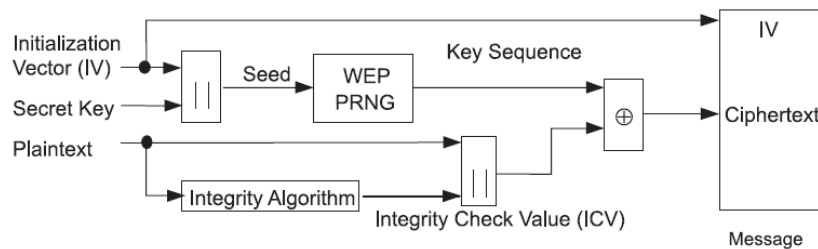
Aktive Scanner versenden in regelmässigen Abständen *Probe Request frames* und interpretieren dann die Antwort der Access Points. Es können auch andere Management Frames eingesetzt werden um weitere Informationen zu erhalten. Scanner welche nur solche aktiven Probes einsetzen, können keine APs mit ausgeschaltetem SSID-Broadcast entdecken. Aktive Scanner können auch keine Paket-Daten preisgeben, da sie nur Pakete analysieren die für sie bestimmt sind. Dafür wird der normale Betrieb nicht beeinflusst.

Der bekannteste aktive Scanner ist *NetStumbler*.

A WEP

WEP [6] ist eine Form von Electronic Code Book Algorithmus, dabei wird der Plaintext mittels XOR mit einer pseudo-zufälligen Schlüsselsequenz der gleichen Länge kombiniert.

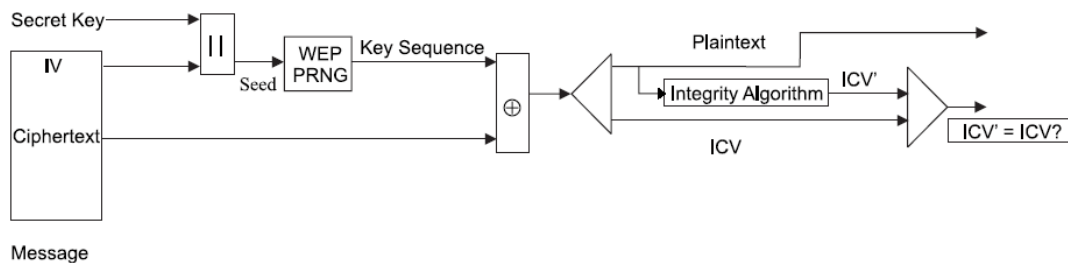
Die folgende Grafik zeigt den kompletten Verschlüsselungsvorgang. Zum einen wird der *secret key*, der über einen geheimen Kanal erst ausgetauscht werden muss, mit einem IV (Initialisierungs Vektor) kombiniert und dient als *seed* für den WEP-PRNG (Pseudo Random Number Generator).



Auf der anderen Seite wird über dem Plaintext der sogenannte *integrity check value* berechnet, um die Integrität der Daten zu garantieren. Dieser ICV wird dann dem Plaintext angehängt und mit dem Schlüsselstrom mittels XOR kombiniert. Das Resultat des XOR Vorgang ist der *ciphertext* dieser ergibt zusammen mit dem verwendete IV die *message* welche übertragen wird.

Als PRNG verwendet WEP den RC4 Algorithmus, siehe Anhang B. Der ICV ist eine einfache CRC-32 Checksumme.

Die folgenden Grafik zeigt die Entschlüsselung einer ankommenden Nachricht.



Mit Hilfe des *secret keys* und dem IV aus der *message* wird wieder die Schlüsselsequenz erzeugt. Diese wird mit dem *ciphertext* per XOR kombiniert. Zum Schluss wird noch der ICV über dem entschlüsselten Text errechnet und mit dem gelieferten Wert verglichen.

B RC4

RC4 [8] ist ein Strom-Chiffrierung mit variabler Schlüssellänge. Es ist einer der am weitesten verbreiteten Algorithmen und wird beispielsweise auch bei SSL eingesetzt.

Der Aufbau von RC4 ist sehr einfach und deshalb auch leicht zu implementieren, zudem ist er sehr schnell. Er hat eine 8x8 S-Box $S_0, S_1, S_2 \dots S_{255}$ die Einträge sind Permutationen von 0-255, die Permutation wird vom Schlüssel erzeugt.

Die S-Box wird folgendermassen initialisiert. Zuerst wird die S-Box linear gefüllt d.h. $S_0 = 0$ $S_1 = 1 \dots S_{255} = 255$ danach wird ein zweites 256-Byte Array mit dem Schlüssel gefüllt, dazu wird der Schlüssel wenn nötig wiederholt ($K_0, K_1 \dots K_{255}$).

```
j = 0
for i = 0 to 255
  j = (j + Si + Ki) mod 256
  swap Si and Sj
```

Der Strom wird nun folgendermassen erzeugt:

```
i = 0
j = 0

i = (i + 1) mod 256
j = (j + Si) mod 256
swap Si and Sj
t = (Si + Sj) mod 256
K = St
```

K ist nun das nächste Byte im Schlüsselstrom, der Vorgang wird für jedes weitere benötigte Byte wiederholt.

C shared-key Authentication

Die Authentisierung ist ein einfaches Challenge-Response Verfahren. Dazu werden 4 Pakete benötigt :

1. *Client* → *AP*
"Ich möchte mich authentisieren"
2. *AP* → *Client*
Der AP sendet ein Challenge Message, 128 zufällig erzeugte Bytes.
3. *Client* → *AP*
Der Client verschlüsselt die Challenge Message mit seinem WEP Schlüssel.
4. *AP* → *Client*
Wenn der AP die Antwort vom Client entschlüsseln kann und seine ursprüngliche Message erhält, wird dem Client ein "successful" gesendet und er ist authentisiert, ansonsten gibts ein "unsuccessful"

D TKIP

Im folgenden werden die einzelnen Elemente von TKIP erklärt.

Michael Michael ist ein völlig neu entwickelter *message authentication code*, dabei waren zwei Punkte wichtig bei Design, zum einen musste er eine genügend grosse Sicherheit bieten und zum anderen mit sehr wenig Rechenleistung auskommen, da er auch auf Hardware funktionieren sollte die dazu nicht dimensioniert wurde.

Der Michael Schlüssel ist 64-bit lang, dargestellt als zwei 32-bit little-endian words (K_0, K_1).

Die Michael tagging Funktion füllt als erstes die Nachricht mit hex 0x5a und genügend null Füll-Bytes das die Gesamtlänge ein vielfaches von 32 Bytes ergibt. Anschliessend wird das Resultat in 32-bit Wörter zerlegt $M_1, M_2, M_3 \dots M_n$. Zum Schluss wird das Tag mit Hilfe des Schlüssels und der Message-Wörter nach folgender Struktur errechnet:

```
(L, R) ← (K0, K1)
do i from 1 to n
    L ← L ⊕ Mi
    (L, R) ← b(L, R)
return (L, R) as the tag
```

⊕ stellt ein exclusive or (XOR) dar und b ist eine einfache Funktion basierend auf Rotationen, Additionen und Bit Tausch.

IV Sequenz Mit Hilfe von Michael kann zwar verhindert werden, dass Pakete als Ganzes gefälscht werden, aber er kann keine Replay Attacke verhindern. Um dies zu verhindern verwendet TKIP den Initialisierungs Vektor (IV) als Sequenzzähler. Dazu wird der IV bei jedem Schlüsselwechsel neu initialisiert und dann mit jedem Paket erhöht. Wenn nun ein Paket ankommt mit einem Wert grösser oder gleich einem bereits empfangenen wird dieses verworfen.

Key mixing Mit Hilfe der Key Mixing Funktion soll die grösste Schwäche im eigentlichen Design von WEP, dem "Missbrauch" des RC4 Algorithmus, behoben werden. Dabei wird für jedes Packet ein neuer temporärer Schlüssel erzeugt.

Dieser temporäre Schlüssel wird in zwei Phasen aus dem Basis WEP Schlüssel und der Sequenz Nummer erzeugt. Als erstes wird ein intermediate Schlüssel erzeugt, welcher die MAC Adresse mit einbezieht. dadurch wird erreicht, dass jeder Link eine andere Key Sequenz erzeugt, auch wenn die initialen Schlüssel dieselben sind. Anschliessend wird die Sequenznummer mit diesem Schlüssel und einem einfachen Algorithmus 'verschlüsselt' das Resultat der Verschlüsselung wird dann als Schlüssel für die WEP Verschlüsselung verwendet.

Rekeying Das letzte Element von TKIP befasst sich mit dem erneuern der verschiedenen Schlüssel die für die Erzeugung der Temporären Schlüssel und für Michael benötigt werden. Dazu wird auf die Authentisierungs-Infrastruktur von 802.1X zurückgegriffen. Mit Hilfe von speziellen Rekey Message Paketen wird der Update der Keys initialisiert. Der Authentisierungs-Server ist dann zuständig für die Verteilung der neuen Schlüssel.

Literatur

- [1] Bernard Aboba. The unofficial 802.11 security web page. <http://www.drizzle.com/~aboba/IEEE/>.
- [2] Nikita Borisov, Ian Goldberg, and David Wagner. Intercepting mobile communications: The insecurity of 802.11. In *7th Annual International Conference on Mobile Computing and Networking*, 2001. <http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf>.
- [3] Scott Fluhrer, Itsik Mantin, and Adi Shamir. Weaknesses in the key scheduling algorithm of rc4, 2001. http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf.
- [4] EAP Working Group. Extensible authentication protocol (eap). RFC 2284. <http://www.ietf.org/internet-drafts/draft-ietf-eap-rfc2284bis-06.txt>.
- [5] Cameron MacNally. Cisco leap protocol description. <http://www.miss1.cs.umd.edu/wireless/ethereal/leap.txt>.
- [6] LAN/MAN Standards Committee of the IEEE Computer Society. Wireless lan medium access control (mac) and physical layer (phy) specifications. IEEE 802.11, 1999. <http://standards.ieee.org/getieee802/802.11.html>.
- [7] LAN/MAN Standards Committee of the IEEE Computer Society. Port-based network access control. IEEE 802.1X, 2001. <http://standards.ieee.org/getieee802/download/802.1X-2001.pdf>.
- [8] Bruce Schneier. *Applied Cryptography*. John Wiley & Sons, second edition, 1996.
- [9] Adam Stubblefield, John Ioannidis, and Aviel D. Rubin. Using the fluhrer, mantin, and shamir attack to break wep. Technical report, AT&T Labs Research, August 2001. http://www.cs.rice.edu/~astubble/wep/wep_attack.pdf.
- [10] Jesse Walker. 802.11 security series. 2002. http://cedar.intel.com/media/pdf/wireless/80211_1.pdf, http://cedar.intel.com/media/pdf/security/80211_part2.pdf, http://cedar.intel.com/media/pdf/security/80211_part3.pdf.
- [11] WiFi-Alliance. Wi-fi protected access (wpa) security web page. http://www.wifialliance.com/OpenSection/protected_access.asp.