Sicherheit von Wireless LANs

Aktuelle und geplante Standards zur Sicherung der Datenübertragung und mögliche Angriffszenarien

Sebastian Klamar
Fakultät Informatik
Technische Universität Dresden
klamar@rn.inf.tu-dresden.de

18. August 2003

Zusammenfassung

In diesem Dokument werden die Schwächen von WEP ausführlich beschrieben. Es wird aufgezeigt, dass 802.11 WEP der Forderung nach Zugriffskontrolle, Datenintegrität und Vertraulichkeit nicht gerecht wird und warum diese Fehler existieren. Im zweiten Teil werden Lösungen vorgestellt, die diese Sicherheitsprobleme bewältigen sollen. Behandelt werden Erweiterungen wie 802.1X/EAP und der neue Standard 802.11i (TKIP und CCMP).

1 Einleitung

Drahtlose Netze nach dem Standard IEEE 802.11 (Wireless LAN, kurz WLAN) erfreuen sich bei Privatanwendern sowie Unternehmen größer werdender Beliebtheit. Die Preise für Access Points und WLAN-Erweiterungskarten für die Stationen sinken immer weiter nach unten. Bei der angebotenen Übertragunsgeschwindigkeit tut sich auch was. Erst kürzlich wurde ein neuer Standard IEEE 802.11g verabschiedet, der sogar Geschwindigkeiten bis zu 54 Mbit/s im 2,4-GHz-ISM-Band unterstützt (Hei03b). Die nachfolgende Tabelle zeigt eine Übersicht derzeit standardisierter Übertragungsraten für WLAN.

Bruttorate/Frequenz	bei 2,4 GHz	bei 5,2 GHz
1/2 Mbit/s	802.11	–
5,5/11 Mbit/s	802.11b[a]	–
22/33/44 Mbit/s	802.11b+/PBCC[b c]	–
6–54 Mbit/s	802.11g[c]	802.11a[d] /802.11h[e]

[a] abwärtskompatibel zu 802.11
[b] proprietäres Verfahren von Texas Instruments, von anderen Chipherstellern derzeit nicht unterstützt
[c] abwärtskompatibel zu 802.11/11b
[d] in Deutschland derzeit nur mit Auflagen
[e] ergänzt 802.11a um automatische Frequenzwahl (DFS) und Sendeleistungssteuerung (TPC)

Tabelle 1: Aktuelle WLAN-Übertragungsraten (nach (Hei03b))

1.1 Allgemeine Sicherheitsprobleme

Grund für den Einsatz von WLANs ist meist eine einfachere Installation gegenüber drahtgebundenen Netzen, die erst das Verlegen von Kabeln notwendig machen. Jedoch hat, wie so oft, jeder Komfort auch seine Schattenseite. Funknetze sind Broadcastmedien, sodass gegenüber kabelgebundenen Netzen das Abhören der Kommunikation viel einfacher ist. Mit einer herkömmliche Antenne ausgerüstet kann der Angreifer von außerhalb des Gebäudes die Funkkommunikation abhören, da mit einer Übertragungsstärke von bis zu 1 W gesendet wird (Eck03). Brauchte der Angreifer bei einem drahtgebundenen Netz noch physischen Zugriff auf das LAN, musste also in das Gebäude eingedrungen sein, reicht es bei WLAN, sich in der Nähe des Gebäudes aufzuhalten, z. B. auf einer Parkbank oder im Auto.

Diese Einfachheit, mit der sich auch Anfänger schnell in das fremde Netz einklinken können, hat zu einem neuen Volkssport geführt, »Wardriving« oder auch »Drive-by-Hacking« genannt (Bre02). Vereinfachend kommt hinzu, dass viele Systemadministratoren nachlässig handeln und Sicherheitsvorkehrungen wie z. B. die Verschlüsselung in WEP (siehe Abschnitt 2) erst gar nicht aktivieren. Die Hobby-Hacker machen sich in diesem Fall nach aktueller Rechtslage in Deutschland nicht einmal strafbar, da sie keine Sicherheitsmaßnahmen brechen (Eck03).

1.2 Drei Prämissen für ein Sicherheitsprotokoll

Bei der Gestaltung eines Sicherheitskonzeptes für Funknetzwerke sind drei Prämissen zu berücksichtigen (BGW01; Cor02):

1. Zugriffskontrolle,
2. Datenintegrität sowie
3. Vertraulichkeit.

Zugriffskontrolle Eine Zugriffskontrolle soll sicherstellen, dass nur legitimierte Nutzer an der Kommunikation teilnehmen können (Authorisierung). Weiterhin soll sie auch gewährleisten, dass sich die Nutzer mit einem vertrauenswürdigen Partner (hier Access Point) verbinden (Authentifizierung), statt die Kommunikation über einen »rogue« (deutsch: Schurke) Access Point abzuwickeln.

Datenintegrität Die Datenintegrität hat als Ziel, dass Angreifer davon abgehalten werden, die Daten einer Nachricht unbemerkt für die Kommunikationspartner zu verfälschen. Ferner stellt sie sicher, dass die Daten von der Station stammen, von der sie es vorgeben zu sein.

Vertraulichkeit Zur Erfüllung der Vertraulichkeit wird meist Verschlüsselung angewandt. Dadurch soll nur der Partner, für den die Übertragung bestimmt ist, den Inhalt der Nachricht lesen können.

1.3 Das Sicherheitskonzept von 802.11

Der IEEE Standard 802.11[1] definiert das WEP Protokoll, das den Anforderungen zur Erfüllung von Zugriffskontrolle, Datenintegrität und Vertraulichkeit gerecht werden soll. Im nachfolgenden Abschnitt werden die WEP-Spezifikation näher erläutert und die Schwächen beleuchtet. Der sich daran anschließende Abschnitt 3 zeigt Erweiterungen und Alternativen zu WEP auf. Der neue IEEE Standard 802.11i, der WEP ablösen soll, wird im Abschnitt 4 genau vorgestellt.

2 WEP und seine Schwächen

Außer den in Tabelle 1 aufgeführten Übertragunsraten definiert der IEEE Standard 802.11 auch das »Wired Equivalent Privacy« (WEP) Protokoll. Dieses Sicherheitsprotokoll soll, wie es der Name schon andeutet, im Funknetz den gleichen Sicherheitslevel wie im drahtgebundenen Netz erzielen (Eck03). WEP ist in den Access Points und WLAN-Karten integriert und bietet Punkt-zu-Punkt-Sicherheit, Ende-zu-Ende-Sicherheit wird jedoch nicht erfüllt.

Im Folgenden wird die Umsetzung der Sicherheitsprämissen Zugriffskontrolle, Datenintegrität und Vertraulichkeit des WEP-Protokolls zusammengefasst, wie sie beispielsweise in (BGW01; Eck03) beschrieben sind. Es wird sich zeigen, dass WEP seine Ziele nicht erfüllt.

2.1 Zugriffskontrolle

2.1.1 Low-Level-Absicherung durch ESSID und MAC

Eine Art Zugriffskontrolle kann bereits außerhalb von WEP erreicht werden, zum einen durch die ESSID (Extended Service Set ID) und zum anderen durch Verwendung von MAC-Black- und -Whitelisten. Die ESSID ist der genaue Identifikationsname eines Service Sets, d. h. eines logischen Bereichs, der durch einen oder mehrere Access Points versorgt wird. Mit der beim Access Point eingestellten ESSID »Any« werden alle Verbindungen akzeptiert. Bei einem anderen Wert können nur die Teilnehmer mit dem AP kommunizieren, die mit der gleichen ESSID konfiguriert sind.

Durch Deklaration von erlaubten und verbotenen MAC-Adressen kann die Kommunikation des APs mit WLAN-Stationen a priori eingeschränkt werden.

Sicherheitsprobleme

Die Absicherung durch Deklaration von legitimierten MAC-Adressen kann leicht hintergangen werden: Durch passives Abhören des Funkverkehrs kann ein Angreifer gültige MAC-Adressen aufzeichnen. Durch MAC-Spoofing gibt er sich dann als Berechtigter aus.

Man könnte die ESSID als eine Art Passwort für den Zugriff auf das Netz halten. Dem ist keinesfalls so. Sofern nicht anders konfiguriert[2],

[1] Die Erweiterungen 802.11a, 802.11b usw. behandeln nur höhere Datenraten von WLAN, das WEP bleibt unberührt.

[2] Leider sind viele Sicherheitseinrichtungen in WEP optional. So kommt es, dass Administratoren die WEP-Authentifizierung und WEP-Verschlüsselung erst gar nicht aktivieren. Das URZ der TU Dresden verfährt bedauerlicherweise so — oder macht es aus dem Grund, dass WEP sowieso unsicher ist.

sendet ein Access Point in den s. g. Beacon Frames seine ESSID aus und bietet den Stationen damit seine Dienste an.

2.1.2 Open und Shared Authentication

WEP definiert zwei Authentifizierungs-Schemata:

- Open System Authentication und
- Shared Key Authentication.

Open System Authentication Bei der Open System Authentication findet keinerlei Überprüfung statt. Stattdessen wird jeder mobile Telnehmer als Benutzer des Funknetzes zugelassen.

Shared Key Authentication Die Shared Key Authentication wickelt die Authentifizierung über ein Challenge-Response-Verfahren ab. Dazu sendet der Access Point eine 1024 Bit lange Zufallszahl an den mobilen Teilnehmer, der diese verschlüsselt zurücksenden muss. Der Access Point entschlüsselt den erhaltenen Wert und vergleicht ihn mit der versandten Zufallszahl. Sind beide gleich, hat der mobile Funkpartner sich korrekt gegenüber dem Access Point ausgewiesen und kann als berechtigter Teilnehmer das Netz für eine Kommunikation benutzen.

Zur Verschlüsselung der Challenge-Response wird der RC4-Algorithmus verwendet. Der hierfür verwendete Schlüssel muss vorher auf dem Access Point und den einzelnen Rechnern verteilt werden. WEP unterstützt bis zu vier solcher Schlüssel, die eine Länge von 48 oder 104 bit haben. Bei der Kommunikation muss der Index des verwendeten Schlüssel mit angegeben werden. Die Schlüssel sind im Allgemeinen geheim.

Der RC4 ist eine Stromchiffre, d. h. unter Verwendung des geheimen Schlüssels wird ein Schlüsselstrom generiert. Der Schlüsselstrom wird per XOR mit dem Klartext verknüpft, um den Chiffretext zu erzeugen.

Sicherheitsprobleme

Meist nur ein Schlüssel benutzt Der WEP-Standard sieht zwar die Verwendung von bis zu vier Schlüsseln vor. Die Angabe des Indexes zur Signalisierung, welcher Schlüssel bei der aktuell verschlüsselten Nachricht verwendet wird, macht es jedoch erforderlich, dass die Schlüssel auf allen Stationen in der gleichen Reihenfolge eingetragen sind. Deshalb wird in der Praxis oft nur ein Schlüssel verwendet.

Kein wirkliches Geheimnis Zur Kommunikation mit einem der Access Points des Basic Service Sets (BSS) verwenden die mobilen Stationen einen der vier geheimen Schlüssel. Der Schlüssel ist nicht nur für die jeweilige Station geheim, sondern jeder Netzteilnehmer teilt sich das Wissen über den »geheimen« Schlüssel auch mit allen anderes Rechnern des BSS. Von einem Geheimnis kann also keine Rede sein!

Kein Schlüsselmanagement Die gemeinsamen, geheimen Schlüssel müssen manuell in jeder Station eingetragen werden, da der Standard kein Schlüsselmanagement vorsieht. Bei einer Kompromittierung, z. B. durch Diebstahl einer Karte, muss der Netzadministrator die WEP-Schlüssel auf allen mobilen Clients per Hand ändern oder die Nutzer zum Ändern veranlassen. Ohne Zweifel ist dies für die Verwaltung zu aufwendig und fehleranfällig.

Keine individuelle Authentifizierung Wenn alle Stationen den/die gleichen Schlüssel verwenden, dann ist eine Authentifizierung eines einzelnen, individuellen Nutzers nicht möglich. Hinzu kommt, dass bereits der Besitz einer WLAN-Karte (z. B. durch Abhandenkommen eines Laptops) dem Angreifer der Zugang zum Funknetz geöffnet wird.

Keine Authentifizierung Netz gegenüber Nutzer Die mobilen Stationen authentifizieren sich zwar mehr oder weniger gegenüber dem Access Point, einer genauere Identifikation des Access Points gegenüber dem Nutzer erfolgt jedoch nicht. Diese Designschwäche eröffnet dem Angreifer die Möglichkeit, Spoofing-Angriffe erfolgreich durchzuführen.

Lieferung Klartext-Kryptopaar Bei der Shared Key Authentication sendet die mobile Station die vom Access Point erhaltene Zufallszahl verschlüsselt zurück. Da für die Verschlüsselung der Challenge-Response der gleiche Schlüssel verwendet wird wie für die Verschlüsselung aller anderen Datenpakete, erhält der Angreifer auf einfache Weise ein Klartext-Kryptopaar, das er für weitergehende Angriffe nutzen kann (die Verschlüsselung im WEP-Protokoll wird später im Abschnitt 2.3 näher beschrieben).

2.2 Datenintegrität

Das WEP-Protokoll benutzt den CRC32-Algorithmus, um die Prüfsumme für einen Frame zu berechnen. Die Prüfsumme hat eine Länge von 32 bit.

Abbildung 1: CRC-32-Verfahren und anschließende Verschlüsselung

Sicherheitsprobleme

Linearitätseigenschaft Das CRC32-Verfahren ist effizient für die Erkennung von Bitfehlern, jedoch ungeeignet für die Integrität im Sinne von kryptografischen Hash-Funktionen (Eck03). Zudem ist CRC ein lineare Algorithmus — ein Problem, das alle CRC-Verfahren haben (BGW01). Bei einem linearem Algorithmus gilt die Linearitätseigenschaft, das bedeutet hier:

$$\text{CRC32}(M \oplus M') = \text{CRC32}(M) \oplus \text{CRC32}(M')$$

Damit ist es möglich, aus der Bitdifferenz zweier Eingabetexte die Bitdifferenz der zugehörigen CRC-Werte zu berechnen.

Chiffretext manipulierbar Prüfsumme und Datenteil werden zwar verschlüsselt, doch kommt hier ein zweiter ungünstiger Umstand hinzu: Auch die Stromchiffre ist linear. Die Linearität von CRC32-Verfahren und Stromchiffre führt dazu, dass ein Angreifer beliebigen Chiffretext manipulieren und gleichzeitig die Prüfsumme anpassen kann. Der Empfänger ist nicht mehr in der Lage, die Manipulation an der Nachricht zu erkennen.

Das folgende Beispiel soll die Problematik veranschaulichen:

Gegeben ist die originale Nachricht M, die zu C verschlüsselt wird. Der Angreifer versucht, die mit Δ modifzierte Nachricht $F = M \oplus \Delta$ einzuspielen. Dazu nutzt er die Linearität aus.

$$\begin{aligned}
(M' \mid \text{CRC32}(M')) &= C' \oplus RC4 \\
&= C \oplus (\Delta \mid \text{CRC32}(\Delta)) \oplus RC4 \\
&= (M \oplus \text{CRC32}(M)) \oplus (\Delta \mid \text{CRC32}(\Delta)) \\
&= (M \oplus \Delta \mid \text{CRC32}(M) \oplus \text{CRC32}(\Delta)) \\
&= (M \oplus \Delta \mid \text{CRC32}(M \oplus \Delta)) \\
&= F \mid \text{CRC32}(F) \qquad \text{wird korrekt akzeptiert.}
\end{aligned}$$

Entschlüsseln der Nachricht Die gezielte Modifikation einer Nachricht kann auch dazu benutzt werden, den Klartext einer chiffrierten Nachricht zu bestimmen. Normalerweise ist dazu der geheime Schlüssel notwendig. Diesen besitzt der Angreifer jedoch nicht. Er kann jedoch die IP-Adresse des Zielrechners in der Nachricht abändern, sodass der Access Point die Nachricht, entschlüsselt, nun an den Rechner des Angreifers außerhalb des WLAN sendet (BGW01).

2.3 Vertraulichkeit

Die Sicherung der Vertraulichkeit ist ein grundlegendes Ziel von WEP. Jedoch wird sich zeigen, dass auch dieses verletzt wird.

Wie weiter oben schon angedeutet wurde, benutzt WEP das RC4-Verfahren, um die Datenpakete zu verschlüsseln. Der dafür verwendete Schlüssel ist der gleiche, der auch bei der Authentifizierung benutzt wird. Er hat eine Länge von 40 bit (s. g. Silber-Karten) oder 104 bit (Gold).

RC4 ist eine Stromchiffre. Stromchiffren dürfen nur unter der Voraussetzung benutzt werden, dass für zwei zu verschlüsselnde Klartexte niemals derselbe Schlüssel zur Erzeugung des Stromchiffre genommen wird. Missachtet man diese Vorgabe, dann kann ein Angreifer durch bekannten Klartext P_1 den Klartext P_2 berechnen, da sich bei der XOR-Verknüpfung die gleichen Stromchiffren aufheben:

$$\begin{aligned}
C_1 &= P_1 \oplus \text{RC4} && \text{bekanntes Klartext-Kryptopaar } P_1C_1 \\
C_2 &= P_2 \oplus \text{RC4} && P_2 \text{ unbekannter Klartext}
\end{aligned}$$

$$\begin{aligned}
C_1 \oplus C_2 &= (P_1 \oplus \text{RC4}) \oplus (P_2 \oplus \text{RC4}) \\
&= P_1 \oplus P_2
\end{aligned}$$

und schließlich

$$P_2 = P_1 \oplus P_2 \oplus P_1$$

Aus diesem Grund wird der statische Schlüssel für jedes Datenpaket um einen individuellen 24-bittigen Initialisierungsvektor (IV) erweitert. Dieser IV bildet mit dem geheimen, statischen WEP-Schlüssel, den beide Funkpartner haben, den Schlüssel für den RC4-Algorithmus. Damit der Empfänger in der Lage ist, das empfangene Paket zu entschlüsseln, wird der IV dem Paket als Klartext hinzugefügt (Eck03).

Sicherheitsprobleme

24 bit IV-Raum zu kurz(lebig) Der Initialisierungsvektor hat nur eine Länge von 24 bit. Das ergibt $2^{24} = 16,7$ Millionen mögliche Pakete, die je einen voneinander unterschiedlichen IV besitzen. Eine einfache Rechnung zeigt jedoch, dass diese Anzahl bei einem stark frequentierten Access Point mit 5,5 Mbit/s (das ist die maximale Datenrate von 11 Mbits/s 802.11b, siehe Tab. 1) und einer Paketgröße von 1500 Byte bereits nach einigen Stunden ausgeschöpft ist (BGW01):

$$\frac{2^{24}}{\frac{5{,}5\ \text{Mbit/s}}{8\ \text{bit/Byte} \cdot 1500\ \text{Byte}}} \approx 5\ \text{h}$$

Kollisionen durch zufällig gleiche IVs Zudem besteht eine große Wahrscheinlichkeit von Kollisionen, die durch zufällig gleich gewählte IVs auftreten können. Als Kollision wird hier die Wiederbenutzung eines alten IVs bezeichnet. So ist die Wahrscheinlichkeit größer 50 % nach bereits $2^{12} = 4823$ Datenpaketen; nach 12340 Paketen beträgt sie mehr als 99 % (BGW01; Eck03).

Implementierungsschwächen Der WEP-Standard *fordert* nicht, sondern *empfiehlt* nur, den IV für jedes Paket zu ändern. Damit sind Implementierungen, die stets den gleichen IV verwenden, völlig standardkonform.

Viele WLAN-Karten bestimmen den IV nicht zufällig, sondern inkrementieren den Zähler für jedes Datenpaket um 1, wobei sie den internen IV-Wert bei Aktivierung auf 0 zurücksetzen. Damit werden IVs mit niedrigen Werten sehr häufig wiederverwendet (BGW01; Eck03).

Aufbau einer IV-Tabelle zum Entschlüsseln Das Fehlen eines Schlüsselmanagements wurde bereits im Abschnitt zur Zugriffskontrolle moniert. An dieser Stelle wird das Problem ein weiteres Mal aufgegriffen und erläutert, wie ein Angreifer auf einfache Weise sukzessiv jeden Kryptotext entschlüsseln kann — begünstigt durch die o. g. Schwächen und dadurch, dass die Anwender selten den geheimen Schlüssels wechseln.

Kennt ein Angreifer ein Klartext-Kryptopaar für einen bestimmten IV (durch durch z. B. Challenge-Response bei Authentifizierung oder typischer Aufbau IP-Header), so kann er bekanntlich den Schlüsselstrom ableiten und damit den Klartext jeder Nachricht entschlüsseln, die den gleichen IV benutzt. Mit der Zeit baut der Angreifer eine Tabelle auf, die die bereits ermittelten Schlüsselströme enthält. Als Index wird der IV genommen. An dieser Stelle wird deutlich, dass es für die Sicherheit der Verschlüsselung egal ist, ob Karten mit 48 oder 104 bit Schlüssel eingesetzt

werden[3], da sich die Größe der Tabelle nach der Länge des IV (24 bit) richtet. Für die Tabelle werden maximal 24 GBytes ($1500 \cdot 2^{24}$ Bytes) benötigt (Eck03) — kein Problem für heutige Festplatten.

FMS-Attacke FLUHRER, MANTIN und SHAMIR veröffentlichten bereits 2001 in ihrem Paper »Weaknesses in the Key Scheduling Algorithm of RC4« (FMS01) verschiedene Schwächen von RC4. Unter anderem beschreiben sie eine einfache und schnelle Methode, wie ein Angreifer den geheimen RC4-Schlüssel durch Sammeln weniger Pakete erlernen kann. Sie entdeckten, dass es eine große Anzahl von geheimen Schlüsseln gibt, für die die Permutation (zur Erzeugung des Schlüsselstroms, genauere Details in (FMS01)) von einer kleinen Anzahl von Bits im geheimen Schlüssel bestimmt wird. Darüber hinaus hat RC4 Fehler im seinem Zufallsgenerator-Algorithmus. Die Folge ist, dass ein Angreifer nur einige Millionen Pakete sammeln braucht, deren erstes Byte er kennt[4], und dadurch den gesamten WEP-Basisschlüssel ableiten kann.

Es gibt freie Tools wie z. B. Airsnort (http://airsnort.shmoo.com/), die diese Schwäche implementieren und sich damit bestens für die eingangs erwähnte »Wardriving«-Gruppe eignen. Diese Tatsache und der Umstand, dass die FMS-Attacke passiv, also unbemerkt für die WLAN-Betreiber abläuft, zeigt, wie ernst die Sicherheitsprobleme von WEP zu nehmen sind.

2.4 Zusammenfassung der Probleme von WEP

1. Der 24 bit lange Initialisierungsvektor ist zu kurz und gefährdet damit die Vertraulichkeit.
2. Die CRC-Prüfsumme ist unsicher, weil sie Modifikationen, die ein Angreifer an abgefangenen Paketen vorgenommen hat, nicht erkennt.
3. WEP kombiniert den Initialisierungsvektor mit dem WEP-Schlüssel. Dadurch kann der Angreifer allein durch passives Abhören von wenigen Millionen Paketen den WEP-Schlüssel erlernen.
4. Es wird keine Integritätssicherung für Quell- und Zieladresse angeboten.

3 Erweiterungen und Alternativen zu WEP

Wie der vorhergehende Abschnitt gezeigt hat, werden die Anforderungen nach Vertraulichkeit, Datenintegrität sowie sicherer Authentifizierung von WEP nicht erfüllt. Gesucht sind deshalb Lösungen, die diese Probleme bewältigen. Die Palette der Lösungsmöglichkeiten reicht von relativ simplen Techniken, die für selektive Anwendungen auf der Transportebene des OSI-Schichtenmodells arbeiten (SSH und TLS) bis runter zur Vermittlungs- bzw. Data-Link-Ebene (VPN) und MAC-Ebene

[3] Marketing-Abteilungen sind gar so dreist, ihr Produkt mit 64 bzw. 128 bit Verschlüsselung zu bewerben, obwohl real nur 48 respektive 104 bit zum Zuge kommen — die restlichen 24 bit (der IV) gehen bekanntlich als Klartext über den Äther.

[4] Zufälligerweise ist das erste Byte der Payload von 802.11 eine Konstante, dem Angreifer demzufolge per se bekannt.

(802.11X/EAP). Diese Techniken sollten je nach Anforderung als Erweiterung zu WEP angewandt werden, solange der neue Standard IEEE 802.11i, der Nachfolger von WEP, noch nicht ratifiziert[5] ist.

3.1 Workarounds — SSH Tunneling und SSL/TLS

Die Technik der Secure Socket Layer (SSL) ist vielen Anwendern aus der Welt des WWW (gemeint ist HTTPS, mit dem der Browser sicher mit einem Webserver kommunizieren kann) und SSH (Secure Shell für den Remote-Zugriff) bekannt. Außer für diese Standardanwendungen lassen sich die SSL-Bibliotheken auch dazu verwenden, eine Verschlüsselung auf Transportebene einzuführen.

SSH/TLS Die Verwendung von SSL/TLS muss in die Anwendung fest einprogrammiert worden sein. Dies wird von immer mehr Anwendungen im Internet unterstützt. Es gibt zwei Modi:

1. TLS-Modus, bei dem die Verbindung über den Standardport läuft und die sichere Kommunikation mit dem Kommando STARTTLS initiiert wird;
2. SSL, bei dem die Kommunikation über einen anderen Port abgewickelt wird (SSL-Tunnel), z. B. »IMAP over SSL« (IMAPS: Port 993) und »LDAP over SSL« (LDAPS: Port 636).

SSH-Tunnel Mit dem Programm SSH lassen sich ganz einfach Tunnel für Anwendungen aufsetzen, die keine SSL-Unterstützung von Herstellerseite anbieten. Durch diesen verschlüsselten Tunnel können nach Aufsetzen sensible Anwendungen geschleust werden, die ihre Daten sonst, da im Klartext gesendet, dem Angreifer aufgrund der zusätzlichen Unsicherheit von WEP preisgeben würden.

3.2 VPN

Mit VPN (Virtual Private Network) in Form von IPsec werden ebenfalls Tunnel mit Verschlüsselung aufgesetzt. Jedoch arbeiten diese Tunnel nicht auf der Socket-/Transportebene, sondern eine Ebene tiefer, auf der IP-/Netzwerk-Ebene[6]. VPN werden meist dazu eingesetzt, um verschiedene Subnetze bzw. die verschiedenen Niederlassungen einer Firma über ein unsicheres Netz miteinander zu verbinden. Der Verkehr über das unsichere Netzwerk erfolgt innerhalb von Tunneln, die zwischen den VPN-Gateways aufgebaut werden.

Die genauere Funktionsweise von VPN respektive IPsec soll an dieser Stelle nicht beschrieben werden. Der Leser mag zusätzliche Literatur zu Rate ziehen, z. B. (Int03).

[5] Im Februar diesen Jahres hieß es, mit einer Verabschiedung des Standards sei im Sommer zu rechnen. Doch wie es sich abzeichnet, wird 802.11i erst nächstes Jahr fertig (Hei03a).

[6] Obwohl man bei Verwendung von PPTP und L2PT auch die Sicherungsschicht (OSI-Schicht 2) mit dazu zählen kann (Zoe).

3.3 802.1X/EAP

IEEE 802.1X ist das Herzstück der neuen Sicherheitsarchitektur von IEEE, des Robust Security Networks (RSN). Es ist ein Framework, das für die IEEE 802-Protokollfamilie sichere Zugriffskontrolle, Authentifizierung sowie Schlüsselmanagement bieten soll. Die Sicherheitsbeschränkungen finden auf der MAC-Ebene statt. Damit prädestiniert sich 802.1X als Erweiterung zu WEP.[7]

Rollenmodell RSN definiert für das Framework drei Rollen:

1. Supplicant,
2. Authenticator und
3. Authentication Server.

In einem Wireless LAN ist der Supplicant der mobile Client, der einen Dienst (eine MAC-Verbindung, d. h. die Assoziation zu einem Access Point) nutzen möchte. Der Authenticator ist ein 802.1X-fähiger Access Point (oder im allg. Fall ein Switch). Der Authentication Server ist eine zentrale Instanz (im logischen Sinne), die über eine Zugriffserlaubnis entscheidet, und nimmt gegenüber Supplicant und Authenticator eine vertrauenswürdige Stellung ein. Er ist irgendwo hinter dem Authenticator positioniert.

Authentifizierung Durch Nutzung von EAP (Extensible Authentication Protocol) ist es möglich, verschiedene Authentifizierungsmethoden wie z. B. Einmalpasswörter, Zertifikate und Smartcards zu verwenden. Der Authenticator agiert bei der Authentifizierung nur als Brücke, der die EAP-Daten zwischen Supplicant und Authentication Server weiterleitet. Dies ermöglicht es, in einem Unternehmensnetzwerk einen neuen Authentifizierungsmechanismus einzuführen, ohne den Access Point aufrüsten oder austauschen zu müssen.

Der Authentifizierungsprozess findet, wie bereits angedeutet, nur zwischen Supplicant und Authentication Server statt — nach dem Challenge-Response-Paradigma. Bei erfolgreicher Prüfung teilt der Authentication Server dem Authenticator mit, dem Supplicant den Zugriff zum Netz zu gewähren. Dazu implementiert der Authenticator ein Dual-Port-Konzept. Ein Port leitet jedes Datenpaket unkontrolliert, d. h. ohne die Autorisierung zu überprüfen, weiter. Dieser Port wird nur während der Authentifizierung benutzt, d. h. die hier weitergeleiteten Daten sind i. d. R. nur EAP-Pakete zwischen Supplicant und Authentication Server. Der unkontrollierte Port kann aber auch aus Rückwärtskompatibilitätsgründen benutzt werden, wenn der Administrator den Zugriff auf andere Weise regeln will. Der andere der zwei Ports, der kontrollierte Port, lässt nach erfolgreicher Authentifizierung alle Pakete des Supplicant passieren.

EAPOL und RADIUS Zwischen mobilem Client (Supplicant) und Access Point (Authenticator) werden die EAP-Daten in EAPOL-Nachrichten gekapselt (*EAP over LAN* für Shared Medien wie 802.11), zwischen Access Point und Authentication Server wird meist RADIUS oder Kerberos eingesetzt (FC02; MA02).

Jedoch liegen bereits erste Analysen vor, die die Möglichkeit eines Man-in-the-Middle-Angriffs und session hijacking aufzeigen (MA02).

[7] In der Tat werden Bestandteile von 802.1X als Teil von 802.11i standardisiert.

4 Der neue Standard 802.11i

Die IEEE 802.11i Task Group i (TGi) ist mit der Aufgabe betraut worden, neue Sicherheitsprotokolle für Wireless LAN zu entwickeln.

WEP ist derart löchrig, sodass es für die TGi das beste schien, ein neues Sicherheitsprotokoll von Grund auf neu zu entwickeln, anstatt die Sicherheitslücken von WEP auszubessern. Dies konnte jedoch nicht der Weg sein, denn die Entwickler hatten zu berücksichtigen, dass eine beträchtlich große Anzahl von 802.11-Installationen am Markt in Benutzung war. Die Industrie hatte gegenbüber ihren Kunden die Pflicht, die Sicherheitsmängel an den installierten Geräten zu beheben, statt die Anwender neue Hardware kaufen zu lassen. Aus diesen Rahmenbedingungen heraus hat die TGi zwei Lösungen für die Problematik von WEP erarbeitet:

1. TKIP — ein WEP-Patch für existierende Hardware;
2. CCMP — Nachfolger von WEP und TKIP.

(CWHWW03; Wal02a)

4.1 TKIP

4.1.1 Anforderungen an den Nachfolger von WEP

TKIP (Temporal Key Integrity Protocol) ist gedacht als Interimslösung, um existierende Hardware unterstützen zu können. Das Diffizile daran ist nicht, das bestehende WEP-Protokoll auszubessern, denn ein gänzlich neues Sicherheitsprotokoll ist auch sehr schwer zu entwickeln. Viel mehr hat man zu beachten, dass typische Access Points mit den billigsten Mikroprozessoren laufen — i486, ARM oder PowerPC bei 40 oder gar 25 MHz. Bei normalem WLAN-Betrieb haben diese eine CPU-Auslastung von bereits 90 %, bieten also wenig Spielraum für neue Algorithmen.

Zusammengefasst hatten die Entwickler von TKIP drei Nebenbedingungen zu berücksichtigen (CWHWW03):

1. Die vorhandenen Systeme bei den Anwendern mussten per Software oder per Firmware nachbesserbar sein,
2. die vorhandene Implementation von WEP in Hardware durfte nicht verändert werden und
3. die Verschlechterung der Performance durch neue Algorithmen sollte so gering wie möglich sein.

4.1.2 Vier neue Sicherheitselemente um WEP

Die Grundelemente von WEP, nämlich der RC4-Algorithmus zur Verschlüsselung und das Zusammenspiel von WEP-Schlüssel und Initialisierungsvektor mussten beibehalten werden, da diese Funktionen in fast allen Access Points in Hardware implementiert sind — wie sonst könnte die schmalbrüstige Ausstattung gängiger Access Points den CPU-intensiven RC4-Verschlüsselungsalgorithmus ausführen.

TKIP adaptiert vier Algorithmen, die altbewährten Konzepten entstammen, und platziert diese, mit leichten Anpassungen durch die Hardware bedingt, um WEP:

1. *Message Integrity Code* (MIC), »Michael« genannt → Fälschungen erkennen;
2. neue *Paketsequenzkontrolle* → Replay-Attacken verhindern;
3. *Per-Packet-Key-Mixing* → Korrelation zwischen im Klartext versandtem IV und Chiffrierschlüssel (WEP-Basis-Schlüssel + IV) beseitigen;
4. *Rekeying* für frische Chiffrier- und Integritätsschlüssel → Key reuse unterbinden.

Message Integrity Code

Im Allgemeinen berechnet ein MIC-Algorithmus einen Hash von den Daten und sendet den berechneten Wert zusammen mit den Daten an den Empfänger. Auf Empfängerseite wird der Hash ebenso berechnet, um ihn im Anschluss mit dem vom Absender der Daten mitgesandten Hash zu vergleichen. Sind beide Werte gleich, dann kann der Empfänger die erhaltene Datensendung als authentisch, d. h. unverfälscht betrachten. Der für die Berechnung des MICs eingesetzte Integritätsschlüssel muss geheim zwischen Sender und Empfänger sein. Ein MIC-Algorithmus ist um so sicherer, je schwieriger es für einen Angreifer ist, den korrekten Hash für eine neue Nachricht auszuwählen, ohne den geheimen Schlüssel zu kennen.

Statt einen der gebräuchlichen MIC-Algorithmen wie z. B. HMAC-SHA1 (IPsec) und DES-CBC-MAC (Finanzapplikationen) verwenden zu können, musste die TGi aufgrund der Hardware-Beschränkungen einen neuen MIC einsetzen: Michael verwendet einen 64 bit Schlüssel, der gemeinsam geheim zwischen den Kommunikationspartnern ist. Der MIC-Algorithmus berechnet einen Hash über die zu versendenden Daten sowie Quell- und Ziel-MAC. Für die Berechnung werden simple Rotationen (Shifts), Additionen und XORs verwendet, sodass der Algorithmus nur 3,5 Zyklen/Byte auf einem ARM7-Prozessor und etwa 5,5 Zyklen/Byte auf einem i486-Prozessor benötigt. Für 802.11b ergeben sich 3,1 Millionen Zyklen/s auf einem ARM7 und 4,8 Millionen Zyklen/s auf einem i486 (Wal02a). Bei einigen Access Points der ersten Generation ist mit Peformanceeinbußen zu rechnen.

Das Sicherheitsmaß eines MICs wird in Bits gemessen. Eine Sicherheit von s bits bedeutet, dass ein Angreifer eine Fälschung für eins von 2^{s-1} Paketen konstruieren kann. Für Michael beträgt diese Sicherheit 20 bit, mehr ist bei den Hardwareanforderungen nicht möglich. Die Entwickler von TKIP sind sich dessen bewusst und fordern deshalb das Aushandeln eines neuen Integritätsschlüssels mit anschließender Sendepause von einer Minute, wenn der MIC eine Fälschung entdeckt. Dies geht auf Kosten der Kommunikation, die dabei leider unterbrochen wird, ist jedoch notwendig, um aktive Angriffe abzuwehren.

Paketsequenzkontrolle

Mit MIC allein ist es für einen Angreifer dennoch möglich, Replay Attacken durchzuführen. Eine Paketsequenzkontrolle nimmt sich diesem Problem an. Jedes Paket wird mit einer Sequenznummer versehen, wobei die Sequenznummer bei jedem Paket um 1 erhöht wird. Erhält der Empfänger ein Paket mit gleichem oder kleinerem Betrag für den Sequenzzähler als der Wert des zuletzt korrekt empfangenen Pakets, dann verwirft er das Paket und erhöht einen internen Zähler für Replay-Attacken.

Der Zähler für die Sequenzkontrolle ist 48 bit groß, wobei das IV-Feld des WEP-Schlüssel verwendet wird. Die Größe von 48 bit stellt sicher, dass dieser Zähler weit länger reicht als die Assoziation eines Funkclient zu einem Access Point. Normalerweise werden Sequenzzähler reinitialisiert (auf Null zurückgesetzt), sobald ein neuer MIC-Schlüssel verwendet wird. Aufgrund der bestehenden Hardwareanforderungen bindet TKIP jedoch das Zurücksetzen des Zählers an den Chiffrierschlüssel.

Per-Packet-Key-Mixing

Bei WEP wurde der Chiffrierschlüssel aus der Konkatenation von dem statischen WEP-Basisschlüssel (48 oder 104 bit) und dem 24 bit langem Initialisierungsvektor gebildet. Der IV sollte einen für jedes Paket unterschiedlichen Schlüssel für den linearen RC4-Algorithmus garantieren. Unter anderem die FMS-Attacke zeigt, dass dieses Ziel nicht erreicht wird.

TKIP führt eine völlig neue Mixfunktion ein, um den jür jedes Paket einzigartigen Chiffrierschlüssel zu generieren. Als Eingabe dazu nimmt es den WEP-Basisschlüssel, die MAC-Adresse des Absenders und die Paketsequenznummer. Die Hinzunahme der Quell-MAC hat den Vorteil, dass das Ergebnis für jeden Host unterschiedlich ist, auch wenn alle Stationen mit dem gleichen Schlüssel operieren.

Um den Rechenaufwand zu minimieren, erfolgt die Mischfunktion in zwei Phasen. Die erste Phase arbeitet mit einer Art Caching. Sie nimmt die MAC-Adresse, den WEP-Schlüssel sowie die ersten 4 Octets (32 von 48 bits) der Paketsequenznummer, um einen Zwischenwert per iterativen XOR zu berechnen. Der so berechnete Wert kann für 2^{16} Pakete verwendet werden.

Die zweite Phase hat die Aufgabe, die Korrelation zwischen bekannten IV (bekannt, weil im Klartext als Zusatz zum Paket mitgesandt) und dem für die Verschlüsselung des Pakets verwendeteten Schlüssels weitestgehend zu beseitigen. Der Algorithmus zur Erreichung einer breiten Streuung des WEP-Schlüssels benutzt wie auch der MIC-Algorithmus einfache Operationen, um den Prozessor nicht übermäßig zu belasten (ungefähr 150 Zyklen für ein Paket). Als Eingabe nimmt der Algorithmus den in Phase 1 berechneten Zwischenwert plus die restlichen 16 bit der Paketsequenznummer und erzeugt den für jedes Paket unterschiedlichen 128-bittigen Schlüssel. Die ersten 3 Bytes entsprechen dem WEP IV, die restlichen 13 Bytes dem WEP-Basisschlüssel — existierende WEP-Hardware geht bekanntlich davon aus, den IV mit dem Basisschlüssel zu konkatenieren, um den Schlüssel für ein Paket zu erhalten.

Rekeying

Entgegen WEP operiert TKIP nicht mehr nur mit einem Schlüssel, sondern benötigt für Michael einen 64 bit MIC-Schlüssel und für die Mixfunktion einen 128 bittigen Schlüssel. TKIP fordert, dass diese Schlüssel bei jeder Zuordnung eines Clients zu einem Access Point frisch vergeben werden. Die TGi adaptiert für TKIP das Schlüsselmanagement von 802.1X.

TKIP definiert eine Hierarchie von drei Schlüsseltypen, um ein sicheres Aushandeln der Schlüssel zu ermöglichen:

1. *Master-Schlüssel* — für die Kommunikation zwischen mobiler Station und Authentication Server. Wird bei Authentifizierung festgelegt und für die sichere Distribution der Chiffrierschlüssel der nächsten Ebene benutzt.

2. *Chiffrierschlüssel für Schlüssel* — zwei Schlüssel: einer für Rekey-Nachrichten, ein zweiter für die Chiffrierung der Schlüssel der nächstunteren Ebene beim Austausch.

3. *temporäre Schlüssel* — 128 bit Chiffrierschlüssel und 64 bittiger MIC-Schlüssel (*2*). Für jede Kommunikationsrichtung wird ein separates Paar dieser Schlüssel verwendet (*2*). Die Schlüssel können für 2^{16} Pakete benutzt werden. Um bei Ablauf dieser Lebenszeit eine Unterbrechung der Kommunikation zu verhinden, werden Nachfolger-Schlüsselpaare vorab ausgehandelt und gespeichert (*2*). Ein Access Point hat demnach für jede Assoziation eines Clients insgesamt $2 \times 2 \times 2 = 8$ temporäre Schlüssel.

4.2 CCMP

CCMP — das Kürzel steht für Counter-Mode-CBC-MAC Protocol — soll wie TKIP alle Schwächen von WEP beheben. Es ist die langfristige Lösung für das WEP-Problem. Dies hat zum Vorteil, dass die Entwickler von CCMP nicht auf die einschränkenden Vorgaben von bereits installierter Hardware achten mussten. So konnte für den Verschlüsselungsalgorithmus die Wahl auf den bewährten AES (Advanced Encryption Standard) fallen.

AES-Modi AES ist eine symmetrische Block-Chiffre (RC4 Stromchiffre), die auf Datenblöcken fester Größe arbeitet. Übliche Modi für AES sind:

- Electronic Codebook (ECB) — verschlüsselt jeden Block einzeln.
- Counter Mode (CTR) — ein Zähler wird verschlüsselt und mit der Nachricht per XOR verknüpft. Für jeden Datenblock wird der Zähler um 1 inkrementiert.

  Der Zähler darf sich nie für den gleichen Schlüssel wiederholen! → Schlüsselmanagement erforderlich.
- Cipher-Block-Chaining (CBC) — am Anfang wird ein zufällig gewählter Initialisierungsvektor ermittelt. Der Initialisierungsvektor wird mit dem Klartext per XOR verknüpft und anschließend verschlüsselt. Für die Verschlüsselung des nächsten Datenblocks wird als Initialisierungsvektor die Chiffre der vorhergehenden Iteration genommen — oder in einfacher Notation:
  FOR $i = (1, n)$ $\{C_i = \text{verschlüssele}(M_i \oplus IV); IV = C_i\}$

  Zu beachten ist, dass der Initialisierungsvektor wirklich zufällig ist.

Für die Erfordernisse von WLAN wurde ein neuer Modus, CCM genannt, entwickelt. CCM benutzt den Counter Mode für die Verschlüsselung und Cipher Block Chaining Message Authentication Code (CBC-MAC) für die Integritätssicherung. Der verwendete Schlüssel ist bei beiden Modi derselbe. Dies ist normalerweise gefährlich, CCM garantiert jedoch, dass sich der Zähler beim Counter Mode und der Initialisierungsvektor des CBC niemals überlappen (CWHWW03; Wal02b).

CCMP Ansonsten hat CCMP viele Gemeinsamkeiten mit TKIP. CCMP benutzt ebenso einen 48 bit Zähler für die Sequenzierung der Pakete. Da AES keine Stromchiffre ist, entfällt die Notwendigkeit für einen gesonderten Schlüssel pro Paket. Eine aufwendige Mix-Funktion wie die in TKIP gibt es somit nicht. Stattdessen kann das CCM-Protokoll für alle Pakete den gleichen AES-Schlüssel verwenden, der IV von 48 bit stellt sicher, dass der AES-Schlüssel weit länger als die Assoziation des mobilen Client benutzt werden kann. Der MIC hat bei CCMP eine Größe von 64 bit (TKIP 20 bit), bietet also mehr Sicherheit als Michael (CWHWW03).

4.3 Vergleich WEP – TKIP – CCMP

Tabelle 2 gibt als Abschluss einen Überblick über die Sicherheitsfeatures der drei Protokolle WEP, TKIP und CCMP (nach (CWHWW03)):

	WEP	TKIP	CCMP
Chiffre	RC4	RC4	AES
Größe des Chiffrierschlüssels	48 oder 104 bit	128 bit für Verschlüsselung, 64 bit für Authentifizierung	128 bit
Lebensdauer des Paketschlüssels	24 bit IV mit Überlauf	48 bit	48 bit
Integritätssicherung der Paketdaten	CRC32	Michael	CCM
Integritätssicherung für den Header	keine	Quell- und Ziel-MAC werden von Michael abgesichert	CCM
Erkennung von Replay-Attacken	keine	IV Sequenzzähler	IV Sequenzzähler
Schlüsselmanagement	keine	IEEE 802.1X	IEEE 802.1X

Tabelle 2: Vergleich der Sicherheitsprotokolle WEP, TKIP und CCMP

4.4 Die Rolle von WPA

Wie bereits in Fußnote 5 angedeutet, lässt die abschließende Ratifizierung von 802.11i auf sich warten. Die WiFi Alliance hat deshalb Teile des neuen Standard vorgenommen und etabliert das ganze unter dem Namen WPA (Wi-Fi Protected Access). Für nähere Informationen sei auf (Hei02) und (Int03) verwiesen.

5 Fazit

Die Sicherheitslücken von WEP sind erschreckend. 1999 wurde IEEE 802.11 verabschiedet, 2001 wurde die FMS-Attacke veröffentlicht. Um so gravierender ist die Tatsache, dass es für die Anwender im Jahre 2003 immer noch keine akzeptable Lösung für die WEP-Problematik gibt. Die Ratifzierung von 802.11i geht schleppend voran, Erweiterungen wie 802.1X und WPA sind selbst löchrig ((MA02) und (Hei02)) oder der Ein-

satz (RADIUS-Server) zu teuer[8]. Der Autor empfiehlt deshalb den Einsatz von IPsec für die zusätzliche Absicherung des Netzes. Außerdem sollte es selbstverständlich sein, dass das WLAN-Funknetz außerhalb des leitungsgebundenen Netzes, sozusagen innnerhalb einer demilitarisierten Zone, betrieben wird.

Wie konnte es passieren, dass WEP so viele gravierende Sicherheitslücken offenbaren muss? Die Autoren in (BGW01) meinen dazu, dass die Fehler von WEP zu vermeiden gewesen wären, da es Standardfehler sind. Zum einen hätte WEP die Erfahrungen, die im Design von anderen Protokollen gemacht wurden — z. B. von IPsec, das zwar andere, aber vergleichbare Ziele verfolgt — nutzen können. Zum anderen wurde der Standard von Netzwerktechnikern entworfen, die die Benutzung von CRC32 und RC4 mehr aus der Ingenieur-Sicht (einfache Implementation und akzeptable Geschwindigkeit) gesehen haben und wenige Know-How bei Sicherheitsalgorithmen haben. Sicherheitsstandards respektive Sicherheitsalgorithmen werden als um so sicherer angesehen, wenn sie von vielen Kryptographen begutachtet werden. Der Fakt, dass die Einsicht eines IEEE-Standards einiges an Geld kostet, hatte hier eine große hemmende Wirkung. Vielen aus der Kryptography-Gemeinschaft blieb die Begutachtung von WEP verwehrt.

Zu hoffen ist, dass durch die Involvierung von mehr Sicherheitsexperten und die — womöglich positiv zu sehende — länger andauernde Ratifizierung des Nachfolgestandards 802.11i ein besseres Sicherheitsprotokoll für Wireless LANs entwickelt wird.

Literatur

[BGW01] Borisov, Nikita, Ian Goldberg und David Wagner: *Intercepting mobile communications: the insecurity of 802.11*. In: *Proceedings of the seventh annual international conference on Mobile computing and networking*, Seiten 180–189. ACM Press, Juli 2001. http://doi.acm.org/10.1145/381677.381695.

[Bre02] Bremmer, Manfred: *WLAN: Kostenlos durch Sicherheitslücken surfen*. Computerwoche, 45, 8. November 2002. http://www1.computerwoche.de/index.cfm?pageid=255&artid=42849&type=detail&category=143.

[Cor02] Corbett, Cherita: *Security for 802.11 Wireless Networks — Current Flaws, New Standards, and Today's Alternatives*. Technischer Bericht, Dept. of Electrical and Computer Engineering, Georgia Institute of Technology, Dezember 2002. http://www.prism.gatech.edu/~gt0369c/Security_survey.pdf.

[CWHWW03] Cam-Winget, Nancy, Russ Housley, David Wagner und Jesse Walker: *Security flaws in 802.11 data link protocols*. Communications of the ACM, 46(5):35–39, 2003. http://doi.acm.org/10.1145/769800.769823.

[8] Die Fakultät Informatik der TU Dresden führt dies als Grund in http://www.inf.tu-dresden.de/index.php?itemid=f0073a an.

[Eck03] ECKERT, CLAUDIA: *IT-Sicherheit: Konzepte, Verfahren, Protokolle*, Kapitel 13.3, Seiten 658–675. Oldenbourg, 2003.

[FC02] FARIA, DANIEL B. und DAVID R. CHERITON: *DoS and authentication in wireless public access networks*. In: *Proceedings of the ACM workshop on Wireless security*, Seiten 47–56. ACM Press, 2002. http://doi.acm.org/10.1145/570681.570687.

[FMS01] FLUHRER, SCOTT, ITSIK MANTIN und ADI SHAMIR: *Weaknesses in the Key Scheduling Algorithm of RC4*. In: *Selected Areas in Cryptography: 8th Annual International Workshop*, LNCS 2259, Seiten 1–24. Springer-Verlag, 2001. http://www.springerlink.com/openurl.asp?genre=article&issn=0302-9743&volume=2259&spage=1.

[Hei02] HEISE NEWS-TICKER: *Verbesserung für WLAN-Sicherheit*, 31. Oktober 2002. http://www.heise.de/newsticker/data/ea-31.10.02-000/.

[Hei03a] HEISE NEWS-TICKER: *Funknetze: Nachbesserung für mehr Sicherheit verspätet sich*, 25. Februar 2003. http://www.heise.de/newsticker/data/ea-25.02.03-000/.

[Hei03b] HEISE NEWS-TICKER: *Standard für schnelles WLAN ratifiziert*, 13. Juni 2003. http://www.heise.de/newsticker/data/ea-13.06.03-000/.

[Int03] INTERLINK NETWORKS: *Link Layer and Network Layer Security for Wireless Networks*, 15. Mai 2003. http://www.forum-intrusion.com/Link_and_Network_Layer_Whitepaper.pdf.

[MA02] MISHRA, ARUNESH und WILLIAM A. ARBAUGH: *An Initial Security Analysis of the IEEE 802.1X Standard*. Technischer Bericht, Dept. of Computer Science, University of Maryland, 6. Februar 2002. http://www.cs.umd.edu/~waa/1x.pdf.

[Wal02a] WALKER, JESSE: *802.11 Security Series, Part II: The Temporal Key Integrity Protocol (TKIP)*. Technischer Bericht, Platform Networking Group, Intel Corporation, 2002? http://cedar.intel.com/media/pdf/security/80211_part2.pdf.

[Wal02b] WALKER, JESSE: *802.11 Security Series, Part III: AES-based Encapsulation of 802.11 Data*. Technischer Bericht, Platform Networking Group, Intel Corporation, 2002? http://cedar.intel.com/media/pdf/security/80211_part3.pdf.

[Zoe] ZOETEMELK, JAN: *Intro to VPNs*. http://www.unit4agresso.com/unit4securitysolutions/customers/5_Intro%20To%20VPNs_SHORT_Jan%20Zoetemelk.ppt.