LANCOM™ Techpaper
WPA und 802.11i

1 Einleitung

Die WLAN-Standards WPA und 802.11i sind dabei, den in der Vergangenheit stark angegriffenen Ruf von WLANs bezüglich der Sicherheit wieder herzustellen. Die im originalen Standard vorgesehenen Verfahren haben sich in der Praxis als unzureichend erwiesen. Dieser Mangel führte zum einen zu einer Reihe von proprietären Erweiterungen des Standards wie 'CKIP' von Cisco oder 'KeyGuard' von Symbol Technologies, zum anderen zu Lösungen, die auf höheren Protokollschichten mit Mitteln wie PPTP oder IPSec die benötigte Sicherheit bieten. All diese Verfahren funktionieren zwar prinzipiell, bringen auf der anderen Seite jedoch Einschränkungen, z.B. bezüglich der Interoperabilität oder des Datendurchsatzes.

Mit dem kürzlich verabschiedeten Standard 802.11i hat das IEEE-Komitee das Thema 'WLAN und Sicherheit' von Grund auf neu definiert. Das Resultat sind standardisierte Methoden, die den Aufbau von sicheren und herstellerübergreifenden WLANs nach aktuellen Maßstäben ermöglichen.

Auf dem Weg vom ursprünglichen WEP des 802.11-Standards bis zu 802.11i sind dabei eine ganze Reihe von Begriffen entstanden, die teilweise eher zu einer Verwirrung und Verunsicherung der Anwender geführt haben. Das vorliegende Dokument soll helfen, die Begriffe zu erklären und die verwendeten Verfahren in der chronologischen Reihenfolge ihrer Entwicklung zu erläutern.

2 Einige Grundbegriffe

Auch wenn immer wieder in Zusammenhang mit Computernetzen pauschal von 'Sicherheit' gesprochen wird, so ist es doch für die folgenden Ausführungen wichtig, die dabei gestellten Forderungen etwas näher zu differenzieren. Als ersten Punkt der Sicherheit betrachten wir den Zugangsschutz:

- Dabei handelt es sich zum einen um einen Schutzmechanismus, der nur autorisierten Nutzern den Zugang zum Netzwerk gewährt.
- Zum anderen soll aber auch sicherstellt werden, dass der Client sich mit genau dem gewünschten Access Point verbindet, und nicht mit einem von unbefugten Dritten eingeschmuggelten Access Point mit dem gleichen Netzwerk-Namen. So eine Authentifizierung kann z.B. durch Zertifikate oder Passwörter gewährleistet werden.
- Ist der Zugang einmal gewährt, so möchte man sicherstellen, dass Datenpakete den Empfänger unverfälscht erreichen, d.h. dass niemand die Pakete verändert oder andere Daten in den Kommunikationsweg einschleusen kann. Die Manipulation der Datenpakete selbst kann man nicht verhindern; aber man kann durch geeignete Prüfsummenverfahren veränderte Pakete identifizieren und verwerfen.

Von den Zugangsschutz getrennt zu sehen ist die Vertraulichkeit, d.h. unbefugte Dritte dürfen nicht in der Lage sein, den Datenverkehr mitzulesen. Dazu werden die Daten verschlüsselt. Solche Verschlüsselungsverfahren sind z.B. DES, AES, RC4 oder Blowfish. Zur Verschlüsselung gehört natürlich auf der Empfängerseite eine entsprechende Entschlüsselung, üblicherweise mit dem gleichen Schlüssel (so genannte symmetrische Verschlüsselungsverfahren). Dabei ergibt sich natürlich das Problem, wie der Sender dem Empfänger den verwendeten Schlüssel erstmalig mitteilt – eine einfache Übertragung könnte von einem Dritten sehr einfach mitgelesen werden, der damit den Datenverkehr leicht entschlüsseln könnte.

Im einfachsten Fall überlässt man dieses Problem dem Anwender, d.h. man setzt die Möglichkeit voraus, dass er die Schlüssel auf beiden Seiten der Verbindung bekannt machen kann. In diesem Fall spricht man von Pre-Shared-Keys oder kurz 'PSK'.

Ausgefeiltere Verfahren kommen dann zum Einsatz, wenn der Einsatz von Pre-Shared-Keys nicht praktikabel ist, z.B. in einer über SSL aufgebauten HTTP-Verbindung – hierbei kann der Anwender nicht so einfach an den Schlüssel von einem entfernten Web-Server gelangen. In diesem Falle werden so genannte asymmetrische Verschlüsselungsverfahren wie z.B. RSA eingesetzt, d.h. zum Entschlüsseln der Daten wird ein anderer Schlüssel als zum Verschlüsseln benutzt. Solche Verfahren sind jedoch viel langsamer als symmetrische Verschlüsselungsverfahren, was zu einer zweistufigen Lösung führt: eine Seite verfügt über ein asymmetrisches Schlüsselpaar und überträgt den Teil zum Verschlüsseln an die andere Seite, üblicherweise als Teil eines Zertifikats. Die Gegenseite wählt einen beliebigen symmetrischen Schlüssel aus und verschlüsselt diesen symmetrischen Schlüssel mit dem zuvor von der Gegenseite erhaltenen asymmetrischen Schlüssel. Den kann der Inhaber des asymmetrischen Schlüsselpaars wieder entschlüsseln, ein potentieller Mithörer aber nicht – das Ziel des gesicherten Schlüsselaustauschs ist erreicht.

In den folgenden Abschnitten werden uns solche Verfahren wieder begegnen, zum Teil auch in etwas modifizierter Form.

LANCOM Systems

3 WEP

WEP ist eine Abkürzung für **W**ired **E**quivalent **P**rivacy. Die primäre Zielsetzung von WEP ist die Vertraulichkeit von Daten. Im Gegensatz zu Signalen, die über Kabel übertragen werden, breiten sich Funkwellen beliebig in alle Richtungen aus – auch auf die Straße vor dem Haus und an andere Orte, wo sie gar nicht erwünscht sind. Das Problem des unerwünschten Mithörens tritt bei der drahtlosen Datenübertragung besonders augenscheinlich auf, auch wenn es prinzipiell auch bei größeren Installationen kabelgebundener Netze vorhanden ist – allerdings kann man den Zugang zu Kabeln durch entsprechende Organisation eher begrenzen als bei Funkwellen.

Das IEEE-Komitee hat bei der Entwicklung der WLAN-Sicherheitsstandards nicht geplant, ein 'perfektes' Verschlüsselungsverfahren zu entwerfen. Solche hochsicheren Verschlüsselungsverfahren werden z.B. für Electronic-Banking verlangt und auch einsetzt – in diesen Fällen bringen allerdings die Anwendungen selber entsprechend hochwertige Verschlüsselungsverfahren mit, und es wäre unnötig, diesen Aufwand nochmals auf der Ebene der Funkübertragung zu treiben. Mit den neuen Sicherheitsstandards sollte lediglich solchen Anwendungen, die in kabelgebundenen LANs üblicherweise ohne Verschlüsselung arbeiten, eine ausreichende Sicherheit gegen das Mitlesen durch unbefugte Dritte ermöglicht werden.

Abbildung 1 zeigt den Ablauf der WEP-Verschlüsselung – die Entschlüsselung verläuft genau umgekehrt. WEP ist also ein symmetrisches Verschlüsselungsverfahren. WEP benutzt als Basistechnologie zur Verschlüsselungs den RC4-Algorithmus, ein in anderen Bereichen bereits bekanntes und durchaus als sicher eingestuftes Verfahren. RC4 benutzt einen zwischen 8 und 2048 Bit langen Schlüssel, aus dem nach einem festgelegten Verfahren eine pseudo-zufällige Folge von Bytes erzeugt wird. Das Datenpaket wird dann sukzessive Byte für Byte mit diesem Byte-Strom XOR-verknüpft. Der Empfänger wiederholt einfach diesen Vorgang mit dem gleichen Schlüssel und damit der gleichen Folge, um wieder das ursprüngliche Datenpaket zu erhalten – eine doppelte Anwendung der XOR-Verknüpfung mit den gleichen Werten hebt sich auf.

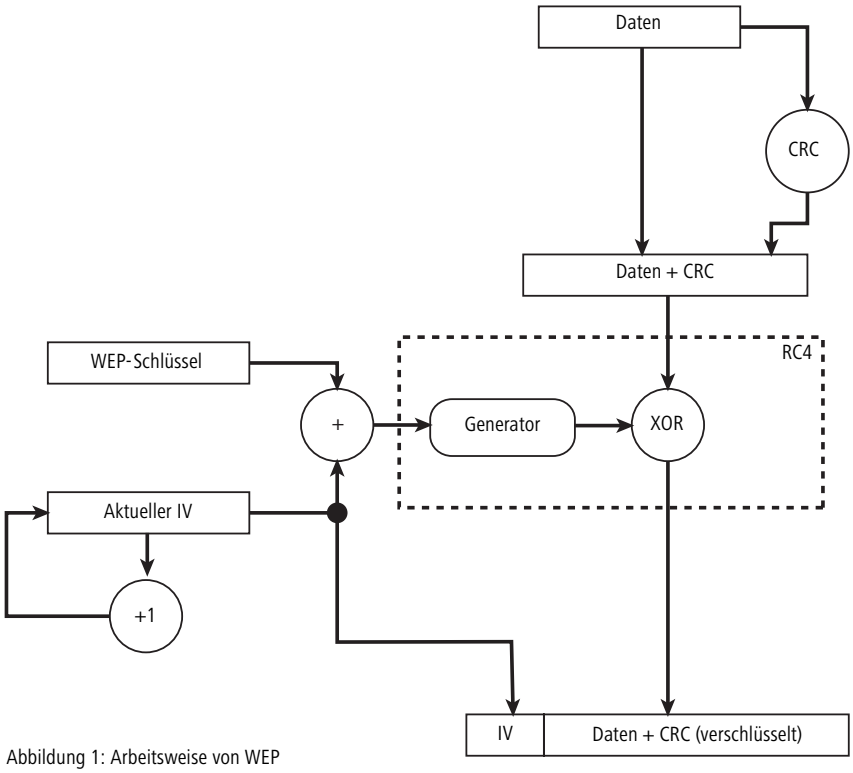

Abbildung 1: Arbeitsweise von WEP

Der Vorteil von RC4 ist, dass die Operationen

- Erzeugung der Byte-Folge aus dem Schlüssel
- XOR-Verknüpfung mit dem Datenstrom

auf Sender- und Empfängerseite identisch sind – man braucht die Hardware also nur einmal in die WLAN-Karte einzubauen und kann sie sowohl zum Senden als auch Empfangen benutzen. Da die Daten im WLAN ohnehin nur halbduplex übertragen werden, wird auch nie gleichzeitig gesendet und empfangen. RC4 hat aber einen gravierenden Nachteil: man darf einen bestimmten RC4-Schlüssel nur einmal für ein einziges Paket verwenden! Verwendet man den gleichen RC4-Schlüssel für zwei verschiedene Datenpakete, so kann ein potentieller Mithörer diese beiden Pakete mitschneiden und miteinander XOR-Verknüpfen. Durch diese Operation erhält man zwar noch nicht direkt Klartext, aber die Pseudo-Zufallsfolge und damit die Verschlüsselung fällt heraus, man hat die XOR-Verknüpfung zweier Klartextpakete. Wenn man dazu den Inhalt eines der beiden Pakete kennt, kann daraus das andere Klartextpaket ermittelt werden. WEP ver-

wendet daher den vom Benutzer eingegebenen Schlüssel nicht direkt für den RC4-Algorithmus, sondern kombiniert diesen mit einem sogenannten **I**nitial **V**ector (IV) zum eigentlichen RC4-Schlüssel. Diesen IV wechselt der Sender automatisch von Paket zu Paket, üblicherweise durch einfaches Inkrementieren, und überträgt ihn zusammen mit dem verschlüsselten Paket. Der Empfänger nutzt den im Paketübertragenen IV, um den für dieses Paket verwendeten RC4-Schlüssel zu konstruieren.

Desweiteren berechnet WEP über das unverschlüsselte Paket noch eine CRC-Prüfsumme und hängt sie an das Paket an, bevor es RC4-verschlüsselt wird. Der Empfänger kann nach der Entschlüsselung diese CRC-Prüfsumme überprüfen und feststellen, ob die Entschlüsselung fehlerhaft war – z.B. durch einen falschen WEP-Schlüssel. Auf diese Weise bietet WEP übrigens einen gewissen Grad an Zugangsschutz, weil ein Eindringling ohne Kenntnis des WEP-Schlüssels nur 'defekte' Pakete erzeugt, die in der WLAN-Karte ausgefiltert werden.

Aus dem zusätzlichen IV erklärt sich die bisweilen auftretende Verwirrung um die Schlüssellänge bei WEP – da sich größere Schlüssellängen sicherer anhören, werden die 24 Bit des IV gerne zur eigentlichen Schlüssellänge hinzuaddiert, obwohl der Anwender selber natürlich nur den Rest konfigurieren kann. Der IEEE-Standard sah ursprünglich eine relativ kurze Schlüssellänge von 40 Bit vor, die sich wahrscheinlich an den damals existierenden US-Exportbeschänkungen für starke Kryptographie orientierte – diese Variante wird in Prospekten meist als WEP64 bezeichnet. Die meisten WLAN-Karten unterstützen heutzutage eine Variante, bei der Anwender einen 104 Bit langen Schlüssel konfigurieren kann, was einen 128 Bit langen RC4-Schlüssel ergibt – folgerichtig wird dies oft als WEP128 bezeichnet. Seltener finden sich Schlüssellängen von 128 Bit (WEP152) oder 232 Bit (WEP256).

Wie oben erwähnt, kann RC4 prinzipiell mit Schlüssellängen bis zu 2048 Bit arbeiten, was WEP-Schlüsseln bis zu 2024 Bit entsprechen würde. In der Praxis stoßen die Schlüssellängen an die einfache Grenze, bis zu der ein Anwender die Zahlenkolonnen noch fehlerfrei eingeben kann. Da WEP ein reines PSK-Verfahren ist, müssen die Schlüssel auf beiden Seiten der Verbindung identisch eingetragen werden. Der IEEE-Standard sieht keinerlei Mechanismen vor, die WEP-Schlüssel in einem WLAN automatisch zu verteilen. Einige Hersteller haben z.B. versucht, dem Anwender das Eintippen zu erleichtern, indem nicht die WEP-Schlüssel selbst eingetragen werden, sondern eine Passphrase (also eine Art überlanges Passwort), aus der die Schlüssel berechnet werden. Dieses Verfahren variiert allerdings von Hersteller zu Hersteller, so dass die gleiche Passphrase bei verschiedenen Herstellern zu unterschiedlichen WEP-Schlüsseln führen kann – außerdem haben Anwender die Tendenz, relativ einfach zu ratende Passwörter zu verwenden, so dass die entstehenden Schlüssel meist schwächer als 40 bzw. 104 Bit sind (die aktuellen IEEE-Standards gehen z.B. davon aus, dass ein typisches Paßwort eine Stärke von etwa 2,5 Bit pro Zeichen ausweist).

Der IEEE-Standard sieht vor, dass in einem WLAN bis zu vier verschiedene WEP-Schlüssel existieren können. Der Sender kodiert in das verschlüsselte Paket neben dem IV die Nummer des verwendeten WEP-Schlüssels, so dass der Empfänger den passenden Schlüssel verwenden kann. Die Idee dahinter war, dass sich so alte Schlüssel in einem WLAN graduell gegen neue Schlüssel austauschen lassen, indem Stationen, die den neuen Schlüssel noch nicht erhalten haben, für eine übergangszeit noch einen alten Schlüssel weiter verwenden können.

Auf Basis von WEP definiert der 802.11-Standard auch ein Challenge-Response-Verfahren zur Authentifizierung von Clients. Dazu schickt der Access Point ein Klartextpaket, das einen 128 Byte langen Challenge enthält, den der Client per WEP verschlüsselt und zurückschickt. Wenn der Access Point diese Antwort erfolgreich entschlüsseln kann (d.h. die CRC stimmt) und wieder den ursprünglich gesendeten Challenge erhält, geht er davon aus, dass der Client über korrekte WEP-Schlüssel verfügt und daher zum Zugriff berechtigt ist.

Leider stellt dieses Verfahren einem potentiellen Angreifer 128 Byte Klartext und den zugehörigen verschlüsselten Text bereit, was Ansätze zur Krypto-Analyse bietet. Des weiteren implementieren viele Clients dieses Variante nicht, so dass dieses Shared Key genannte Verfahren selten angewendet wird – stattdessen werden heutzutage zur Authentifizierung der WLAN-Anmeldung nachgeschaltete Verfahren wie z.B. 802.1x (s.u.) benutzt.

Während das WEP-Verfahren in der Theorie bisher relativ gut klingt, haben sich leider in der Praxis schwerwiegende Fehler im Verfahren gefunden, welche die Vorteile deutlich reduzieren – und zwar unabhängig von der verwendeten WEP-Schlüssellänge. Diese Schwächen hätten sich bei einer genauen Analyse eigentlich bereits bei der Definition von WEP finden müssen. Leider waren bei der WEP-Definition keine Kryptologie-Experten beteiligt, so dass diese Fehler erst offensichtlich wurden, als das WEP-Verfahren mit dem Markterfolg von 802.11b-WLAN-Karten massenweise eingesetzt wurde (frühere 2MBit-Designs enthielten oft gar keine Verschlüsselung – WEP ist eine optionale Funktion im 802.11-Standard).

Die Hauptschwäche von WEP ist die viel zu kurze IV-Länge. Wie bereits erwähnt, ist die Wiederverwendung eines Schlüssels bei RC4 eine große Sicherheitslücke – das passiert bei WEP aber spätestens alle 16 Millionen Pakete, wenn der IV-Zähler von 0xffffff auf Null überläuft. Ein 11Mbit-WLAN erreicht eine Nettodatenrate von ca.

5MBit/s, bei einer maximalen Paketlänge von 1500 Bytes sind das also ca. 400 Pakete pro Sekunde bei vollem Durchsatz. Nach etwa 11 Stunden würde der IV-Zähler theoretisch überlaufen und ein Mithörer bekommt die benötigten Informationen zum 'Knacken' des WEP-Schlüssels. In der Praxis bekommt der Angreifer die gesuchten Informationen sogar noch viel früher. Mathematische Analysen von RC4 haben ergeben, dass man bei bestimmten Werten des RC4-Schlüssels schon Rückschlüsse auf die ersten Werte der sich ergebenden Pseudo-Zufallsfolge machen kann – also auf die Bytes, mit denen der Anfang des Paketes verschlüsselt wird. Diese Eigenschaft von RC4 lässt sich relativ leicht umgehen, indem man z.B. die ersten Bytes des pseudo-zufälligen Byte-Stroms verwirft und erst die 'späteren' Bytes zur Verschlüsselung heranzieht, und dies wird heutzutage auch häufig beim Einsatz von RC4 getan. Als diese Erkenntnisse bekannt wurden, war WEP aber in der beschriebenen Form bereits Teil des IEEE-Standards und unabänderlich in die Hardware der weit verbreiteten WLAN-Karten eingeflossen.

Dummerweise sind diese 'schwachen' Werte von RC4-Schlüsseln an bestimmten Werten in den ersten Bytes des RC4-Schlüssels zu erkennen, und das ist bei WEP der in jedem Paket im Klartextübertragene IV. Nachdem dieser Zusammenhang bekannt wurde, tauchten im Internet schnell spezialisierte Sniffer-Tools auf, die nur auf Pakete mit solchen 'schwachen IVs' lauschen, und die dadurch nur einen Bruchteil des gesamten Verkehrs mitschneiden müssen. Je nach Datenaufkommen in einem WLAN können solche Tools die Verschlüsselung in einem Bruchteil der oben genannten Zeit knacken. Bei längeren WEP-Schlüsseln (z.B. 104 statt 40 Bit) dauert dies zwar etwas länger, aber der Zeitaufwand zum Knacken wächst bestenfalls linear mit der Schlüssellänge, nicht exponentiell, wie man dies sonst kennt.

Leider hat auch die in den Paketen enthaltene CRC-Prüfsumme nicht das gehalten, was man sich von ihr versprach. Es wurden Wege gefunden, mit denen man unter bestimmten Bedingungen verschlüsselte Pakete auch ohne Kenntniss des WEP-Schlüssels so verändern kann, dass nach der Entschlüsselung auf Empfängerseite die CRC immer noch stimmt. WEP kann daher also nicht garantieren, dass ein Paket auf dem Weg vom Sender zum Empfänger nicht verändert wurde.

Diese Schwachstellen degradierten WEP leider zu einem Verschlüsselungsverfahren, das bestenfalls zum Schutz eines Heimnetzwerkes gegen 'zufällige Lauscher' taugt. Diese Erkenntnisse haben für einigen Aufruhr gesorgt, WLAN den Ruf einer unsicheren Technologie eingetragen und die Hersteller zum Handeln gezwungen. WLAN ist aber eine standardisierte Technologie, und bessere Standards entstehen nicht von heute auf morgen – deshalb gibt bzw. gab es bis zu einer wirklich sicheren Lösung einige Zwischenschritte, welche die schlimmsten Design-Fehler von WEP zumindest abmildern.

4 WEPplus

Wie im vorangegangenen Abschnitt ausgeführt, ist die Verwendung 'schwacher' IV-Werte das Problem gewesen, welches das WEP-Verfahren am stärksten schwächt. Nur wenige Wochen nach der Veröffentlichung tauchten Tools wie 'WEP-Crack' oder 'AirSnort' im Internet auf, die automatisiert eine beliebige WLAN-Verbindung innerhalb weniger Stunden knacken konnten. WEP war damit faktisch wertlos geworden.

Ein erster 'Schnellschuss', um WLANs gegen solche Programme zu sichern, war die einfache Überlegung, dass die schwachen IV-Werte bekannt sind und man sie beim Verschlüsseln einfach überspringen kann – da der verwendete IV ja im Paket mit übertragen wird, ist so eine Vorgehensweise voll kompatibel gegenüber WLAN-Karten, die diese WEPplus getaufte Erweiterung nicht kennen. Eine echte Verbesserung der Sicherheit erhält man natürlich erst dann, wenn alle Partner in einem WLAN diese Methode benutzen.

Ein potentieller Angreifer ist in einem mit WEPplus ausgestatteten Netzwerk wieder darauf angewiesen, den ganzen Datenverkehr mitzuschneiden und auf IV-Wiederholungen zu warten – es reicht nicht mehr aus, nur auf die wenigen Pakete mit schwachen IVs zu warten. Das legte die Latte für einen Angreifer schon wieder höher, insbesondere wenn man beim Initialisieren einer WLAN-Karte den IV-Zähler nicht einfach auf Null, sondern einen zufälligen Wert initialisiert: der IV-Zähler in einem Access Point beginnt ja erst dann zu zählen, wenn sich die erste Station einbucht und mit der Datenübertragung beginnt. Wenn Access Point und Station ihre IV-Zähler jeweils einfach auf Null initialisieren, erhält man damit praktisch sofort nach dem Start der Verbindung Pakete mit identischen IV-Werten. Durch die Initialisierung auf einen zufälligen Wert kann man die Kollision so wenigstens um durchschnittlich 223 Pakete verzögern, also den halben Raum möglicher IVs – bei mehr als einer Station in einem WLAN reduziert sich dieser Wert natürlich. WEPplus ist daher bei sachlicher Betrachtung nur eine leichte Verbesserung – aber es war geeignet, die Anwenderschaft wieder so weit zu beruhigen, WEP wenigstens für den Heimgebrauch wieder akzeptabel zu machen (solange man häufig genug neue Schlüssel konfiguriert). Für den Einsatz im professionellen Umfeld reichte das natürlich nicht.

5 EAP und 802.1x

Es liegt auf der Hand, dass ein 'Zusatz' wie WEPplus das grundsätzliche Problem des zu kurzen IVs nicht aus der Welt schaffen kann, ohne das Format der Pakete auf dem WLAN zu ändern und damit inkompatibel zu allen bisher existierenden WLAN-Karten zu werden. Es gibt aber eine Möglichkeit, mehrere der aufgetauchten Probleme mit einer zentralen Änderung zu lösen: man verwendet nicht mehr wie bisher die fest konfigurierten WEP-Schlüssel und handelt sie stattdessen dynamisch aus. Als dabei anzuwendendes Verfahren hat sich dabei das Extensible Authentication Protocol durchgesetzt. Wie der Name schon nahelegt, ist der ursprüngliche Zweck von EAP die Authentifizierung, d.h. der geregelte Zugang zu einem WLAN – die Möglichkeit, einen für die folgende Sitzung gültigen WEP-Schlüssel zu installieren, fällt dabei sozusagen als Zusatznutzen ab. Abbildung 2 zeigt den grundsätzlichen Ablauf einer mittels EAP geschützten Sitzung.

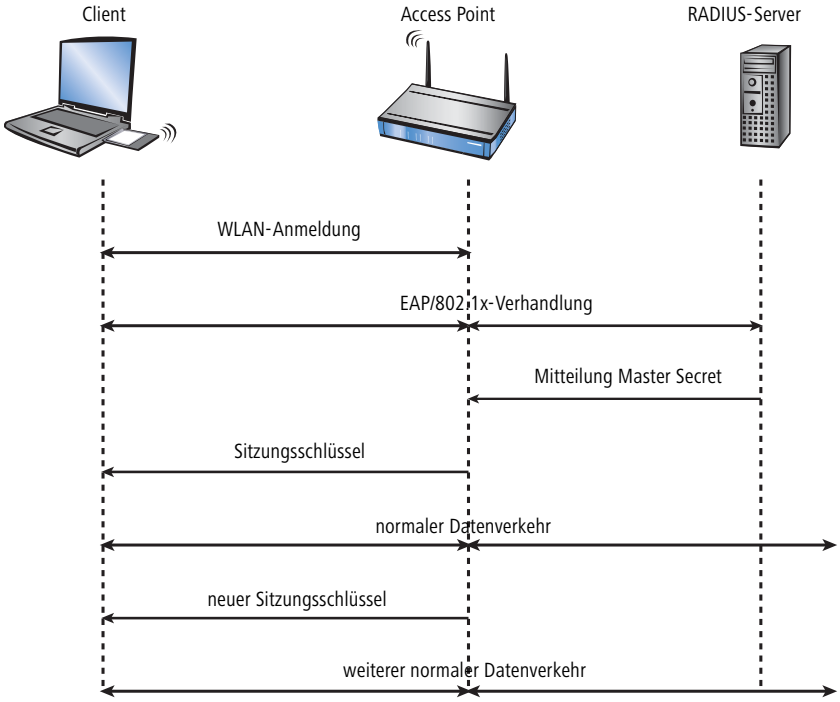

Abbildung 2: Schematischer Ablauf einer WLAN-Sitzung mit EAP/802.1x

In der ersten Phase meldet sich der Client wie gewohnt beim Access Point an und erreicht einen Zustand, in dem er bei normalem WEP oder WEPplus jetzt über den Access Point Daten senden und empfangen könnte – nicht so jedoch bei EAP, denn in diesem Zustand verfügt der Client ja noch über keinerlei Schlüssel, mit denen man den Datenverkehr vor Abhören schützen könnte. Stattdessen steht der Client aus Sicht des Access Points in einem 'Zwischenzustand', in dem er nur bestimmte Pakete vom Client weiter leitet, und diese auch nur gerichtet an einen Authentifizierungs-Server. Bei diesen Paketen handelt es sich um das bereits erwähnte EAP/802.1x, das sich an ihrem Ethernet-Typ 0x888e zweifelsfrei von sonstigen Protokollen unterscheiden lässt. Der Access Point verpackt diese Pakete in RADIUS-Anfragen um und reicht sie an den Authentifizierungs-Server weiter. Umgekehrt wandelt der Access Point darauf vom RADIUS-Server kommende Antworten wieder in EAP-Pakete um und reicht sie an den Client weiter.

Der Access Point dient dabei sozusagen als 'Mittelsmann' zwischen Client und Server: er muss den Inhalt dieser Pakete nicht prüfen, er stellt lediglich sicher, dass kein anderer Datenverkehr von oder zu dem Client erfolgen kann.

Dieses Verfahren hat zwei Vorteile:

- Der Implementierungsaufwand im Access Point ist gering. Während Client und Server meist PCs mit vergleichsweise beliebig viel Ressourcen sind, sind Access Points Geräte, die sowohl hinsichtlich Speicherplatz als auch Rechenleistung beschränkt sind.
- Neue Verfahren zur Authentifizierung erfordern kein Firmware-Upgrade auf dem Access Point.

Über den so gebildeten Tunnel durch den Access Point versichern sich Client und Server nun ihrer gegenseitigen Authentizität, d.h. der Server überprüft die Zugangsberechtigung des Clients zum Netz, und der Client überprüft, ob er wirklich mit dem richtigen Netz verbunden ist. Von Hackern aufgestellte 'wilde' Access Points lassen sich so erkennen.

Es gibt eine ganze Reihe von Authentifizierungsverfahren, die in diesem Tunnel angewendet werden können. Ein gängiges (und von Windows XP unterstütztes) Verfahren ist z.B. TLS, bei dem Server und Client Zertifikate austauschen, ein anderes ist TTLS, bei dem nur der Server ein Zertifikat liefert – der Client authentifiziert sich über einen Benutzernamen und ein Paßwort.

Nachdem die Authentifizierungsphase angeschlossen ist, ist gleichzeitig ein auch ohne WEP-Verschlüsselung gesicherter

Tunnel entstanden, in den im nächsten Schritt der Access Point eingebunden wird.

Dazu schickt der RADIUS-Server das sogenannte 'Master Secret', einen während der Verhandlung berechneten Sitzungsschlüssel, zum Access Point. Obwohl das LAN hinter dem Access Point in diesem Szenario als sicher betrachtet wird, erfolgt auch diese Übertragung verschlüsselt.

Mit diesem Sitzungsschlüssel übernimmt der Access Point jetzt den gebildeten Tunnel und kann ihn nutzen, um dem Client die eigentlichen WEP-Schlüssel mitzuteilen. Je nach Fähigkeiten der Access-Point-Hardware kann das ein echter Sitzungsschlüssel sein (d.h. ein WEP-Schlüssel, der nur für Datenpakete zwischen dem Access Point und genau diesem Client benutzt wird) oder ein sogenannter Gruppenschlüssel, den der Access Point für die Kommunikation mit mehreren Clients benutzt. Klassische WEP-Hardware kennt meistens nur Gruppenschlüssel, nämlich die im Kapitel über WEP erwähnten vier.

Der besondere Vorteil dieses Verfahrens ist es, dass der Access Point über den EAP-Tunnel die WEP-Schlüssel regelmäßig wechsel kann, d.h. ein sogenanntes Rekeying durchführen kann. Auf diese Weise lassen sich WEP-Schlüssel gegen andere ersetzen, lange bevor sie durch IV-Kollisionen Gefahr laufen, geknackt zu werden. Eine gängige 'Nutzungszeit' für so einen WEP-Schlüssel sind z.B. 5 Minuten.

Zu den weiteren Vorteil dieses Verfahrens zählt die einfache Implementation im Access Point mit geringen Erweiterungen auf existierender Hardware. Nachteilig ist bei diesem Verfahren seine Komplexität: Die Pflege des zentralen RADIUS-Servers und der dort gespeicherten Zertifikate ist im allgemeinen nur in größeren Einrichtungen mit separater IT-Abteilung möglich – für den Heimgebrauch oder kleinere Unternehmen ist es weniger geeignet. Des weiteren ist bisher nirgendwo eine Mindestmenge an Verfahren festgelegt, die ein Client bzw. ein Server unterstützen müssen. Es sind also durchaus Szenarien denkbar, in denen ein Client und ein Server keinen EAP-Tunnel aufbauen können, weil die Menge unterstützter Verfahren nicht übereinstimmt. Diese praktischen Hürden haben den Einsatz von EAP/802.1x daher bisher auf professionellen Bereich beschränkt – der Heimanwender musste sich weiterhin mit bestenfalls WEPplus begnügen, oder sich selber auf Anwendungsebene um das Sicherheitsproblem kümmern.

6 TKIP und WPA

Wie in den letzten Abschnitten klar geworden sein sollte, ist der WEP-Algorithmus prinzipiell fehlerhaft und unsicher; die bisherigen Maßnahmen waren im wesentlichen entweder 'Schnellschüsse' mit nur geringen Verbesserungen oder so kompliziert, dass sie für den Heimbenutzer oder kleine Installationen schlicht unpraktikabel sind.

Die IEEE hatte nach Bekanntwerden der Probleme mit WEP eine Task Group gegründet, die sich mit der Definition besserer Sicherungsmechanismen befassen sollte, und die schließlich in den Standard IEEE 802.11i münden sollten. Die Ausarbeitung und Ratifizierung eines solchen Standards dauert jedoch üblicherweise mehrere Jahre. Zwischenzeitlich war der Druck aus dem Markt so groß geworden, dass man in der Industrie nicht mehr auf die Fertigstellung von 802.11i warten konnte und wollte. Unter Federführung von Microsoft wurde daher von der WiFi-Alliance, der 'Standard' Wifi Protected Access (WPA) definiert. Die WiFi-Alliance ist ein Zusammenschluss von WLAN-Herstellern, der die herstellerübergreifende Funktion von WLAN-Produkten fördern möchte und z.B. das Wifi-Logo vergibt.

Bei der Definition von Standards, so auch bei 802.11i, sind die grundlegenden Mechanismen üblicherweise recht schnell klar. Die Verabschiedung der Standards ziehen sich meistens aufgrund von unterschiedlichen Detailauffassungen in die Länge. Diese Details sind dann aber häufig nur für seltene Anwendungen wichtig. WPA ging deshalb den pragmatischen Weg, die bereits klaren und für den Markt wichtigen Dinge aus den Entwürfen von 802.11i herauszunehmen und in einen eigenen Standard zu packen. Zu diesen Details gehören im einzelnen:

- TKIP und Michael als Ersatz für WEP
- Ein standardisiertes Handshake-Verfahren zwischen Client und Access Point zur Ermittlung/Übertragung der Sitzungsschlüssel.
- Ein vereinfachtes Verfahren zur Ermittlung des im letzten Abschnitt erwähnten Master Secret, das ohne einen RADIUS-Server auskommt.
- Aushandlung des Verschlüsselungsverfahrens zwischen Access Point und Client.

6.1 TKIP

TKIP steht für **T**emporal **K**ey **I**ntegrity **P**rotocol. Wie der Name nahelegt, handelt es sich dabei um eine Zwischenlösung, die nur übergangsweise bis zur Einführung eines wirklich starken Verschlüsselungsverfahrens genutzt werden soll, aber trotzdem mit dem Problemen von WEP aufräumt. Eine Design-Anforderung war demzufolge, dass das neue Verschlüsselungsverfahren auch auf existierender WEP/RC4-Hardware mit vertretbarem Aufwand implementierbar sein sollte. Als TKIP

definiert wurde, war bereits abzusehen, dass es bis weit in die Ära der 54/108MBit-WLANs genutzt werden würde, und eine reine Software-Verschlüsselung wäre auf den meisten Systemen mit zu hohen Geschwindigkeitseinbußen verbunden gewesen. Im 'Blockschaltbild' von TKIP (Abbildung 3) finden sich deshalb viele von WEP bekannte Komponenten wieder, die in WLAN-Kartenüblicherweise in Hardware existieren und damit effektiv für TKIP genutzt werden können.

Als Komponenten, die auch schon von WEP her bekannt sind, erkennt man die RC4-Engine zur eigentlichen Ver- und Entschlüsselung sowie die CRC-Bildung davor. Als neue Komponente (grün) wird den unverschlüsselten Paket neben der CRC allerdings noch der sogenannte Michael-MIC angehängt. Bei diesem handelt es sich um einen extra für WLAN entwickelten Hash-Algorithmus, der so konzipiert wurde, dass er auch auf älterer WLAN-Hardware mit vertretbarem Overhead berechnet werden kann. Da im Gegensatz zur CRC in diesen Hash ein weiterer Schlüssel (der Michael-Schlüssel) eingeht, lässt er sich ohne die Kenntnis des Schlüssels weder berechnen, noch lässt sich ein Datenpaket verfälschen, ohne dass der Empfänger dies erkennt. Dies gilt natürlich nur unter Voraussetzung, dass ein Angreifer den Michael-Hash nicht mit Brute-Force-Methoden bricht. Wegen der Forderung der hohen Laufzeiteffizienz geht Michael hier gewisse Kompromisse ein: obwohl ein 64 Bit langer Schlüssel verwendet wird, beträgt die effektive Stärke von Michael nur etwa 40 Bit. Dies wurde allerdings als hinreichend angesehen, da ein potentieller Angreifer erst einmal die TKIP-Komponente brechen müsste, um Datenpakete zu erzeugen, welche die CRC-Prüfung der WEP/RC4-Komponente überstehen.

TKIP (rot) kümmert sich um die Berechnung der eigentlichen Schlüssel für die RC4-Engine. Im Gegensatz zu WEP wird der

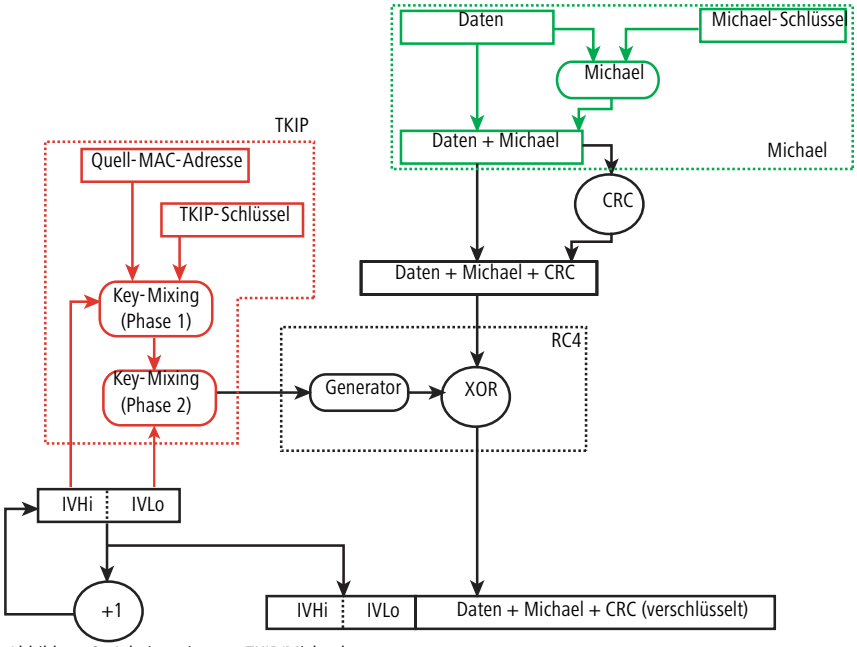

Abbildung 3: Arbeitsweise von TKIP/Michael

eigentliche Schlüssel und der im Paket enthaltene IV hier niemals direkt als RC4-Schlüssel genutzt, sondern er durchläuft zusammen mit dem IV zwei sogenannte Key-Mixing-Phasen – ein Angreifer kann also vom im Klartext enthaltenen IV keine direkten Rückschlüsse auf den RC4-Schlüssel machen, was das Problem der 'schwachen' IVs von WEP löst (das Key-Mixing selber ist so ausgelegt, dass niemals schwache RC4-Schlüssel entstehen können).

Desweiteren ist der intern hochgezählte und im Paket im Klartext übertragene IV statt 24 jetzt 48 Bit lang - damit kann ein Sender jetzt etwa 280 Billionen Pakete übertragen, bevor der 128 Bit lange TKIP-Schlüssel zwingend gewechselt werden müsste. Selbst in einem modernen WLAN mit brutto 108 MBit/s, was netto ca. 50 MBit/s erreicht, würde das bei ansonsten gleichen Voraussetzungen wie oben bei WEP ca. 2000 Jahren entsprechen.

Es bleibt noch zu erwähnen, dass der IV aus Optimierungsgründen in zwei Teile geteilt ist: einen 16 Bit langen Lo-Teil und einen 32 Bit langen Hi-Teil. Der Hintergrund dafür ist, dass das Key-Mixing wie im Bild gezeigt in zwei Phasen abläuft:

- Für die erste (rechenintensive) Phase wird nur der obere Teil benötigt, sie braucht daher nur alle 65536 Pakete durchlaufen werden.
- Die zweite, relativ einfache Phase des Key-Mixing benutzt die Ausgabe der ersten Phase sowie den Lo-Teil des IV (der sich mit jedem Paket ändert), um den eigentlichen RC4-Schlüssel zu erstellen.

Im Gegensatz zu WEP ist bei TKIP darüber hinaus festgelegt, dass die von Paket zu Paket zu verwendenden IVs streng monoton ansteigen müssen, der Empfänger muss die Phase 1 also auch nur für alle 65536 empfangenen Pakete durchlaufen. Der Entschlüsselungsteil von TKIP ist gehalten, diese Sequentialität zuüberprüfen und Pakete zu verwerfen, die einen bereits benutzen IV enthalten, was Replay-Attacken verhindert.

Als weiteres Detail mischt TKIP in der ersten Phase auch noch die MAC-Adresse des Senders ein. Auf diese Weise ist sichergestellt, dass eine Verwendung gleicher IVs von verschiedenen Sendern nicht zu identischen RC4-Schlüsseln und damit wieder zu Angriffsmöglichkeiten führt.

Wie oben erwähnt, stellt der Michael-Hash keine besonders hohe kryptographische Hürde dar: kann der Angreifer den TKIP-Schlüssel brechen oder verschlüsselte Pakete durch Modifikationen ähnlich wie bei WEP an der CRC-Prüfung vorbeischleusen, bleiben nicht mehr allzuviele Hürden zu überwinden. WPA definiert aus diesem Grund Gegenmaßnahmen, wenn eine WLAN-Karte mehr als zwei Michael-Fehler pro Minute erkennt: sowohl Client als auch Access Point brechen dann für eine Minute den Datentransfer ab und handeln danach TKIP- und Michael-Schlüssel neu aus.

6.2 Der Key-Handshake

Bereits bei der Besprechung von 802.1x wurde dargestellt, dass EAP/802.1x die Möglichkeit bietet, dem Client beim Beginn einer Sitzung die dafür gültigen Schlüssel mitzuteilen. WPA stellt dies jetzt auf eine standardisierte Grundlage, und berücksichtigt dabei auch die von modernen Access Points gegebene Möglichkeit, neben den vier 'globalen' Schlüsseln auch noch für jeden eingebuchten Client einen Session-Key auszuhandeln, der exklusiv für Datenpakete von oder zu diesem Client benutzt wird.

Betrachtet man noch einmal den in Abbildung 2 gegebenen Ablauf, so ersetzt der neu definierte Key-Handshake die Phase, in welcher der Access Point nach Erhalt des Master-Secret vom RADIUS-Server die WEP-Schlüssel an den Client übermittelt. Der Key-Handshake gliedert sich in zwei Phasen: zuerst den Pairwise Key Handshake, dann den Group Key Handshake (Abbildung 4).

Wie man sehen kann, besteht der Handshake jeweils aus Paaren von Paketen, die jeweils aus einer 'Anfrage' des Access Points und einer 'Bestätigung' des Clients bestehen. Das erste Pärchen dient im wesentlichen dazu, dass Client und Access Point für diese Verhandlung spezifische Zufallswerten (sogenannte Nonces) austauschen. Das auf beiden Seiten bereits bekannte Master Secret wird dann mit diesen Nonces gemischt und nach einem festgelegten Hash-Verfahren werden auf diese Weise weitere Schlüssel generiert, die zum einen dem Schutz des weiteren Austausches dienen und zum anderen als der Pairwise-Key für diese Station genutzt werden. Da das Master Secret nicht direkt verwendet wird, lässt es sich später für eventuell notwendige Neuverhandlungen wiederverwenden, indem es dann mit neuen Zufallswerten gemischt wird und so andere Schlüssel ergibt.

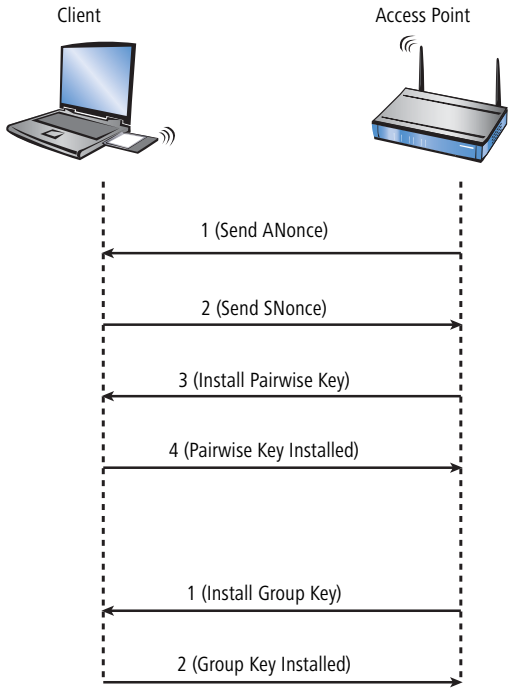

Abbildung 4: Key-Handshake bei WPA

Im zweiten Pärchen instruiert der Access Point den Client, den berechneten TKIP-Sitzungsschlüssel zu installieren, und sobald der Client dies bestätigt, tut dies auch der Access Point. Damit ist der Pairwise-Handshake abgeschlossen, und als Ergebnis besteht jetzt eine Möglichkeit, zwischen Client und Access Point Daten per TKIP auszutauschen.

Damit kann der Client aber noch nicht ganz 'freigeschaltet' werden, weil der Access Point noch einen weiteren Schlüsselübermitteln muss – den Group Key, den er benutzt, um Broadcast- und Multicast-Pakete gleichzeitig an alle Stationen zuübermitteln. Diesen muss der Access Point einseitig festlegen, und er übermittelt ihn einfach an die Station, die seinen Empfang bestätigt. Da zu diesem Zeitpunkt bereits ein Pairwise-Key auf beiden Seiten installiert ist, sind diese beiden Pakete bereits verschlüsselt.

Nach erfolgreichem Group-Key-Handshake kann der Access Point den Client endlich für den normalen Datentransfer freischalten. Es steht dem Access Point dabei frei, auch weiterhin während der Sitzung über solche Pakete ein Rekeying durchzuführen. Prinzipiell könnte sogar der Client das Rekeying vom Access Point anfordern.

WPA berücksichtigt auch den Fall älterer WLAN-Hardware, in dem der Access Point keine Pairwise-Keys unterstützt, sondern nur Group-Keys. Die erste Phase des Handshakes läuft in diesem Fall genauso ab wie vorher, nur führt dies nicht zu der Installation eines Pairwise-Keys – der Group-Key-Handshake läuft weiterhin im Klartext ab, eine Verschlüsselung in den EAP-Paketen selber verhindert aber, dass ein Angreifer die Schlüssel einfach mitlesen kann.

6.3 WPA mit Passphrase

Der im vorigen Abschnitt beschriebene Handshake läuft bei WPA grundsätzlich ab, d.h. der Anwender wird niemals selber irgendwelche TKIP- oder Michael-Schlüssel definieren müssen. In Umgebungen, in denen kein RADIUS-Server zur Erteilung des Master-Secrets vorhanden ist (z.B. bei kleinere Firmen oder Heimanwendern) sieht WPA deshalb neben der Authentifizierung über einen RADIUS-Server noch das PSK-Verfahren vor; dabei muss der Anwender sowohl auf dem Access Point als auch auf allen Stationen eine zwischen 8 und 32 Zeichen lange Passphrase eingeben, aus der zusammen mit der verwendeten SSID das Master-Secret über ein Hash-Verfahren berechnet wird. Das Master Secret ist in so einem PSK-Netz also konstant, die Nonces sorgen aber dafür, dass sich trotzdem immer unterschiedliche TKIP-Schlüssel ergeben.

In einem PSK-Netz hängen – ähnlich wie bei klassischem WEP – sowohl Zugangsschutz als auch Vertraulichkeit davon ab, dass die Passphrase nicht in unbefugte Hände gerät. Solange dies aber gegeben ist, bietet WPA-PSK eine massiv höhere Sicherheit gegen Einbrüche und Abhören als jede WEP-Variante. Für größere Installationen, in denen eine solche Passphrase einem zu großen Nutzerkreis bekannt gemacht werden müsste, als dass sie geheimzuhalten wäre, wird EAP/802.1x in Zusammenhang mit dem hier beschriebenen Key-Handshake genutzt.

LANCOM Systems hat mit dem **LEPS**-Feature (LANCOM Enhanced Passphrase Security) diese potentielle Sicherheitslücke geschlossen. Ohne komplizierte und aufwendige Server-Infrastruktur wird dabei jedem Client anhand seiner MAC-Adresse über den Eintrag in der ACL (Access Control Liste) eine individuelle Passphrase zugewiesen. Firmenweite Passphrases und die damit verbundenen Risiken sind damit nicht mehr notwendig.

6.4 Verhandlung des Verschlüsselungsverfahrens

Die ursprüngliche WEP-Definition sah lediglich eine feste Schlüssellänge vor, so dass in den Anmeldepakete von Station und Access Point lediglich ein einziges Bit erforderlich war, um anzuzeigen, ob Verschlüsselung benutzt werden soll oder nicht. Dies war bereits in dem Moment nicht mehr hinreichend, als WEP mit anderen Längen als 40 Bit eingesetzt wurde – der Anwender musste einfach aufpassen, dass neben dem gleichen Wert auch die gleiche Länge definiert ist. WPA stellt einen Mechanismus bereit, mit dem sich Client und Access Point über das zu verwendende Verschlüsselungs- und Authentifizierungsverfahren verständigen können. Zu diesem Zweck wurde ein neues Info-Element definiert, das folgendes enthalten kann:

- Das in diesem Netz zu verwendende Verschlüsselungsverfahren für Broadcasts (also die Art des Group Keys). Jeder Client, der sich in ein WPA-WLAN einbuchen will, muss dieses Verfahren unterstützen. Hier ist neben TKIP auch noch WEP zugelassen, um gemischte WEP/WPA-Netze zu unterstützen – in einem reinen WPA-Netz wird man aber TKIP wählen.
- Eine Liste von Verschlüsselungsverfahren, die der Access Point für den Pairwise Key anbietet – hier ist WEP explizit nicht mehr erlaubt.
- Eine Liste von Authentifizierungsverfahren, über die sich ein Client gegenüber dem WLAN als zugangsberechtigt zeigen kann – mögliche Verfahren sind im Moment EAP/802.1x oder PSK.

Der Access Point strahlt ein solches Element mit seinen Beacons aus, so dass sich Clients informieren können, ob dieses Netz für sie geeignet ist. Bei der Anmeldung am Access Point schickt der Client wiederum ein solches Paket, in dem er den von ihm gewünschten Typ des Pairwise Keys sowie das Authentifizierungsschema angibt. Der Access Point startet daraufhin entweder die EAP/802.1x-Verhandlung oder beginnt direkt mit dem Key-Handshake.

Da sowohl Beacons als auch Anmeldepakete noch nicht kryptographisch geschützt sind, ist es denkbar, dass Dritte in diesen Austausch eingreifen und Client und/oder Access Point auf ein schwächeres als das eigentlich gewünschte Verfahren herunterdrücken. Sowohl Access Point als auch Client sind deshalb gehalten, diese Info-Elemente während des Key-Handshakes nochmals auszutauschen, und wenn das dann empfangene sich nicht mit dem aus der Anmeldung deckt, brechen sie die Verbindung sofort ab.

Wie erwähnt, sieht der ursprüngliche WPA-Standard einzig TKIP/Michael als verbessertes Verschlüsselungsverfahren vor. Mit der Weiterentwicklung des 802.11i-Standards wurde das weiter unten beschriebene AES/CCM-Verfahren hinzugenommen. So ist es heutzutage in einem WPA-Netz möglich, dass einige Clients über TKIP mit dem Access Point kommunizieren, andere Clients jedochüber AES.

7 AES und 802.11i

Mitte 2004 wurde der lang erwartete Standard 802.11i vom IEEE verabschiedet, der das ganze Sicherheitskonzept von WLAN auf eine neue Basis stellen soll – und dies wohl auch tun wird, denn nach den Problemen bei der Einführung von WEP ist es nicht zu erwarten, dass sich bei 802.11i ähnlich grobe Fehler finden lassen werden. Wie im vorigen Abschnitt erwähnt, hat WPA bereits eine ganze Reihe von Konzepten in 802.11i vorweggenommen – deshalb sollen in diesem Abschnitt nur die Komponenten beschrieben werden, die gegenüber WPA neu sind.

7.1 AES

Die augenfälligste Erweiterung betrifft die Einführung eines neuen Verschlüsselungsverfahrens, nämlich AES-CCM. Wie der Name schon andeutet, basiert dieses Verschlüsselungsverfahren auf dem DES-Nachfolger AES, im Gegensatz zu WEP und TKIP, die beide auf RC4 basieren. Da nur die neueste Generation von WLAN-Chips AES-Hardware enthält, definiert 802.11i auch weiterhin TKIP, allerdings mit umgekehrtem Vorzeichen: eine 802.11i-standardkonforme Hardware muss AES unterstützen, während TKIP optional ist – bei WPA war es genau umgekehrt. Aufgrund der hohen Verbreitung nicht-AES-fähiger Hardware ist aber zu erwarten, dass jede AES-fähige WLAN-Karte auch weiterhin WEP und TKIP unterstützen wird. WLAN-Geräte werden allerdings voraussichtlich Einstellmöglichkeiten bieten, die den Einsatz von TKIP unterbinden – diverse Behörden in USA betrachten TKIP nicht als sicher genug, was angesichts des vergleichsweise schwachen Michael-Hashes auch durchaus gerechtfertigt ist.

Der Zusatz CCM bezieht sich auf die Art, wie AES auf WLAN-Pakete angewendet wird.

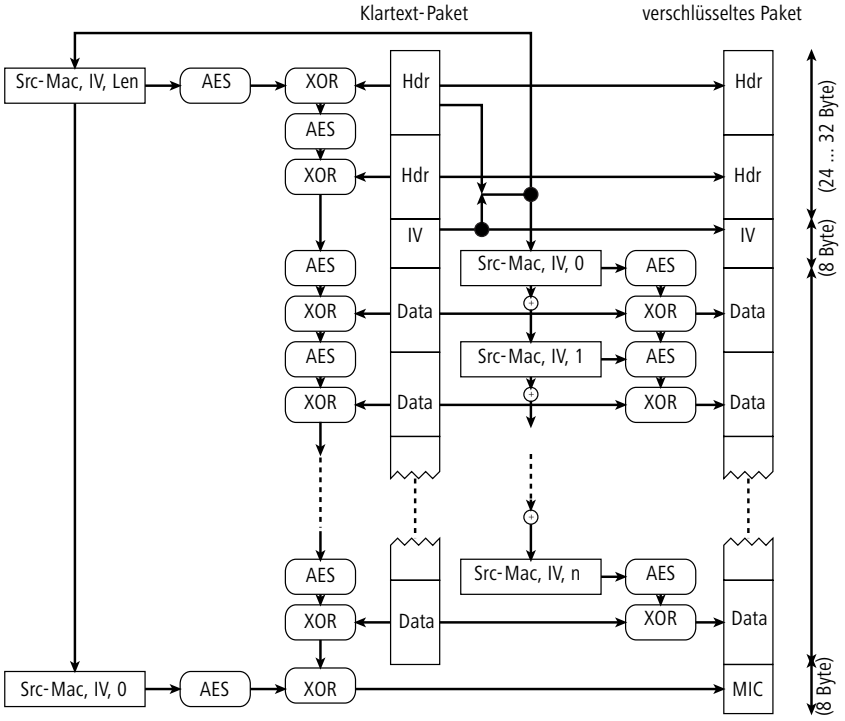

Abbildung 5: Schema von CCM

AES selber ist im Gegensatz zu RC4 und ein Block-Cipher, d.h. es wird immer gleich ein ganzer Block von Daten (im Falle von AES-CCM 16 Byte) am Stück verschlüsselt. AES selber wird dabei sowohl für die Erzeugung des MIC als auch für die Verschlüsselung im Chained Mode angewendet, d.h. für jeden AES-Datenblock werden entweder veränderte Eingangsdaten oder die Ergebnisse des letzten Schrittes verwendet, so dass gleiche Klartextdaten von Schritt zu Schritt einen unterschiedlichen Schlüsseltext ergeben. Bei DES ist diese Vorgehensweise z.B. als Chained Block Coding geläufig.

Das schematische Bild von CCM (Abbildung 5) deutet bereits seine Komplexität an (die XOR- und AES-Einheiten sind in Wirklichkeit natürlich nur einmal vorhanden!), weshalb CCM nur in Hardware effizient implementiert werden kann. Softwarebasierte Implementationen sind zwar möglich, erreichen auf den üblicherweise in Access Points eingesetzten Prozessoren nicht den Durchsatz moderner WLANs.

Im Gegensatz zu TKIP benötigt AES nur noch einen 128 Bit langen Schlüssel, mit dem sowohl die Verschlüsselung als auch der Schutz gegen unerkanntes Verändern von Paketen erreicht wird. Des weiteren ist CCM voll symmetrisch, d.h. es wird der gleiche Schlüssel in beide Kommunikationsrichtungen angewendet – eine konforme TKIP-Implementierung hingegen verlangt die Verwendung unterschiedlicher Michael-Schlüssel in Sende- und Empfangsrichtung, so dass CCM in seiner Anwendung deutlich unkomplizierter ist als TKIP.

Gelegentlich findet man in älteren Publikationen oder Drafts des 802.11i-Standards noch eine andere AES-Variante, nämlich AES-OCB oder WRAP. Bei dieser Variante wurde AES in einer anderen Form benutzt,

die aber im endgültigen Standard zu Gunsten von CCM fallen gelassen wurde. WRAP hat heute keine Bedeutung mehr.

Ähnlich wie TKIP verwendet CCM einen 48 Bit langen Initial Vector in jedem Paket – eine IV-Wiederholung ist damit in der Praxis ausgeschlossen. Wie bei TKIP merkt der Empfänger sich den zuletzt benutzten IV und verwirft Pakete mit einem IV, der gleich oder niedriger als der Vergleichswert ist.

7.2 Prä-Authentifizierung und PMK-Caching

Wie schon früher erwähnt, sind es oft die Details, welche die Verabschiedung eines Standards verzögern. Im Falle von 802.11i waren es dabei zwei Details, die insbesondere beim Einsatz von WLAN für Sprachverbindungen (VoIP) in Unternehmensnetzen helfen sollen. Vor allem in Zusammenhang mit WLAN-basierten schnurlosen Telefonen kommt einem schnellen Roaming, d.h. dem Wechsel zwischen Access Points ohne längere Unterbrechungen, eine besondere Bedeutung zu. Bei Telefongesprächen sind bereits Unterbrechungen von wenigen 100 Millisekunden störend, jedoch ist abzusehen, dass eine vollständige Authentifizierung über 802.1x, inklusive der folgenden Schlüsselverhandlung mit dem Access Point, deutlich länger dauern kann.

Als erste Maßnahme wurde deshalb das sogenannte PMK-Caching eingeführt. Der 802.11i-Standard bezeichnet mit dem PMK (Pairwise Master Key) das nach einer 802.1x-Authentifizierung in Client und Access Point vorhandene Master Secret, das die Basis für den Schlüsselaustausch darstellt. In VoIP-Umgebungen ist es denkbar, dass ein Anwender sich zwischen einer relativ kleinen Zahl von Access Points hin- und herbewegt. Dabei wird es vorkommen, dass ein Client wieder zu einem Access Point wechselt, an dem er bereits früher einmal angemeldet war. In so einem Fall wäre es unsinnig, die ganze 802.1x-Authentifizierung noch einmal zu wiederholen. Aus diesem Grund kann der Access Point das PMK mit einer Kennung, der sogenannten PMKID, versehen, die er an den Client übermittelt. Bei einer Wiederanmeldung fragt der Client mittels der PMKID, ob dieses PMK noch gültig ist. Falls ja, kann die 802.1x-Phase übersprungen werden und es ist nur der Austausch von sechs kurzen Paketen erforderlich, bis die Verbindung wieder steht. Diese Optimierung ist bei PSK-basierten WLANs nicht erforderlich, denn dort ist das PMK ja ohnehin überall gleich und bekannt.

Eine weitere Maßnahme erlaubt auch für den Fall der erstmaligen Anmeldung eine Beschleunigung, sie erfordert aber etwas Vorausschau vom Client: dieser muss bereits im Betrieb eine schlechter werdende Verbindung zum Access Point erkennen und einen neuen Access Point selektieren, während er noch Verbindung zum alten Access Point hat. In diesem Fall hat er die Möglichkeit, die 802.1x-Verhandlung über den alten Access Point mit dem neuen Access Point zu führen, was wiederum die 'Totzeit' um die Zeit der 802.1x-Verhandlung verkürzt.

8 Fazit

Nach dem Bekanntwerden der Sicherheitslücken in der WEP-Verschlüsselung, den kurzfristigen Lösungsversuchen wie WEPplus und Zwischenschritten wie WPA hat das IEEE-Komitee den neuen WLAN-Sicherheitsstandard 802.11i vorgelegt. Das bei WPA verwendete TKIP-Verfahren basiert auf dem schon älteren RC4-Algorithmus, auf dem schon WEP aufbaute. Erst mit AES wird der wichtige und endgültige Schritt zu einem wirklich sicheren Verschlüsselungsverfahren vollzogen. Die bekannten praktischen und theoretischen Sicherheitslücken der Vorgängerverfahren gehören mit 802.11i/AES der Vergangenheit an.

Das AES-Verfahren bietet genügend Sicherheit, um die notwendigen Spezifikationen des Federal Information Standards (FIPS) 140-2 einzuhalten, die von vielen staatlichen Stellen gefordert werden.

LANCOM Systems verwendet in seinen 54MBit/s-Produkten den Atheros Chipsatz mit einem Hardware-AES-Beschleuniger. Dadurch ist die höchstmögliche Verschlüsselung ohne Perfomanceverluste gewährleistet.

Mit dem benutzerfreundlichen Pre-Shared-Key-Verfahren (Eingabe einer Passphrase von 8-63 Zeichen Länge) ist 802.11i für jedermann schnell und einfach einzurichten. In professionellen Infrastrukturen mit einer großen Anzahl von Nutzern kann mit 802.1x und RADIUS-Servern gearbeitet werden.

Im Zusammenspiel mit weiteren Einstellungsmöglichkeiten wie Multi-SSID und VLAN-Tagging ist es möglich, rundum sichere und gleichzeitig für mehrere Benutzergruppen angepasste Netze mit verschiedenen Sicherheitsstufen anzubieten.

- VLAN-Tagging ist ab LCOS Version 3.32 verfügbar.
- Multi-SSID ist ab LCOS 3.42 verfügbar.
- LANCOM Systems bietet ab der LCOS Version 3.50 das PSK-Verfahren an.
- 802.1x wird ab der LCOS-Version 3.52 unterstützt.
- Einfache Authentifizierung durch individuelle Passphrases pro MAC-Adresse (LEPS) ab LCOS-Version 4.0.