WPA-TKIP Uberblick und Angriffe

1 author:

Richard Zahoransky
University of Freiburg
8 PUBLICATIONS **25** CITATIONS

WPA-TKIP: Überblick und Angriffe

Richard Zahoransky

Lehrstuhl für Kommunikationssysteme

Zusammenfassung Drahtlosnetzwerke (WLANs) sind weit verbreitet. Diese Arbeit befasst sich mit der Verschlüsselung dieser Netzwerke. Die bestehenden, standardisierten Verschlüsselungsalgorithmen und deren Sicherheitsziele werden erklärt. Der nicht mehr sichere Standard WEP dient als Beispiel zur Erläuterung grundlegender Angriffe auf Drahtlosnetzwerke. WPA (Wi-Fi Protected Access) ersetzt das ältere WEP und soll bestehenden Probleme lösen. Die hierfür neu eingeführten Funktionen und Algorithmen werden erklärt. Einige Angriffspunkte bleiben bestehen. Der Text beschreibt, wie diese ausnutzbar sind und erläutert Gegenmaßnahmen, WPA verschlüsselte Drahtlosnetzwerke weiter abzusichern.

1 Einleitung

Laptops, PDAs oder Handys haben häufig WLAN-Hardware eingebaut. Die hohe Verbreitung und Verfügbarkeit dieser Technik ist seit einiger Zeit gegeben. Gleichzeitig wird die Frage nach der Sicherheit dieser Daten immer wichtiger. Die gesendeten und empfangenen Daten könnte man sonst aus der "Luft" mit einer Antenne abfangen. Die Frequenzen sind nicht geschützt, da WLAN das lizensfreie ISM-Band im 2,4 GHz und 5 GHz nutzt [1]. Ohne Authentifizierung und Authorisierung wäre ein Angreifer also in der Lage, sich mit einem fremden WLAN zu verbinden. Ohne eine Spur zu hinterlassen, könnte der Angreifer unter einer fremden IP-Adresse im Internet agieren, hätte dieses Netz eine Internetverbindung. Wired Equivalent Privacy (WEP) [2], als Standard im Jahr 1997 eingeführt, zeigt große Sicherheitslücken. Mit der Zeit wurden Angriffe bekannt, die bei aktivem Datenverkehr einen WEP-Schlüssel in wenigen Minuten entziffern konnten. Das IEEE Konsortium reagierte mit einem neuen Standard: WPA. Aufsetzend auf WEP werden Sicherheitlücken geschlossen und versucht, zukünftige Angriffe zu erschweren. Diese Arbeit umfasst die Erläuterung von WPA und dessen Unterschiede gegenüber WEP. Zu Beginn wird das WEP Protokoll und darauf aufbauend, die Veränderungen durch WPA erklärt. Das nächste Kapitel konzentriert sich auf bereits bekannte Schwachstellen, die Aufgrund von Kompatibilitätsgründen noch bestehen und erläutert, wie sich diese Schwachstellen ausnutzen lassen.

1.1 Notation

In dieser Arbeit werden folgende Notationen verwendet:

- $\oplus$ steht für die Addition Modulo 2, also die XOR Operation
- $||$ stellt die Konkatenation dar
- $>> 1$ ist ein Bitshift nach rechts um ein Bit
- $A \rightarrow B$ bedeutet, A sendet eine Nachricht nach B.
- $F(x, y)$ bedeutet, die Funktion oder der Algorithmus F wird mit den Parametern x und y aufgerufen.

2 Verschlüsseln der Drahtlosdaten

Modifizierte Systemtreiber [1], die für viele WLAN-Karten zur Verfügung stehen sind in der Lage, Pakete von umliegenden WLAN-Stationen aufzuzeichnen, ohne mit diesen verbunden zu sein. Ohne Verschlüsselung würden diese Daten lesbar bleiben. Die Daten der WLAN-Nutzer können aber durch verschiedene Techniken vor unbefugtem Zugriff geschützt werden.

Ist solch eine verschlüsselte Verbindung aufgebaut, werden mitgeschnittene Pakete für einen Angreifer nutzlos.

[1] Siehe `http://www.aircrack-ng.org`, Menüpunkt "compatibility"

2.1 Fehlerhafte Implementierung: WEP

Der WLAN Standard 802.11 beschreibt die Verschlüsselungstechnik WEP. Bereits im Standard existieren ausnutzbare Schwächen. Die Schlüssellängen wurden zu gering gewählt. Mitschnitte von Paketen erlauben Rückschlüsse auf den geheimen Schlüssel. Herzstück von WEP ist der RC4 Algorithmus [3] zur Verschlüsselung. Als Parameter dienen dem RC4 ein geheimer Schlüssel und ein Initialisierungsvektor IV. WEP bietet keine Funktion, Replayattacken zu erkennen. Das heißt, abgefangene Pakete lassen sich wiederholt senden, ohne dass der Empfänger diese abweisen oder erkennen kann. Je nach wiederholtem Pakettyp sendet dass Netzwerk neue, verschlüsselte Antworten. So kann ein Angreifer viel Datenverkehr erzeugen. Nutzen zwei empfangene Datenpakete den selben IV, lässt sich die Linearität von RC4 ausnutzen [4] um an den Klartext zu gelangen. WEP schützt vor Übertragungsfehler durch CRC. Eine CRC Prüfung arbeitet allerdings nicht kryptografisch sicher. Verschlüsselte Nachrichten können unerkannt verfälscht werden. Ein Jahr nach Festlegung von WEP existierten bereits Angriffe, die diese und weitere Schwachstellen nutzen, um WEP-Schlüssel zu erspähen. Bestehende Angriffsmethoden umfassen zusammengefasst [4]:

- Keystream re-use: Wiederholt auftauchende IVs
- Replay Attacken: Erneutes Senden von mitgeschnittenen Paketen
- Message falsifying: Abändern von Paketen, ohne die Prüfsumme zu verletzen
- Chop-Chop: Erraten des Passwortes durch Manipulationen und erneutes Senden von abgefangen Paketen
- Prüfen des geklauten Schlüssels anhand abgefangener Pakete

2.2 WPA-TKIP

WEP wurde durch WPA [3] ersetzt. Die bis dahin verkauften WLAN-Geräte sollten aber nicht teuer ersetzt, sondern durch Softwareupdates aktualisiert werden. Das IEEE Konsortium definierte zwei Standards, wovon nur die erste Version kompatibel mit WEP-Hardware ist: WPA-TKIP. Diese Version spezifiziert keine neuen Algorithmen, sondern implementiert zusätzliche Funktionen um den RC4 Code. Größere Änderungen wären zu komplex für die bestehende Hardware.
WPA-TKIP besteht wie WEP aus zwei Teilen: Einem 64-Bit Schlüssel K^* für einen neu eingeführten Integritätscheck (MIC) und einem 128-Bit Schlüssel K für die Datenverschlüsselung. Beide Teile werden aus dem geheimen Schlüssel k generiert. Dieser Vorgang wird in regelmäßigen Abständen wiederholt und nennt sich Re-Keying. Daher heißt K auch temporärer Schlüssel.

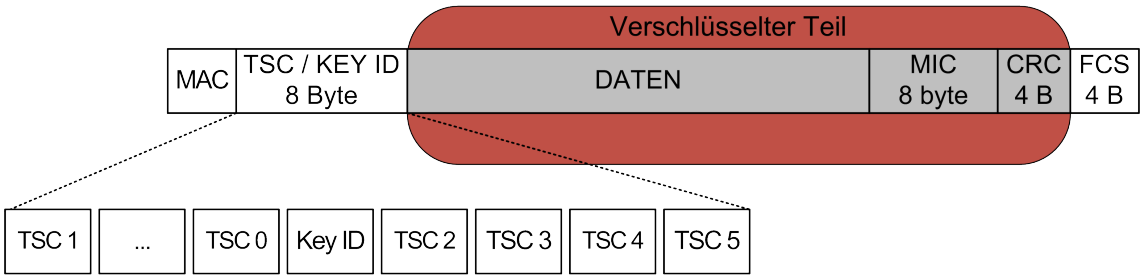

Abbildung 1. Ein von WPA verschlüsseltes Paket. Der Initialisationsvektor umfasst einen Sequenzzähler, die MAC-Adresse und einen geheimen Schlüssel K. Der verschlüsselte Teil ist rot markiert, nach [3]

Michael : Eine CRC-Prüfsumme schützt auch in WPA die Übertragung. Ein Integritätscheck (MIC-check) namens Michael schützt in WPA-TKIP die kryptografisch unsichere CRC-Summe. Michael arbeitet nicht linear. Nur Stationen, die K^* kennen, sind in der Lage korrekte MIC Codes zu erzeugen. So sollen Fälschungen durch einen Angreifer unmöglich sein. Der Integritätscheck wird generiert aus den unverschlüsselten Anwendungsdaten A und dem Integritätsschlüssel K^*.

$$\mathrm{M} = \mathrm{A}||michael(K^*, \mathrm{A}), \tag{1}$$

Dabei nutzt Michael zusätzlich die Sende- und Quelladresse, um daraus einen 64-Bit Wert zu erzeugen, der an A angehängt wird. Eine CRC Summe (32 Bit) schützt die Nachricht M und den MIC gegen Übertragungsfehler.

$$\mathrm{D} = \mathrm{M}||CRC(\mathrm{M}) \tag{2}$$

Der Datenstrom D wird von RC4 verschlüsselt.

Temporal Key Hash Große Sicherheitslücken entstanden in WEP durch den zu schwachen Initialisationsvektor IV. Der IV dient als Eingabe für RC4. Er wurden in WPA von 24 Bit auf 48 Bit erweitert. Eine Hashfunktion, genannt Alternate Key Hash, oder, der Einfachheit halber WPA-Hash, erzeugt den IV. Der Hash soll gewährleisten, dass der Initialisierungsvektor keine Rückschlüsse auf den geheimen Schlüssel ermöglicht. Der Hash arbeitet in zwei Phasen mit mehreren Runden, wobei das Ergebnis einer Runde in die nächste Runde einfließt. In der erste Phase werden die MAC-Adresse, der temporärer Schlüssel K und Teile einer Sequenznummer verarbeitet. Das Ergebnis ist ein Byte Array (P1K[$0 \cdots 4$]). Die zweite Phase nimmt dieses Array und erneut die Sequenznummer als Eingabe, um den 48 Bit IV zu erzeugen (siehe Abbildung 2 und 1). Der Temporäre Schlüssel K ist in der Abbildung als Bytearray K[0] bis K[15] dargestellt. In den einzelnen Schritten sichert eine S-Box die zwischengeschalteten Schlüssel K[0...13] und macht das Verfahren irreversibel. Durch die Verwendung der MAC-Adresses werden Reuse-Attacken effektiv verhindert. Verschiedene Stationen nutzen daher nie den gleiche Initialvektor IV.

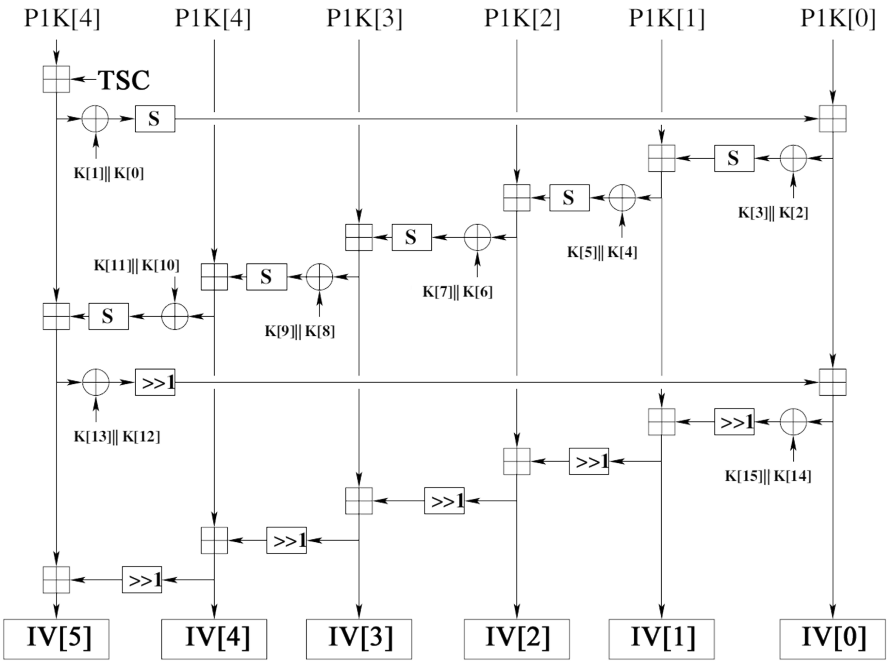

Abbildung 2. Die zweite Phase des Temporal Key Hashes. Aus der MAC-Adresse, dem Sequenzzähler und dem temporärer Schlüssel (K[0...15]) werden die IV-Werte IV[0...5] generiert, die den RC4 Algorithmus speisen [5].

TKIP Sequence Counter Eine weitere Änderung in WPA-TKIP ist die Einführung von Sequenznummern, um Replay-Attacken zu verhindern. Der TKIP sequence counter (TSC) fließt in den IV (siehe Abschnitt oben). Um erfolgreich vor Replay-Attacken zu schützen, schreibt der Standard vor, den TSC nach jeder Übertragung zu inkrementieren. Die Verschlüsselung lässt sich zusammengefasst schreiben:

$$C_i = (\text{Nachricht}_i) \oplus RC4(\text{WPA-hash}(K, \text{MAC-Adresse}, TSC_i), TSC_i) \tag{3}$$

C_i ist das verschlüsselte Paket mit der Sequenznummer i. Nach jeder Nachricht wird i, also der TSC Counter inkrementiert. Der TSC wird im Klartext vor die verschlüsselten Daten gehängt. Der Empfänger vergleicht den TSC Wert mit dem gespeichertem. Ist der empfangene TSC kleiner oder gleich dem gespeichertem Wert für i, wird das Paket verworfen, ohne eine Fehlermeldung an den Sender zu übermitteln. Nach erfolgreichem Empfang wird der TSC Zähler inkrementiert. Ein Angreifer kennt K nicht. Er kann den WPA-hash, der K zusammen mit dem TSC verarbeitet, nicht ausführen, um ein zuvor abgefangenes Paket wieder gültig zu machen.

Entschlüsselung Die verschlüsselten, gesendeten Nachrichten werden von allen Stationen in Empfangsreichweite empfangen. Nur Stationen mit gemeinsamen Schlüssel k können die Nachrichten interpretieren. Hierfür wenden sie WPA-TKIP in umgekehrter Reihenfolge an und erhalten so die Nachricht M:

$$(\mathrm{M}_i||CRC32(\mathrm{M}_i)) = C_i \oplus RC4(IV_i, TSC_i). \tag{4}$$

Es gilt $IV_i = \text{WPA-hash}(K, \text{MAC-Adresse}, TSC_i)$.
Der Empfänger überprüft die CRC-Summe. Sind keine Fehler entdeckt, werden die Daten weiter verarbeitet. Ansonsten wird das Paket, ohne eine Fehlermeldung zu generieren, verworfen. Der TSC-Wert wird ausgelesen und mit dem Gespeicherten verglichen. Ist er abgelaufen, wird das Paket still verworfen. Zusammen mit Schlüssel K ist der WPA-Hash nun durchführbar, um den IV zu generieren. Mit bekanntem IV sind die Daten jetzt entschlüsselbar. Der Integritätcheck Michael überprüft die Daten. Treten Unstimmigkeiten auf, wird eine Fehlermeldung (MIC-failure) gesendet und das Paket verworfen. Treten mehr als zwei solcher Fehler innerhalb einer Minute auf, geht das Protokoll von einem Angriff aus und erzeugt aus dem geheimen Schlüssel k einen neuen Integritätschlüssel K^*. Abbildung 3 zeigt das Schema von WPA für den Sender einer Nachricht.

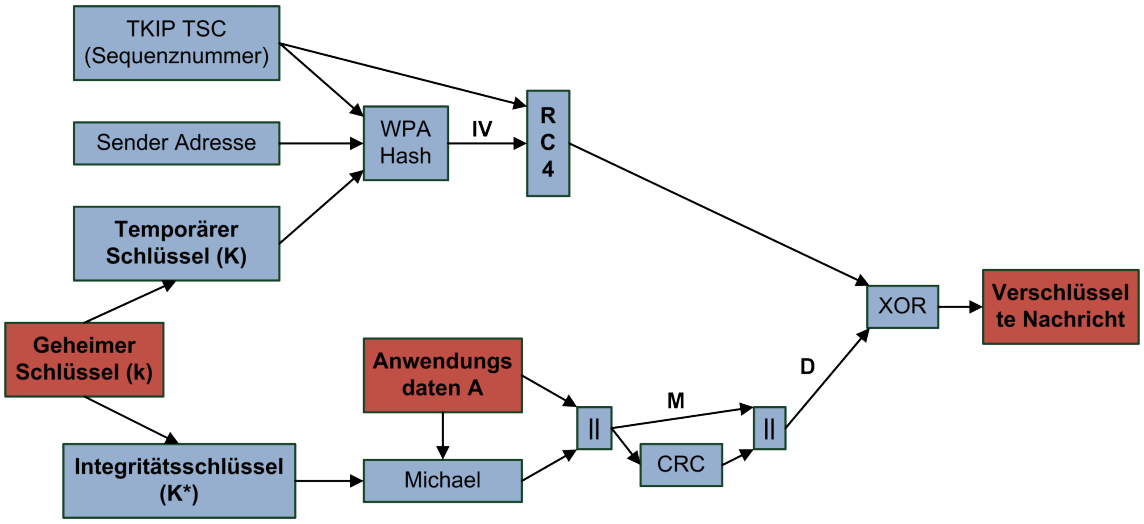

Abbildung 3. Schema der WPA-TKIP Verschlüsselung. Der TSC fließt nicht direkt in den RC4 Algorithmus, sondern wird zuvor gehasht. Der MIC-check "Michael" schützt vor Manipulationen, nach [6]

2.3 WPA2-CCMP

WPA2 beziehungsweise WPA-CCMP ist der zweite Standard des IEEE Konsortiums [3]. WPA-CCMP nutzt zur Verschlüsselung nicht den RC4 Algorithmus, sondern CCP ("Counter mode with Cipher block chaining MAC Protocol"). CCP fasst die Verschlüsselung und Authentifizierung der Daten zusammen. Diese Algorithmen sind nicht mit alter WEP-Hardware kompatibel, bieten aber einen bis heute nicht angreifbaren Standard. Aufbauend auf dem CCM Standard für generische

Verschlüsselung [7], verschlüsselt WPA-CCMP jedes gesendete Paket mit AES. Im Gegensatz zu WPA-TKIP, werden die Daten vor der Verschlüsselung in 128-Bit lange Blöcke aufgeteilt. Jeder Block erhält einen Zähler, ähnlich dem TSC [8]. Nur das verwendete Passwort bietet einen Angriffspunkt durch Wörterbuch oder Brute Force Angriffe. Die Sicherheit von WPA2 steigt mit direktem Zusammenhang zum Passwort. Lange und nicht erratbare Schlüssel sollten gewählt werden[2].

2.4 Externe Authentifizierung

Sowohl WPA-TKIP als auch WPA-CCMP unterscheiden zwei Modi der Authentifizierung. Im privaten Umfeld tauschen die Teilnehmer eines Netzwerkes meist mündlich den geheimen Schlüssel k untereinander aus. In großen Netzwerken mit einer nicht mehr überschaubaren Anzahl an Teilnehmer ist diese Lösung nicht anwendbar. WPA arbeitet mit dem 802.1X EAP Framework zusammen. Den Benutzern können also Schlüsselpaare zugewiesen werden, die von einem externen RADIUS-Server stammen. Über diesen Server können Benutzer zentral für das Netzwerk freigeschalten oder ausgesperrt werden. Scheidet ein Teilnehmer aus, wurde ein authentifiziertes Gerät entwendet oder ist ein Schlüssel nicht mehr sicher, lässt sich der entsprechende Schlüssel löschen. Andere Benutzer sind nicht gezwungen, neue Passwörter in ihre WLAN-Clienten einzutragen.

3 Angriffe auf WPA-TKIP

Trotz großer Bemühung hat WPA-TKIP einige Schwächen seines Vorgängers geerbt. Unter bestimmten Bedingungen sind Replayattacken möglich und Schwächen im WPA-Hash erlauben den temporären Schlüssel K mit einigem Aufwand zu errechnen.

3.1 Replayattacken

Gerade um Replayangriffe zu vermeiden, erzwingt WPA die strikte Inkrementierung der Sequenznummer TSC. Ohne diesen Zähler könnten mitgeschnittene Paket (P^*) zu jeder Zeit wieder an das Netzwerk gesendet werden. Die Gefahr eines solchen Angriffs besteht in der Wahl von P^*. Ist P^* beispielsweise eine ARP-Anfrage, erzeugt das Netzwerk wieder neue, verschlüsselte Pakete. Deren Inhalte sind erneut bekannt und ausnutzbar. Durch wiederholtes Ändern und Senden eines mitgeschnittenen Paketes und der Analyse der Antworten kann der Integritätschlüssel K^* sowie die ursprüngliche Nachricht im Klartext berechnet werden. Ein Angriff, der nach solch einem Prinzip arbeitet, nennt sich Chop-Chop.

QoS Schwachstelle Trotz TSC Zählern zeigten Tews und Beck in ihrer Arbeit [10] solch einen Angriff auf WPA (Chop-Chop). Modernere WLAN Geräte bieten QoS Funktionen [3]. WLANs mit diesem Standard haben acht logische Kanäle mit unterschiedlicher Priorität, um zeitkritische Daten auch bei starker Auslastung zu transportieren. Jeder dieser Kanäle besitzt einen unabhängigen TSC Counter. Die Wirksamkeit von TSC in solchen Netzwerken ist Tews und Beck zufolge nicht mehr gegeben. Zeichnet also ein Angreifer ein Paket auf einem viel benutzten QoS Kanal auf, so ist es sehr wahrscheinlich, dass zumindest einige der anderen Kanäle einen geringeren TSC-Wert haben, siehe Abbildung 4. Auf den wenig benutzten Kanälen lässt sich dann ein Chop-Chop Angriff realisieren. weil der abgefangene TSC dort noch Gültigkeit besitzt.

Chop - Chop Chop-Chop nutzt die Linearität der CRC Prüfsumme aus. Der Angriff entschlüsselt, ein empfangenes Paket P Stück für Stück, indem dies mit leichten Änderungen an den Sender zurückgesandt wird.
Angenommen, ein Angreifer möchte P mit Chop-Chop entschlüsseln. Dazu schneidet er das letzte Byte von P ab. Hierdurch verfälscht er unweigerlich die Prüfsumme. Das abgeschnittene Byte sei R und das restliche Paket P'. Die Prüfsumme von P ist, zusammen mit den Daten, verschlüsselt. Würde der Angreifer wissen, wie die abgeschnittenen Daten R im Klartext aussehen, könnte er die Prüfsumme entsprechend korrigieren, damit das Paket wieder gültig wird. Die Funktionsweise

[2] `http://www.google.com/accounts/PasswordHelp`

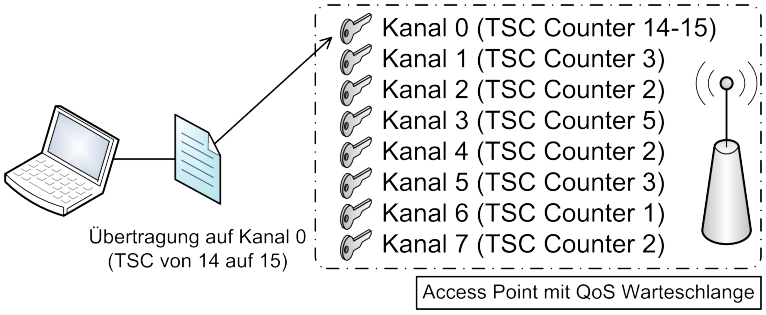

Abbildung 4. Netzwerke mit QoS Funktion. Jeder Kanal hat einen eigenständigen TSC-Zähler, nach [6]

dieser Korrekturfunktion wurde von E. Tews beschrieben [11]. Sie behält auch im verschlüsseltem Zustand ihre Gültigkeit. Die Korrektur einer Prüfsumme im unverschlüsselten Raum, korrigiert also auch die Prüfsumme im verschlüsselten Zustand. Das bedeutet, der Angreifer kann raten, was R im Klartext bedeutet um auf dieser Mutmaßung die Korrektur an P' durchführen. P' bleibt verschlüsselt. Das so erzeugte Paket sendet er wieder an das Netzwerk. Hat er den Klartext von R falsch geraten, kommt keine Antwort zurück (Abschnitt **??**), schließlich besteht P' dann nicht den CRC-check. Erneut wählt der Angreifer die nächste Permutation für das unverschlüsselte R, rechnet darauf die Korrektur und sendet das Paket mit der neu ermittelten Prüfsumme. Ist R richtig geraten, besteht das Paket beim Empfänger die CRC-Prüfung und wird weiter verarbeitet. Der darauf folgende MIC-check Michael entdeckt die Manipulation und die Station sendet einen MIC-failure report. Der Korrekturfaktor war also richtig. Damit weiß der Angreifer, dass er auch den Klartext von R richtig erraten hat. Das erste Byte von P ist ihm somit bekannt. Nun muss er mindestens eine Minute warten, sonst würde er ein Re-Keying auslösen. Danach kann er mit dem nächsten Byte fortfahren, bis das ganze Paket entschlüsselt ist.

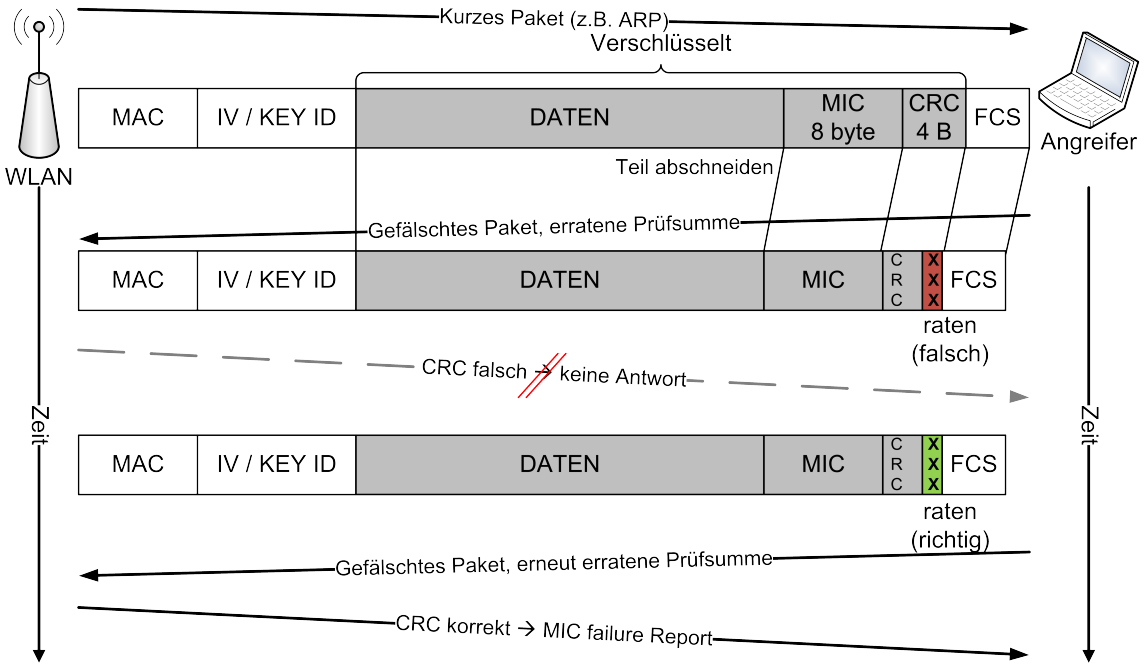

Abbildung 5. Prinzip eines Chop-Chop Angriffs auf WPA Netzwerke. Ein Teil des Paketes wird abgeschnitten. Er wird geraten, die Prüfsumme entsprechend korrigiert und das Paket erneut versandt. Ist die Prüfsumme inkorrekt, wird keine Antwort generiert. Stimmt die Prüfsumme, erzeugt der Access-Point eine MIC-failure. Die Korrektur der Prüfsumme gilt sowohl am verschlüsseltem Paket als auch im Klartext. Dadurch ist der abgeschnittene Klartext dann bekannt.

Um den Angriff durchzuführen, ist ein Mitschnitt eines kleinen, verschlüsselten Paketes sinnvoll. Als Beispiel wird das Vorgehen anhand einer ARP-Anfrage erläutert. ARP Pakete unterscheiden sich nur gering untereinander. Ein ARP-Antwort hat stets die Broadcastadresse als Ziel. Weitere bekannte Teile sind die Quelladresse und meist die ersten Bytes der IP-Adressen [3]. Somit bleiben 2 Byte, die im Vorfeld unbekannt sind. Ein WPA-TKIP Paket hat damit 14 unbekannte Bytes: Zwei Byte fallen auf das ARP Paket. Acht Bytes gehören zu dem Integritätschek Michael (MIC-check) und vier Bytes zu der CRC Checksumme. Die MIC-Bytes und die Checksumme können mit beschriebenem Chop-Chop durch wiederholtes Anwenden ermittelt werden. Der MIC-Schlüssel K^* lässt sich extrahieren, da Michael eine umkehrbare Funktion ist.
Für die unbekannten Bytes aus dem ARP-Protokoll kann eine effizientere Methode gewählt werden. Es bleiben 2^{16} Möglichkeiten. Für jede dieser Möglichkeiten kann der CRC und MIC Wert berechnet werden, da der Schlüssel K^* bereits bekannt ist. Stimmt das erzeugte mit dem abgefangenem Paket überein, ist die korrekte Permutation erraten. Somit liegt das gesamte Paket im Klartext vor. Durch XOR mit dem verschlüsseltem Paket erhält man den IV.
Ist ein Chop-Chop Angriff bereits einmal durchgeführt worden, können weitere Angriffe effektiver arbeiten. Angenommen, das empfangene Paket ist wieder eine ARP-Anfrage:

- Der MIC-Schlüssel K^* ist bereits bekannt
- Von der IP-Adresse sind die ersten sieben Bytes bekannt (in einem /24-Netz)
- Lediglich der neue CRC-Wert ist unbekannt

Obwohl das letzte Byte der IP-Adresse unbekannt ist, muss der Angreifer nur die CRC Summe entschlüsseln. Danach kann er die IP-Adresse raten, damit das entsprechende Paket erzeugen, und die CRC Prüfsumme anwenden. Stimmt diese mit der entschlüsselten CRC-Summe überein, ist da letzte unbekannte Byte gefunden.
Die Informationen aus dem Chop-Chop erlauben es auch, eigene Nachrichten einzuschleusen.

Einschleusen von Nachrichten Nach erfolgreichem Chop-Chop ist von einem Paket sowohl der Klartext, als auch die verschlüsselte Kopie bekannt. Durch XOR der beiden erhält man den IV, der für dieses Paket galt. In einem mit QoS ausgestattetem Netzwerk gibt es sieben weitere Kanäle, die einen kleineren TSC-Wert haben und somit diesen IV akzeptieren. Der MIC Schlüssel K^* ist ebenfalls bekannt. So kann der Angreifer verschlüsselte Nachrichten erzeugen und auf den anderen QoS Kanälen absetzen. Hierzu muss er die eigene MAC-Adresse an die des ursprünglichen Senders anpassen. Sind alle QoS Kanäle ausgeschöpft, muss erneut auf dem Kanal mit dem höchsten TSC-Wert auf ein kurzes, verschlüsseltes Paket gewartet und Chop-Chop ausgeführt werden. Es können nun auf den verbleibenden QoS Kanälen wieder gültige Nachrichten eingeschleust werden.

3.2 Man in the Middle Angriff

In [6] demonstrieren Ohigashi und Masakatu die Durchfürbarkeit einer Man in the Middle Attacke auf WPA-TKIP Netzwerke. Dieser Angriff erfordert keine QoS Funktionalität. Wichtig für eine erfolgreiche Chop-Chop Strategie ist, dass man Pakete abfangen kann, ohne dass dies die WLAN-Station erreichen. So erhöht sich der TSC Zähler auf der Empfangsseite nicht. Der Angreifer ist also im Besitz eines (noch) gültigen Paketes. Ein gültiger Benutzer muss im Netzwerk registriert sein, der sich an der Empfangsgrenze des Access Points befindet.
Ein Angreifer braucht einen Ort, von dem aus er beide Stationen gut empfangen kann. Nun spannt er selbst ein Netzwerk mit der gleichen Kennung (SSID) auf[4]. Daher wird die Funkkarte des Opfers das stärkere Signal bemerken und sich damit verbinden. Abb. 6 verdeutlicht das Verfahren. Ohigashi und Masakatu unterscheiden drei Modi des Angriffs:

[3] Die häufigsten, anzutreffenden WLAN Netzwerke haben IP-Adressen mit einer /24er Netzmaske
[4] Dies verstößt nicht gegen den WLAN Standard 802.11, sondern ist erlaubt, um große Gebiete mit einem einheitlichem WLAN zu versorgen. Eine mobile Station kann so ungehindert, auch über weite Strecken, den Kontakt zu dem entsprechendem Funknetzwerk aufrecht halten. Die WLAN Karte sucht sich automatisch die Station mit dem besten Empfang

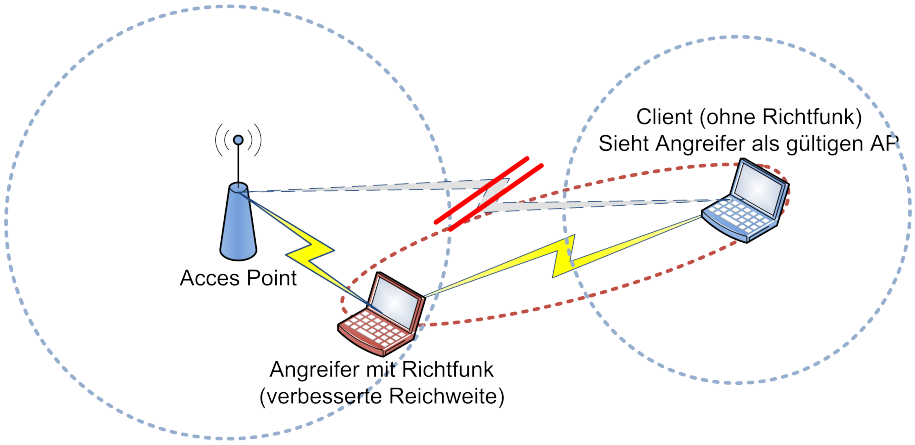

Abbildung 6. MITM Angriff bei WLAN. Der Angreifer kann den Client mit einer Richtfunkantenne erreichen. Der Client allerdings kann die Kommunikation zwischen dem Angreifer und dem AP nicht erkennen. Der Angriff bleibt somit unbemerkt.

Repeater Modus So lange interaktiv Pakete zwischen Accesspoint und Client ausgetauscht werden, oder sie nutzlos erscheinen, leitet der Angreifer die Pakete an die eigentliche WLAN-Station entgegen. Benutzt der Angreifer Richtfunkantennen, um den Angriff durchzuführen, hat das Opfer kaum Möglichkeiten, den Angriff zu erkennen.

MIC Angriff Dieser Modus zielt darauf ab, den geheimen MIC Schlüssel K^* zu erspähen. Erkennt der Angreifer ein nutzbares Paket, zum Beispiel erwähnte ARP-Anfragen, fängt er dieses ab, ohne es weiterzuleiten. Das TSC-Feld des eigentlichen Accesspoints wird nicht erhöht. So startet der Angreifer interaktiv einen Chop-Chop Angriff. Während den benötigten 12-15 Minuten kann das Opfer nicht mit seinem WLAN kommunizieren.

Verfälschen von Nachrichten Nachdem der Schlüssel K^* bekannt ist, können Nachrichten eingeschleust werden. Tews und Beck demonstrieren in ihrer Arbeit [10] die exakte Vorgehensweise. Die benötigte Zeit liegt bei vier Minuten.

Um nicht entdeckt zu werden, kann der Angreifer interaktiv zwischen den genannten Modi wechseln. In vielen Fällen wird eine Unterbrechung des Datenstrom vom Benutzer nicht bemerkt. Das Ausbleiben einer ARP-Anfrage löst beim Betriebsystem keine direkte Fehlermeldung aus. Der Angreifer kann solch ein Paket also unbemerkt abfangen und Chop-Chop ausführen. Will das Opfer eine interaktive Kommunikation beginnen (HTTP, E-Mail, etc.) wird vom MIC Angriff wieder zum Repeatermodus gewechselt. Ist ein MIC-Angriff beendet, kann der Angreifer ein eigenes Paket an das Netzwerk senden. Danach muss wieder ein gültiger IV angegriffen werden.

Beschleunigung der MITM Attacke Ist der MIC-Schlüssel K^* erspäht, beschleunigt dies einen erneuten Chop-Chop Angriff, da nur noch die CRC Summe und die IP-Adresse unbekannt sind. [10]. Ohigashi und Masakatu [6] zeigten allerdings eine weitere Verfeinerung des Angriffs. Einerseits verringern sie die Dauer des Kommunikationsblackout als auch die Angriffszeit. Statt die gesamte CRC-Prüfsumme zu entschlüsseln, schlagen sie vor, nur das letzte Byte durch Chop-Chop zu ermitteln. Dieser Vorgang ist ohne Zwangspause möglich, da nur ein MIC-failure getriggert wird. Aus der unbekannten IP-Adresse ergeben sich in einem 255.255.255.0 IP-Netzwerk 2^8 Möglichkeiten für das ARP-Paket. Der Angreifer kann alle Variationen erzeugen und mit dem einen bekannten Byte der Prüfsumme vergleichen. Angenommen, das letzte Byte ist gleichverteilt, ergibt sich bei einer Übereinstimmung eine Wahrscheinlichkeit von $(2^8 - 1)/2^8$, dass der erratene Wert am Ende doch nicht mit der gesamten Prüfsumme übereinstimmt. Mit einer Wahrscheinlichkeit von

$$\left(\frac{2^8 - 1}{2^8}\right)^{2^8 - 1} \approx 0,369$$

wird das erzeugte Paket also akzeptiert. Die Angriffszeit wird hierdurch auf 1/3 reduziert, wobei die Erfolgsrate größer 1/3 ist. Es entsteht also ein Zeitgewinn.

3.3 Schwächen im WPA-Hash

Angriffe auf WEP, die von dem benutzten IV auf den Schlüssel K schließen, soll der WPA-Hash verhindern. Statt des geheimen Schlüssels könnten diese lediglich den einmal gültigen IV aufdecken. Da der Hash so konstruiert wurde, dass er nicht umkehrbar ist, kann daraus nicht der geheime Schlüssel K abgeleitet werden.
In ihrer Arbeit [5] fanden die Autoren Moen, Raddum und Hole jedoch eine Schwäche des WPA-Hashes, die es ermöglicht, den temporären Schlüssel K sowie den MIC-Schlüssel K^* mit Laufzeit $O(2^{105})$ zu entschlüsseln. Im Vergleich zu einem Brute Force Angriff ($O(2^{128})$) stellt dies eine signifikante Beschleunigung dar. Voraussetzung ist, dass bereits einige Initialisationsvektoren IV (Abb.3) bekannt sind, die dem selben TSC-Wert entspringen. Mehr als zehn Stück sind nicht nötig. Das Vorgehen lässt sich grob beschreiben (siehe dazu Abb. 2):
Durch ein abgefangenes Paket sind bereits acht Bit von K bekannt, da IV[5] aus K[15] || K[14] berechnet wird. Da der WPA-Hash in großen Teilen reversibel ist, lassen sich auch die sieben höchsten Bits von K[0] und das LSB von K[1] zurückrechnen. Schrittweise ist es möglich, so immer größere Teile von K aufzudecken. Auch IV[3] und IV[4] werden ähnlich wie IV[5] errechnet. Das Verfahren lässt sich bis zur S-Box Operation umkehren. Danach muss ein Wert für K[10]||K[11] geraten werden. Hieraus lässt sich P1K[4] berechnen. Für jeden der Abgegriffenen IV wird dieses Verfahren mit dem gleichen Wert für K[10]||K[11] wiederholt. Stimmen die erlangten Werte für P1K[4] überein, wurde K[10]||K[11] richtig erraten.
Auf diese Weise kann sich ein Angreifer in umgekehrter Reihenfolge durch Phase 2 des temporal Key Hashes durcharbeiten. Die S-Box Operationen sind nicht umkehrbar. Die entsprechenden Teile müssen geraten werden. Die erratenen Werte kann er aber mit den Ergebnissen für die anderen IVs vergleichen. Stimmen sie überein, hat er korrekt geraten. Der Temporäre Schlüssel K lässt sich in folgender Reihenfolge auflösen:
K[10,11], K[8,9], K[6,7], K[0,1,12,13], K[2,3,14,15] und letztendlich K[4,5].
Das letzte Bit von K[12] und K[14] bleibt unbekannt. Die verbleibenden vier Möglichkeiten können aber generiert und mit P1K verglichen werden, da die erste Phase des Hashes nur die unteren Bits von TSC erwartet. Der Angriff bleibt theoretischer Natur, da sich kaum ein Szenario ergibt, bei welchem ein Angreifer an verschiedene IVs herankommt, die mit gleichem TSC-Wert generiert wurden. Auch die Zeitkomplexität ist noch zu hoch für einen praktikablen Angriff. Allein aber die Möglichkeit zeigt, dass der Verlust von Initialvektoren ähnlich gefährlich ist wie der Verlust von K.

3.4 Brute-Force

Treten zwei WLAN-Geräte erstmalig in Kontakt, um über WPA und einem geheimen Schlüssel k zu kommunizieren, führen sie zuerst einen Vier-Wege-Handshake aus. Bei diesem Prozess wird ein mehrmals durchlaufener Hash von k übermittelt [12]. Mit gefälschten Paketen kann ein Angreifer zwei bereits verbundene Geräte zu solch einem neuen Handshake zwingen. Wird dieser aufgezeichnet, kann der Angreifer Passwörter erraten oder durchprobieren und mit dem Hashwert vergleichen. Es besteht seit 2008 sogar ein Programm, das diesen Vorgang unter Verwendung von Nvidia Grafikprozessoren erheblich beschleunigt [13]. Einzig Brute-Force Angriffe sind auch auf WPA-CCMP verschlüsselte Netzwerke möglich [14].

4 Gegenmaßnahmen

Trotz den bekannten Schwachstellen bietet WPA-TKIP immer noch eine größere Sicherheit als WEP. Um mögliche Angriffe zu erschweren, lassen sich einige Einstellungen und Voraussetzungen ändern.

MIC Failure Reports unterdrücken Gegenmaßnahmen können so weit gehen, den eigentlichen Standard zu brechen. So bietet OpenBSD an, für WPA Netzwerke den MIC Failure Report zu deaktivieren [10]. Treten zwei MIC failure innerhalb einer Minute auf, werden gleich zwei MIC Failure Reports in kurzen Zeitabständen gesendet und so ein Re-Keying ausgelöst. Chop-Chop Angriffe sind auf MIC-Failure Reports angewiesen, ohne dass der MIC-Key geändert wird.

Starke Passwörter Die Sicherheit von WPA-TKIP und WPA-CCMP hängt von der Qualität des Passwortes ab. Kurze Passwörter oder Namen sind mit einem abgefangenem WPA-Hash schnell verifiziert und sollten vermieden werden. Dies gilt auch für zusammengesetzte Passwörter aus mehreren Begriffen oder Wörtern.

QoS deaktivieren Die einfachste Art, eine Replay-Attacke zu unterbinden ist es, QoS zu deaktivieren. Ohne zusätzliche Kanäle mit kleinem TSC nimmt man einem potentiellen Angreifer die Chance, gültige Pakete zu erzeugen. Man-in-the-Middle Angriffe wehrt dies aber nicht ab.

Funkreichweite Viele WLAN-Geräte können die Sendestärke variieren. Kann das WLAN außerhalb der eigenen Wohnung nicht mehr einwandfrei empfangen werden, sinken auch die Erfolgschancen eines MITM Angriffs.

Re-Keying Time WPA-Netzwerke lassen sich anweisen, in bestimmten Zeitabständen ein Re-Keying durchzuführen. In den Standardeinstellungen ist dieser Wert zu groß. Ist das Intervall klein genug, kann Chop-Chop nicht mehr korrekt arbeiten. Die Zeit, die der Angriff benötigt, ist somit größer als das Re-Keying Intervall.

5 Fazit

Unumstritten bietet eine Verschlüsselung durch WEP keine Sicherheit mehr [2], [10]. Replay und Re-use Attacken sind möglich, da keine Seuqenznummern genutzt werden und die Schlüssellänge zu gering ist. Doch auch das auf WEP aufbauende WPA-TKIP hat Schwächen geerbt. Es ist noch kein praktikabler Angriff bekannt, der die Sicherheit vollständig kompromittiert, doch die Funktionen, die in WPA-TKIP die Sicherheit erhöhen sind, wie beschrieben, teilweise angreifbar. Durch gezeigte Gegenmaßnahmen lässt sich ein WPA-TKIP verschlüsseltes Netzwerk so weit anpassen, dass die bekannten Angriffe erschwert oder unmöglich werden. WPA-CCMP bietet als ein neu entwickeltes Protokoll eine höhere Sicherhei, ohne bekannte Angriffe. WLAN-Adapter, wie sie in modernen Laptops verbaut sind, unterstützen sowohl WPA als auch WPA2. Sofern keine alten Geräte in das WLAN integriert sind, sollte WPA2 als Verschlüsselung gewählt werden, um keine Angriffsfläche zu bieten.

Literatur

1. Sikora, A., Groza, V.: Coexistence of ieee802.15.4 with other systems in the 2.4 ghz-ism-band. In: Instrumentation and Measurement Technology Conference, 2005. IMTC 2005. Proceedings of the IEEE. Volume 3. (2005) 1786 –1791
2. Borsc, M., Shinde, H.: Wireless security privacy. In: Personal Wireless Communications, 2005. ICPWC 2005. 2005 IEEE International Conference on. (2005) 424 – 428
3. 802.11, I.S.: Wireless lan medium access control (mac) and physical medium acces control (phy) specifications (1999) `http://standards.ieee.org/getieee802/download/802.11i-2004.pdf`.
4. Borisov, N., Goldberg, I., Wagner, D.: Intercepting mobile communications: the insecurity of 802.11. In: MobiCom '01: Proceedings of the 7th annual international conference on Mobile computing and networking, New York, NY, USA, ACM (2001) 180–189
5. Moen, V., Raddum, H., Hole, K.J.: Weaknesses in the temporal key hash of wpa. SIGMOBILE Mob. Comput. Commun. Rev. **8**(2) (2004) 76–83
6. Ohigashi, T., Masakatu, M.: A practical message falsification attack on wpa, Hiroshima University, Kobe University, Joint Workshop on Information Security (2009)
7. Whiting, D., Housley, R., Ferguson, N.: Counter with cbc-mac (ccm). Technical report, United States (2003)
8. Jakob, J.: On the security of ctr + cbc-mac, nist modes of operation additional ccm documentation. Technical report, NIST: National Institute of Standards and Technology, jakobjonsson@yahoo.se (2001) `http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/ccm/ccm-ad1.pdf`.
9. Tews, E., Beck, M.: Practical attacks against wep and wpa. In: WiSec '09: Proceedings of the second ACM conference on Wireless network security, New York, NY, USA, ACM (2009) 79–86
10. Tews, E.: Attacks on the wep protocol. Master's thesis, TU Darmstadt, `e_tews@cdc.informatik.tu-darmstadt.de` (2007) `http://www.cdc.informatik.tu-darmstadt.de/reports/reports/Erik_Tews.diplom.pdf`.
11. Moskowitz, R.: Weakness in passphrase choice in wpa interface, ICSA Labs (2003) `http://wifinetnews.com/archives/2003/11/weakness_in_passphrase_choice_in_wpa_interface.html`.

12. “ebfe”: Ankündigung, wpa-psk mit hilfe von gpus anzugreifen. `http://forums.nvidia.com/index.php?showtopic=76778` (2008)
13. MacMichael, J.L.: Auditing wi-fi protected access (wpa) pre-shared key mode. Linux J. **2005**(137) (2005) 2