Fachhochschule Wedel

University of Applied Sciences

Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2

Seminar IT-Sicherheit
Sommersemester 2018

Steffen Kurt
inf102857

Betreuung:
Prof. Dr. Gerd Beuster

16. August 2018

Inhaltsverzeichnis

Abkürzungsverzeichnis

Abk.	Abkürzung
AES	Advanced Encryption Standard
AP	Access Point
CBC-MAC	Cipher Block Chaining Message Authentication Code
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
EAPOL	Extensible Authentication Protocol over Local Area Network
GCMP	Galois/Counter Mode Protocol
GTK	Group Temporal Key
HTTPS	Hypertext Transfer Protocol Secure
IEEE	Institute of Electrical and Electronics Engineers
IV	Initialisierungsvektor
KCK	Key Confirmation Key
KEK	Key Encryption Key
KRACK	Key Reinstallation AttaCK
MAC	Media Access Control -oder- Message Authentication Code
MIC	Message Integrity Check
MitM	Man-in-the-Middle
OSA	Open System-Authentifizierung
PMK	Pairwise Master Key
PSK	Preshared Keys
TK	Temporal Key
TKIP	Temporal Key Integrity Protocol
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2

1 Einleitung

Wi-Fi Protected Access 2, kurz WPA2, wurde im Jahr 2004 zum Standard für die Authentifizierung und Verschlüsselung von WLANs, die auf den IEEE-Spezifikationen 802.11 basieren. Seitdem wurde WPA2 zum meist genutzten Standard für die Sicherung von WLAN-Netzen weltweit, bei nahezu allen geschützten WLAN-Netzen kommen verschiedene Versionen von WPA2 zum Einsatz. WPA2 wird seit über einem Jahrzehnt eingesetzt und wurde als sehr ausgereift und sicher bezeichnet. Zudem wurde die Sicherheit des Standards formell bewiesen.

Mitte Oktober stellten zwei IT-Sicherheits-Forscher der belgischen Universität Leuven ein Paper vor, in dem sie beschreiben, wie WPA2 trotz dieses formellen Beweises zu brechen ist. [3] Der von ihnen beschriebene Angriff richtet sich gegen den Vier-Wege-Handshake, der sich über 14 Jahre bewährt hat, und erhielt den Namen KRACK.

Dieses Seminar stellt das Paper der zwei IT-Sicherheits-Forscher Mathy Vanhoef und Frank Piessen zum KRACK-Angriff vor. Dabei werden zunächst die Grundlagen von WPA2, insbesondere der Vier-Wege-Handshake vorgestellt. Anschließend folgt ein Abschnitt über das XOR-Problem von Verschlüsselungen, bevor der Angriff auf den Vier-Wege-Handshake beschrieben wird. Den Abschluss des Seminars bildet eine Abschätzung des Gefahrenpotentials und eine Zusammenfassung der Schutzmöglichkeiten. Neben der Beschreibung des KRACK-Angriffes soll auch beschrieben werden, warum der formale Beweis keine Sicherheit garantieren konnte.[1]

2 Grundlagen

Um KRACK verstehen zu können, ist ein gewisses Maß an Hintergrundwissen über WPA2 erforderlich. Daher werden in diesem Abschnitt zunächst die Grundlagen zu WPA2 und insbesondere der Vier-Wege-Handshake erläutert, bevor dann im nächsten Abschnitt die Beschreibung des Angriffes folgt.

2.1 WPA2 nach IEEE 802.11i

Der ursprüngliche Standard-Verschlüsselungsalgorithmus für drahtlose Netze nach dem IEEE 802.11-Standard ist „Wired Equivalent Privacy“, kurz WEP. Aufgrund verschiedener Schwachstellen gilt das Verfahren schon seit längeren als unsicher. So kann ein Angreifer aus in wenigen Minuten gesammelten Daten in Sekunden das Passwort berechnen.[12]

Zu dem Zeitpunkt, als Forscher zeigten, dass WEP grundlegend gebrochen ist, war eine Erweiterung des Standards zwar in Arbeit, aber größtenteils noch nicht verabschiedet. Daher wurde eine vorläufige Version des Standard IEEE 802.11i als Zwischenlösung unter den Namen WPA aus den schon verabschiedeten Teilen herausgegeben. Mit ihr wurden dynamische Schlüssel auf Grundlage des Temporal Key Integrity Protocol, kurz TKIP, und auch der Vier-Wege-Handshake, der den Angriffspunkt von KRACK bildet, eingeführt. Während der weiteren Entwicklung des 802.11i-Zusatzes wurden schon Geräte mit der Zwischenlösung WPA betrieben.[1]

Mit der Ratifizierung der endgültigen Version D9.0 von 802.11i wurde WPA2 als offiziell ratifizierte Version eingeführt. Mit der Ratifizierung wurde auch der Verschlüsselungsalgorithmus AES in den Standard integriert. Zum 1. September 2004 wurden die ersten Geräte von der Herstellervereinigung Wi-Fi Alliance mit WPA2 zertifiziert. WPA2 verwendet als Verschlüsselungsalgorithmus den Advanced Encryption Standard, abgekürzt AES. Außerdem wurde in WPA2 zu dem TKIP Protokoll, welches aus WPA übernommen wurde, ein weiteres Protokoll eingeführt. Das neue Protokoll trägt den langen Namen "Counter Mode with Cipher Block Chaining Message Authentication Code Protocol", welcher sich auf CCMP verkürzen lässt. Wozu diese Protokolle dienen, wird in einem späteren Kapitel verdeutlicht.

Wie in der Einleitung schon erwähnt galt WPA2 als sehr ausgereift und sicher. Bis zur Vorstellung von KRACK waren nur Wörterbuchangriffe auf das Passwort bekannt, welche durch ein geeignetes Passwort verhindert werden konnten.[4]

2.2 Authentifizierung und der Vier-Wege-Handshake

Der Verbindungsaufbau zwischen Client und Access Point, kurz AP, wird vom Client initiiert. Dazu beginnt der Client sich mit dem AP zu authentifizieren. Dabei wird die Open System-Authentifizierung, kurz OSA, verwendet, wodurch es jedem Client möglich ist, sich zu authentifizieren. Die OSA ist eine offene Authentifizierung, die eine ungesicherte Verbindung zum AP bereitstellt. Dieser Schritt stellt aber keine tatsächliche Authentifizierung dar. Die tatsächliche Authentifizierung findet während des nachfolgenden Vier-Wege-Handshakes statt. Nach der offenen Authentifizierung sendet der Client einen „association request“ Verbindungs-Request an den AP, um sich mit dem Netzwerk zu verbinden. Diese Nachricht enthält die Paarweisen- und Gruppen-Chiffre Suites, die der Client verwenden möchte. Eine Cipher Suite beinhaltet dabei eine standardisierte Sammlung kryptographischer Verfahren mit zugehörigen Blockgrößen und den festgelegten Modies. Auf den Verbindungs-Request antwortet der AP mit einem „association response“ Verbindungs-(Zuordnungs)-Response. Dabei teilt er dem Client mit, ob der Verbindungsaufbau erfolgreich war.[1]

Abbildung 2.1: Authentifizierung

Nach dem offenen Verbindungsaufbau folgt der Vier-Wege-Handshake. Mithilfe dieses Verfahrens erfolgt die gegenseitige Authentifizierung. Sie basiert auf einem gemeinsamen Schlüssel, der „Pairwise Master Key“, kurz PMK, genannt wird. Für die Verteilung dieses Schlüssels gibt es zwei Möglichkeiten. Entweder wird der PMK von einem „Preshared Key“, kurz PSK, also einem vorab geteilten Passwort abgeleitet, dies wird meist in kleineren Netzwerken gemacht, oder es kommt ein Authentifizierungsserver mit entsprechenden Zugriffskontroll-Protokollen zum Einsatz. Dies ist meist in größeren Netzwerken der Fall und macht den PSK überflüssig. Ziel des Vier-Wege-Handshakes ist neben der

Authentifizierung das Aushandeln eines neuen Sitzungsschlüssels, der als „Pairwise Transient Key“, abgekürzt PTK, bezeichnet wird. Der PTK wird gebraucht, um für die eigentliche Kommunikation die temporären Schlüssel zu berechnen.

Der Vier-Wege-Handshake besteht, wie der Name schon andeutet, aus vier einzelnen Nachrichten, die zwischen dem Client und dem AP ausgetauscht werden. Während dieses Verfahrens wird der Client als „Supplicant“ und der AP als „Authenticator“ bezeichnet. Vor dem Senden und nach dem Empfangen von Nachrichten erfolgen dabei auf beiden Seiten noch weitere Aktionen.

Die vier Nachrichten sind dabei über EAPOL-Frames definiert, die wie folgt aufgebaut sind. Am Anfang steht der Header, über ihn wird definiert, um welche Nachricht des Handshakes es sich handelt. Danach folgt das Wiederholungszählerfeld, mit ihm werden wiederholte Nachrichten gekennzeichnet. Der Authenticator erhöht den Wiederholungszähler immer nach dem Übertragen eines Frames. Der Supplicant dagegen antwortet immer mit dem Wiederholungszähler der Nachricht, auf die er antwortet. Das „Nonce“-Feld wird dazu genutzt, die generierten Nonces zu transportieren. Wenn die Nachricht genutzt wird, um einen Gruppenschlüssel „Group Temporal Key“, kurz GTK, zu transportieren, enthält das „Receive Sequence Counter“-Feld, kurz RSC, die Startpaketnummer dieses Schlüssels. Das Feld für den eigentlichen Gruppenschlüssel befindet sich am Ende des Frames. Es wird mit dem „Key Encryption Key“, abgekürzt KEK, verschlüsselt. Der GTK wird genutzt, um Broadcast und Multicast, die übers WLAN gesendet werden, zu verschlüsseln. Das Frame wird mit den „Key Confirmation Key“, kurz KCK, gesichert, der im „Message Integrity Check“-Feld, kurz MIC, transportiert wird.

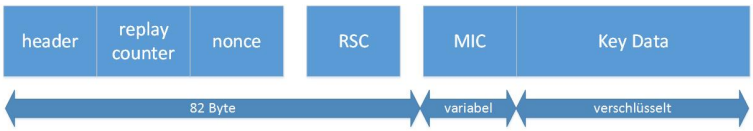

Abbildung 2.2: Aufbau einer Nachricht

Nachfolgend wird der Ablauf des Vier-Wege-Handshakes einmal schematisch in vier Abschnitten dargestellt. Die Notation dabei ist wie folgt: MsgN (r, Nonce; GTK). Wobei „N“ für die Nte Nachricht des Vier-Wege-Handshake steht. Das r gibt den Stand des Wiederholungszählers und „Nonce“ die zu transportierende Nonce an, falls diese vorhanden ist. Alle Parameter, die nach dem Semikolon folgen, werden im Schlüsseldatenfeld transportiert und sind damit verschlüsselt.[5]

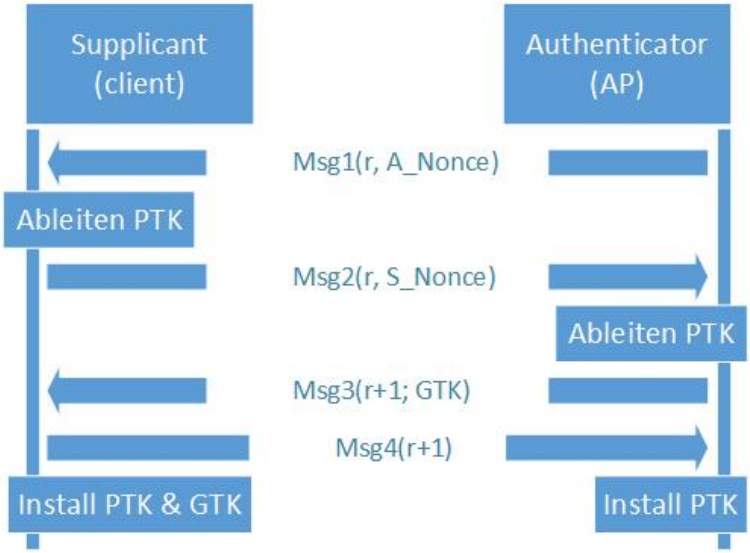

Abbildung 2.3: Vier-Wege-Handshake

1.Nachricht

Die erste Nachricht des Vier-Wege-Handshakes wird vom Authenticator an den Supplicant geschickt. Sie enthält die „Authenticator Nonce“, abgekürzt a-Nonce, und ist die einzige EAPOL-Nachricht, die nicht durch einen MIC geschützt ist.

Nachdem der Supplicant die Nachricht empfangen hat, berechnet er den PTK. Dazu erzeugt er zuerst die „Supplicant Nonce“, kurz s-Nonce. Der PTK wird aus dem vorab bekannten PMK, der empfangenen a-Nonce, der generierten s-Nonce und den MAC-Adressen vom Supplikanten und vom Authentifikator berechnet. Nach dem Generieren wird der PTK in den KCK, den KEK und einen „Temporal Key“, kurz TK aufgeteilt. Der KCK und der KEK werden, wie schon erwähnt, genutzt,um die weiteren Handshake Nachrichten zu schützen. Der TK wird unter anderem dazu genutzt, später die eigentlichen Daten zu verschlüsseln.

2.Nachricht

Die zweite Nachricht des Handshakes sendet der Supplicant, nachdem er den PTK erzeugt hat. Sie enthält die generierten s-Nonce und den zugehörigen EAPOL-MIC-Wert. Nach Empfangen dieser Nachricht kann der Authenticator genau wie der Supplicant den PTK berechnen. Dieses Vorgehen hat den Vorteil, dass der PTK niemals übertragen wird. Nachdem der Authenticator den PTK berechnet hat, kann auch er den TK ableiten. Danach überprüft er anhand seines TK den EAPOL-MIC-Wert der empfangenen Nachricht.

3.Nachricht

Nachdem der Authenticator den EAPOL-MIC-Wert geprüft hat, sendet er in der dritten Nachricht den GTK, wenn dieser in dem Netzwerk zum Einsatz kommt. Andernfalls teilt er dem Supplicanten mit der dritten Nachricht nur mit, dass der PTK aktiviert werden kann. Der GTK wird dabei verschlüsselt übertragen, und die Nachricht wird über den EAPOL-MIC-Wert des GTK gesichert.

4.Nachricht

Den Empfang der Nachricht drei bestätigt der Supplicant mit Senden der Nachricht vier und schließt so den Vier-Wege-Handshake ab. Nachdem er die Nachricht vier gesendet hat, setzt er den GTK und aktiviert den ausgehandelten PTK. Nachdem der Authenticator die Nachricht vier empfangen hat, aktiviert auch er den PTK. Der GTK wurde schon beim Start des AP gesetzt.

Zusammenfassend kann gesagt werden, dass die ersten beiden Nachrichten zum Austausch der beiden Nonces und die letzten beiden zum Transport des Gruppenschlüssels und zum Schutz vor Downgrade-Angriffen genutzt werden.[6] Der Vier-Wege-Handshake wurden formell analysiert und hat sich als sicher erwiesen.[1]

Dank des Hotspot 2.0-Programms können heutzutage auch öffentliche Hotspots eine authentifizierte Verschlüsselung nutzen, die auch einen solchen Vier-Wege-Handshake beinhaltet. Das Hotspot 2.0-Programm dient dazu, dem Nutzer das Wechseln zwischen verschiendenen WLAN Netzen so einfach wie möglich zu machen. Hotspots sollen dabei automatisch entdeckt werden und die Verknüpftung soll automatisiert erfolgen.[17]

2.3 Der Gruppenschlüssel-Handshake

Der Gruppenschlüssel wird wie schon erwähnt genutzt, um Broadcast und Multicast übers WLAN verschlüsselt an alle Clients gleichzeitig senden zu können. Im laufenden Betrieb ist es öfter nötig, den Gruppenschlüssel zu erneuern. Dies ist zum Beispiel immer der Fall, wenn ein Client die Gruppe verlässt und in regelmäßigen Abständen, wenn der Schlüssel abgelaufen ist. Um den GTK zu aktualisieren, gibt es den Gruppenschlüssel-Handshake, mit dem der Authentifikator den aktualisierten GTK an alle Clients sendet. Auch beim Gruppenschlüssel-Handshake kommt das schon bekannte EAPOL-Frame zum Einsatz.

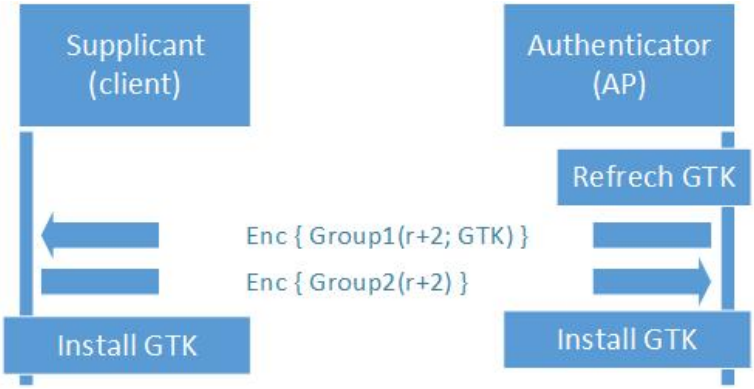

Abbildung 2.4: Gruppenschlüssel-Handshake

Um den neuen GTK zu verbreiten, sendet der Authentifikator die Nachricht eins des Gruppenschlüssel-Handshakes an alle Clients. Diese enthält auch den RSC des neuen Gruppenschlüssels. Der GTK ist bei der Übertragung mit dem KEK verschlüsselt. Die zweite und auch letzte Nachricht des Handshakes ist die Empfangsbestätigungs-Nachricht der Supplikanten, mit der er den neuen GTK bestätigt. Je nach Implementierung des Authentifikators sendet dieser die neuen Multicast-Pakete direkt nach Senden der Nachricht eins schon mit dem neuen GTK gesichert, oder er nutzt den alten GTK noch so lange, bis alle Supplikanten den Schlüssel betätigt haben, und installiert erst dann den neuen Schlüssel.

Da ein Gruppenschlüssel-Handshake nur nach einem erfolgreichen Vier-Wege-Handshake erfolgt, ist zu diesem Zeitpunkt ein PTK installiert. Somit ist der gesamte EAPOL-Rahmen durch das Daten-Vertraulichkeitsprotokoll geschützt.

Auch der Gruppenschlüssel-Handshake wurden formell analysiert und hat sich ebenfalls als sicher erwiesen.[1]

2.4 Die Vertraulichkeits- und Integritätsprotokolle

In der IEEE-Spezifikation 802.11i sind zwei kryptografische Verfahren definiert. Genauer eines in der Zwischenlösung WPA und ein weiteres in WPA2, welches das Erste aufgrund von Sicherheitsbedenken ersetzt.

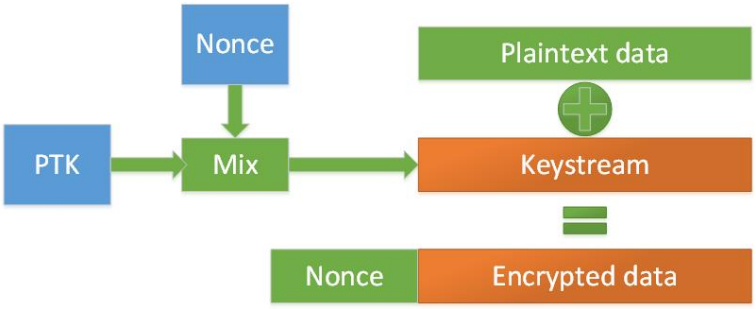

Abbildung 2.5: Ablauf der Verschlüsselung

Mit WPA wurde das „Temporal Key Integrity Protocol“, abgekürzt TKIP, eingeführt. Es verwendet zwei 64-Bit lange „Message Integrity Check“-Schlüssel, kurz MIC-Schlüssel. Der eine wird für die Kommunikationsrichtung vom AP zum Client, und der andere für die Gegenrichtung genutzt. Sie werden zusammen mit dem 128 Bit langen Verschlüsselungsschlüssel aus dem TK Anteil des PTK gebildet. Zur Verschlüsselung der Nutzdaten kommt RC4 zum Einsatz. RC4 ist eine Stromverschlüsselung, die den Klartext Bit für Bit per XOR mit einem einmaligen Schlüssel verknüpft. Dieser einmalige Schlüssel setzt sich aus den gebildeten 128-Bit-Verschlüsselungsschlüssel, der Absender-MAC-Adresse und einer 48-Bit-Nonce zusammen. Um einen einmaligen Key Stream zu erhalten, wird die Nonce nach jedem Übertragen eines Frames inkrementiert. Nach dem Vier-Wege-Handshake wird sie beim Installieren der TK auf 1 initialisiert.

Mit der Einführung von WPA2 wurde auch das (AES-) CCMP-Protokoll veröffentlicht. Es ist derzeit das am weitesten verbreitetste und am häufigsten verwendete Protokoll zur Verschlüsselung und Integritätssicherung. Es besteht aus zwei Komponenten. Die „Counter Mode“-Komponente, abgekürzt CM, ist für die Verschlüsselung der Daten zuständig. Der „Cipher Block Chaining Message Authentication Code“, kurz CBC-MAC, sichert die Integrität und Authentizität der Daten.

Das Protokoll arbeitet mit einer Block- und Schlüssellänge von 128 Bit. Es basiert darauf, dass eine Nonce, die als Zähler genutzt wird, verschlüsselt und mit der Nachricht XOR-verknüpft wird. Somit ist zur Ver- und Entschlüsselung nur ein Schlüssel notwendig. Als Schlüssel kommt dabei der TK zum Einsatz. Das Verfahren ist sicher, solange der Initialisierungsvektor, kurz IV, unter einem bestimmten Schlüssel einmalig ist. Als IV kommen dabei eine Verkettung aus der Absender-Hardware-Adresse, auch MAC-Adresse genannt[18], ein 48-Bit Nonce und einige zusätzliche Flags zum Einsatz. Die Nonce wird, wie schon erwähnt, als Zähler benutzt und bei der Installation der TK auf 0 initialisiert. Vor

dem Senden jeder Nachricht wird er dann um eins inkrementiert. Somit wird sichergestellt, dass der IV auf den Schlüssel bezogen immer einmalig ist.

Zur Authentisierung und zum Schutz der Integrität wird eine Prüfsumme berechnet. Dazu wird jeder verschlüsselte Datenblock mit seinem Nachfolger XOR-verknüpft und das Ergebnis AES verschlüsselt. Der letzte Block dieser Berechnungskette dient dann als Prüfsumme.[7]

Das CCMP-Protokoll wurde ebenfalls formal analysiert und wurde, wie auch der Vier-Wege-Handshake, als sicher eingestuft.

Der Broadcast- oder Multicast-Datenverkehr geht immer vom AP aus. Das heißt Broadcast- oder Multicast-Frames, die ein Client senden möchte, sendet er als Unicast-Frame an den AP, der sie mit dem Gruppenschlüssel verschlüsselt und an alle Clients innerhalb seiner Reichweite weiterleitet. So wird sichergestellt, dass alle Clients in Reichweite des AP die Nachricht empfangen und nicht nur die Clients in Reichweite des sendenden Clients.

3 KRACK

Der KRACK entstand aus der Nachforschung der zwei IT-Sicherheits-Forscher Mathy Vanhoef und Frank Piessen zur Sicherheit von WPA2. Dabei fielen ihnen folgende Zeilen Pseudocode aus dem 802.11i Standard auf:

```
/* install the PTK */
if ((*ic->ic_set_key)(ic, ni, k) != 0) {
   reason = IEEE80211_REASON_AUTH_LEAVE;
   goto deauth;
}
ni->ni_flags \&= ~IEEE80211_NODE_TXRXPROT;
ni->ni_flags |= IEEE80211_NODE_RXPROT;
```

(aus den Folien zur Präsentation des Angriffes.)[7]

Der Abschnitt warf die Frage auf, was passieren würde, wenn die Funktion „ic_set_key“ wieder aufgerufen würde. Würde das zu einer erneuten Installation des Schlüssels führen? Aus diesen Überlegungen entstand die Idee zu KRACK. Dabei sollten folgende Fragen geklärt werden. Wie kann erreicht werden, dass die Funktion „ic_set_key“ mehrmals mit dem gleichen Schlüssel aufgerufen wird? Was sind die Auswirkungen, wenn der Schlüssel neu installiert wird und wie ließe sich dies für einen Angriff nutzen?

In den nachfolgenden Kapiteln wird zuerst erläutert, was die Hauptschwachstelle der in WPA2 eingesetzten Verschlüsselung ist. Anschließend wird beschrieben, wie diese Schwachstelle prinzipiell vom KRACK ausgenutzt wird. Danach folgt ein Kapitel, welches beschreibt, wie es zu dieser Schwachstelle kommen konnte. Anschließend folgt ein Kapitel, in dem detailliert beschrieben wird, wie KRACK die verschiedenen Handshake Varianten angreift. Abschließend folgt noch ein Kapitel über KRACK in der Praxis.

3.1 Brechen von Verschlüsselungen, das XOR Problem

Wie schon erwähnt wird die Klartext Nachricht verschlüsselt, in dem sie mit der verschlüsselten Nonce XOR-verknüpft wird. Die XOR-Verknüpfung ist eine in der Kryptographie sehr häufig genutzte Funktion, um Daten sicher zu verschlüsseln. Das unknackbare One Time Pad ist eines der häufigsten Verfahren, die diese Funktion nutzen. Das Verfahrens ist sehr einfach. Dabei wird die Bit-Folge der Nachricht oder der Daten mit der Bit-Folge des Schlüssels via XOR bitweise verknüpft.

Die XOR-Verknüpfung hat eine ganz zentrale Schwachstelle. Wird ein Schlüssel wiederverwendet, ist die Verschlüsselung gebrochen. Da die XOR-Verknüpfung assoziativ ist, ist es nicht relevant, in welcher Reihenfolge Daten und Schlüssel miteinander verknüpft werden. Hat nun ein Angreifer zwei Nachrichten, die mit dem gleichen Schlüssel k verschlüsselt wurden, und kennt den Klartext einer der beiden Nachrichten, kann er den Klartext der anderen Nachricht berechnen.

Die folgende Zeile zeigt, wie sich der Schlüssel aus zwei verschlüsselten Nachrichten herausrechnen lässt. Allerdings ist so nur die XOR-Verknüpfung der beiden Nachrichten in Klartext berechenbar. A' und B' sind hierbei der verschlüsselte Nachrichtentext, A und B der Nachrichtentext in Klartext und k der Schlüssel.

$A' \oplus B' = (A \oplus k) \oplus (B \oplus k) = A \oplus (k \oplus k) \oplus B = A \oplus B$

Ist nun noch eine der Nachrichten in Klartext vorhanden, lässt sich folgende Formel aufstellen.

$A' \oplus B' \oplus B = A$

Dabei ergibt sich aus der Verknüpfung von B' und B der Schüssel, der A' entschlüsselt.

Daher ist es für die Sicherheit der Verschlüsselungsverfahren, die auf der XOR-Verknüpfung beruhen, zwingend notwendig, dass ein Schlüssel nur ein einziges Mal verwendet wird.[9]

3.2 Funktionsprinzip von KRACK

Die zentrale Schwachstelle der Verschlüsselung war natürlich auch bei der Entwicklung von WPA2 bekannt. Daher wird, wie schon im Grundlagen-Teil erwähnt, die Nachricht nicht direkt mit dem TK XOR-verknüpft, sondern mit dem verschlüsselten TK. Als IV für die Verschlüsselung des TK kommt dabei eine Nonce zum Einsatz, die nach jeder gesendeten Nachricht um eins inkrementiert wird. So soll sichergestellt werden, dass nie zweimal die gleiche Nonce zum Einsatz kommt, und somit auch

das Ergebnis der Verschlüsslung des TK immer einmalig ist. Damit sollte die zentrale Schwachstelle umgangen sein.

Mit dem Wissen um die Funktion „ic_set_key“ und die zentrale Schwachstelle der Verschlüsselung ist die Idee zu KRACK nun naheliegend. Wenn ein Weg gefunden würde, die Funktion „ic_set_key“ mit dem gleichen Schlüssel noch einmal aufzurufen, würde der Schlüssel neu installiert und auch der zugehörige Paketzähler, die Nonce, zurückgesetzt. Dies würde dazu führen, dass alle Schlüssel, die seit der ersten Installation genutzt wurden, erneut zum Einsatz kommen würden. Dabei ist zu beachten, dass sich verschlüsselte Pakete mit bekannten Daten fast immer irgendwie finden oder erzwingen lassen.

Im Grundlagen-Teil wurde auch erwähnt, dass die Installation des TK, was ja die Aufgabe der Funktion „ic_set_key“ ist, während des Vier-Wege-Handshakes ausgelöst wird. Also führt der Weg zur Neuinstallation des TK über die Manipulationen im Vier-Wege-Handshake.

Da bei WPA2 verschiedene Vier-Wege-Handshake Variationen zum Einsatz kommen, folgt an dieser Stelle nur eine Beschreibung des grundsätzlichen Ablaufes der Manipulationen. Eine detailliertere Beschreibung folgt in einem späteren Kapitel.

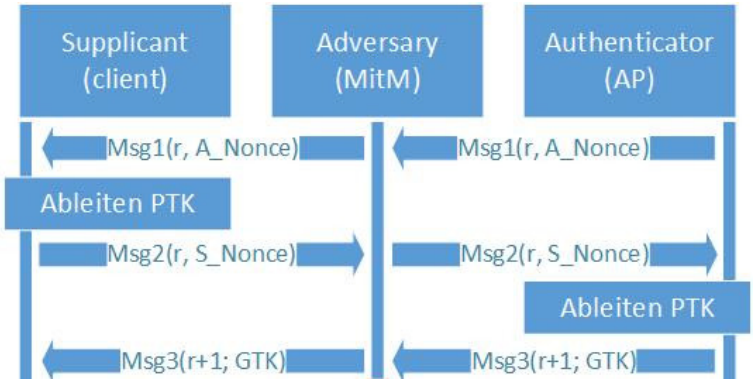

Abbildung 3.1: Vier-Wege-Handshake

Wie im Grundlagen-Teil beschrieben erfolgt die Installation des TK auf Supplicanten Seite nach dem Senden der Nachricht vier. Die Nachricht vier ist dabei die Empfangsbestätigung der Nachricht drei, die der Authenticator schickt. Damit der Supplicant die Nachricht vier erneut sendet und dabei auch den TK neu installiert, muss erreicht werden, dass der Authenticator die Nachricht drei erneut schickt. Dies ist der Fall, wenn er die Empfangsbestätigung in Form der Nachricht vier nicht empfängt. Wird nun verhindert, dass der Authenticator die Nachricht vier empfängt, muss dieser davon ausgehen, dass seine Nachricht drei den Supplicanten nicht erreicht hat und sendet die Nachricht drei erneut. Was kein Problem wäre, hätte diese tatsächlich den Supplicanten nicht erreicht. So aber hat der Supplicant seine Nachricht vier schon gesendet und den TK installiert. Da mit dieser Aktion der Vier-Wege-Handshake für ihn abgeschlossen ist, beginnt er verschlüsselte Nachrichten zu senden. Erreicht ihn nun die neu

gesendete Nachricht drei des Authenticators, sendet er seine Nachricht vier und installiert den selben TK erneut. Dabei wird auch die Nonce neu initialisiert. Danach beginnt er wieder, verschlüsselte Nachrichten zu senden. Dabei werden dann die Schlüssel wieder verwendet und der Angreifer kann die Nachrichten entschlüsseln.

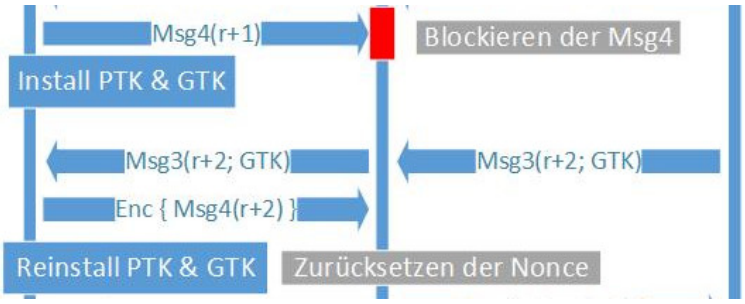

Abbildung 3.2: Blockierte Nachricht vier

3.3 Der Designfehler in 802.11i und formale Sicherheit

Bei einer eigentlich so offensichtlichen Schwachstelle stellt sich zwangsläufig die Frage, wie es dazu kommen konnte. Der Hauptgrund ist ein Designfehler in der 802.11i-Änderung, mit der WPA2 veröffentlicht wurde. Es fehlen wichtige Informationen und Definitionen.

So enthält der Standard keine formale Zustandsmaschine des Vier-Wege-Handshakes. Das Verhalten des Supplicanten wird nur durch Pseudocode beschrieben. Dabei wird lediglich beschrieben, wie bestimmte Handshake-Nachrichten verarbeitet werden sollten. Die wichtigen Informationen, wann bestimmte Nachrichten zulässig sind, sind nicht enthalten. So ist auch das erneute Empfangen und Verarbeiten der Nachricht drei zulässig.

Beachtenswert an KRACK ist, dass die Sicherheitseigenschaften der angegriffen Verfahren, also des Vier-Wege-Handshakes, des Gruppenschlüssel-Handshakes und des CCMP-Protokolls, in der formalen Analyse bewiesen wurden. Das Problem an den formellen Sicherheitsbeweisen in diesem Fall ist, dass sie nicht das Zusammenspiel der Verfahren abbilden. Somit liegt KRACK außerhalb der Grundannahme des formellen Sicherheit-Beweises und widerspricht ihm somit nicht.

3.4 Angriff auf den Handshake im Detail

Im WPA2-Standard sind verschiedene Handshake Variationen, wie der Vier-Wege-Handshake und der Gruppenschlüssel-Handshake definiert. In den nachfolgenden Unterkapiteln wird der Angriff auf zwei der verschiedenen Handshakes erläutert.

Der Angriff auf jeden Handshake wird aus einer „Man-in-the-Middle“-Position, kurz MitM, zwischen dem Supplicanten und dem Authenticator geführt. So können bestimmte Nachrichten blockiert oder gespeichert und später weitergeleitet werden.

Allerdings kann der Angriff nicht immer gleich ausgeführt werden, da nicht bei allen WLAN-Clients der Standard ordnungsgemäß implementiert ist. So akzeptieren Windows und iOS zum Beispiel keine erneuten Übertragungen von Nachricht drei und verstoßen somit gegen den Standard 802.11. Allerdings sind sie anfällig für Angriffe auf den Gruppenschlüssel-Handshake. Daher muss der Angriff bei manchen Clients etwas abgewandelt oder verfeinert werden.

3.4.1 Vier-Wege-Handshake

Beim Angriff auf den Vier-Wege-Handshake wird unterschieden, ob der Client die erneute Übertragung von Nachricht drei als Klartext akzeptiert oder nur, wenn sie verschlüsselt ist.

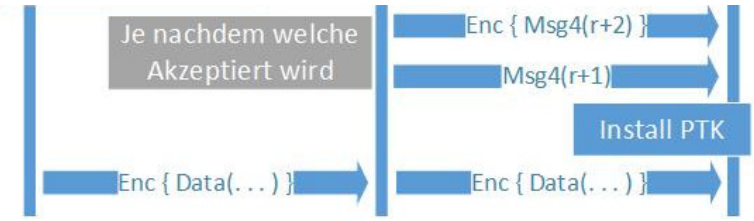

Abbildung 3.3: Senden der Nachricht vier

Wenn der Client die erneute Übertragung von Nachricht drei als Klartext akzeptiert, läuft der Angriff im wesentlichen so ab, wie im vorigen Kapitel beschrieben. Der Angreifer kann die Nachricht vier des Clients blockieren. Daraufhin überträgt der Authentifizierer die Nachricht drei erneut, weil er die Nachricht vier nicht empfangen hat. Diese leitet der Angreifer an den Client weiter. Der Angreifer kann keine alte Nachricht drei wiedergeben, weil der EAPOL-Wiedergabezähler der Nachricht nicht mehr aktuell ist. Allerdings kann der Angreifer beliebig lange warten, bevor er die erneut übertragene Nachricht drei an den Client weiterleitet. Der Abschluss des Angriffes auf den Vier-Wege-Handshake ist etwas komplizierter, da der Client den TK schon bei der ersten Nachricht drei installiert hat. Daher sendet er seine Antwort auf die zweite Nachricht drei verschlüsselt. Der AP dagegen hat den TK noch nicht installiert und erwartet daher eine unverschlüsselte Nachricht vier. Somit würde er eine verschlüsselte Nachricht vier ablehnen. Da der AP aber laut 802.11-Standard jeden Wiederholungszähler, der im Vier-Wege-Handshake verwendet wurde, akzeptiert, nicht nur den neuesten, kann der Angreifer die ältere unverschlüsselte Nachricht vier als Empfangsbestätigung auf die erneut gesendete Nachricht drei an den AP weiterleiten. Damit ist der manipulierte Vier-Wege-Handshake abgeschlossen. Der Angreifer kann den Angriff erneut durchführen, indem er den Client authentifiziert. Dieser verbindet sich daraufhin erneut mit dem Netzwerk und führt einen neuen Vier-Wege-Handshake aus.

Wenn der Client die erneute Übertragung von Nachricht drei als Klartext nicht akzeptiert, wird der Angriff komplizierter. Eine Möglichkeit, die die Sicherheitsforscher entdeckt haben, ist beide Nachrichten drei kurz hintereinander zu senden. Dabei landet die zweite Nachricht drei in der Paketempfangswarteschlange und wird auch unverschlüsselt akzeptiert. Dazu lässt der Angreifer den AP und den Client die ersten beiden Nachrichten normal austauschen und blockiert dann die Nachricht drei. Wenn der AP die zweite Nachricht drei schickt, sendet der Angreifer beide Nachrichten drei direkt hintereinander an den Clienten. Dieser wertet die erste aus und in der Zeit, die er für das Auswerten der zweiten braucht, sendet er schon verschlüsselte Pakete. Hat er dann die zweite Nachricht ausgewertet, installiert er den Schlüssel neu.

3.4.2 Gruppenschlüssel-Handshake

Ein Angriff auf den Gruppenschlüssel-Handshake ermöglicht es dem Angreifer, dem Clienten ältere Broadcast-Nachrichten als neue Nachrichten unterzujubeln. Das Vorgehen richtet sich dabei nach dem Verhalten des APs. Dieses unterscheidet sich im Zeitpunkt der Installation des GTK. Entweder wird dieser unmittelbar nach dem Senden der Gruppennachricht eins installiert, oder erst nachdem alle Clients mit der Gruppennachricht zwei geantwortet haben.

Bei sofortiger Schlüsselinstallation gestaltet sich der Angriff recht einfach. Der AP sendet die Gruppennachricht eins und installiert den GTK. Der Angreifer sendet die Nachricht an den Client, blockiert allerdings seine Antwort. Der AP sendet daraufhin eine weitere Gruppennachricht eins, die der Angreifer blockiert und zwischenspeichert. Der Angreifer wartet dann bis eine Broadcast-Datennachricht gesendet wird und leitet diese an den Clienten weiter. Danach leitet er ihm auch die zwischenspeicherte Gruppennachricht eins weiter. Dadurch ist es dem Angreifer möglich, die Broadcast-Datennachricht erneut abzuspielen. Dies funktioniert, da durch das Senden der zwischenspeicherten Gruppennachricht eins der Wiedergabezähler neu initialisiert wird.

Bei verzögerter Schlüsselinstallation ist das Vorgehen mühsamer, da der vorher beschriebene Angriff hier nicht funktionieren würde. Das liegt daran, dass der AP erst nach Erhalten aller Antwort-Gruppennachrichten den neuen GTK installiert. Bis zu diesem Zeitpunkt bleibt sozusagen alles beim Alten, und der Client würde keine wiederholten Nachrichten des Angreifers akzeptieren. Allerdings akzeptiert der AP, wie schon erwähnt, auch ältere Wiederholungszähler, solange diese im Handshake verwendet wurden. Das Vorgehen ist ähnlich wie beim vorherigen Angriff. Der AP sendet die Gruppennachricht eins, die der Angreifer an den Client weiterleitet. Die Antwort des Client blockiert und speichert der Angreifer. Der AP sendet daraufhin eine weitere Gruppennachricht eins, die der Angreifer genau wie beim vorherigen Angriff blockiert und zwischenspeichert. Allerdings antwortet er jetzt selbst auf diese Nachricht und zwar mit der ersten zwischenspeicherten Antwort des Client. Daraufhin installiert der AP den GTK und der weitere Angriff läuft analog zum Vorherigen ab.

3.5 Praktische Umsetzung

Wie schon erwähnt wird der Angriff aus einer „Man-in-the-Middle“-Position zwischen dem Client und dem AP geführt. Dazu wird ein Klon des Netzwerkes auf einem anderen Kanal erzeugt. Dabei wird auch die MAC-Adresse des AP mit übernommen, da diese Teil der Schlüsselberechnung ist. So kann der Angreifer gezielt Nachrichten weiterleiten, speichern und auch manipulieren.

Wenn jetzt der Client sich mit dem WLAN-Netzwerk verbinden möchte, wird er versuchen, sich mit dem echten Netzwerk zu verbinden. Dies kann verhindert werden, indem der Angreifer spezielle WLAN-Steuernachrichten sendet, die dem Client befehlen, auf einen anderen Kanal zu wechseln. Dadurch verbindet der Client sich doch mit den Netzwerk des Angreifers. Jetzt kann der Angreifer auf die Nachrichten zugreifen und seinen Angriff durchführen.

Zum Beispiel kann er bei einem Angriff auf ein Android oder Linux Gerät durch KRACK den Datenverkehr in Klartext mitlesen. Wenn er dazu noch ein sslstrip-Programm verwendet, welches versucht, den HTTPS Schutz von nicht ordnungsgemäß konfigurierten Webseiten zu entfernen[13], kann er mit Hilfe eines Analyse-Programms wie „Wireshark“ die Anmeldedaten des Clients zu bestimmten Webdiensten stehlen[14].

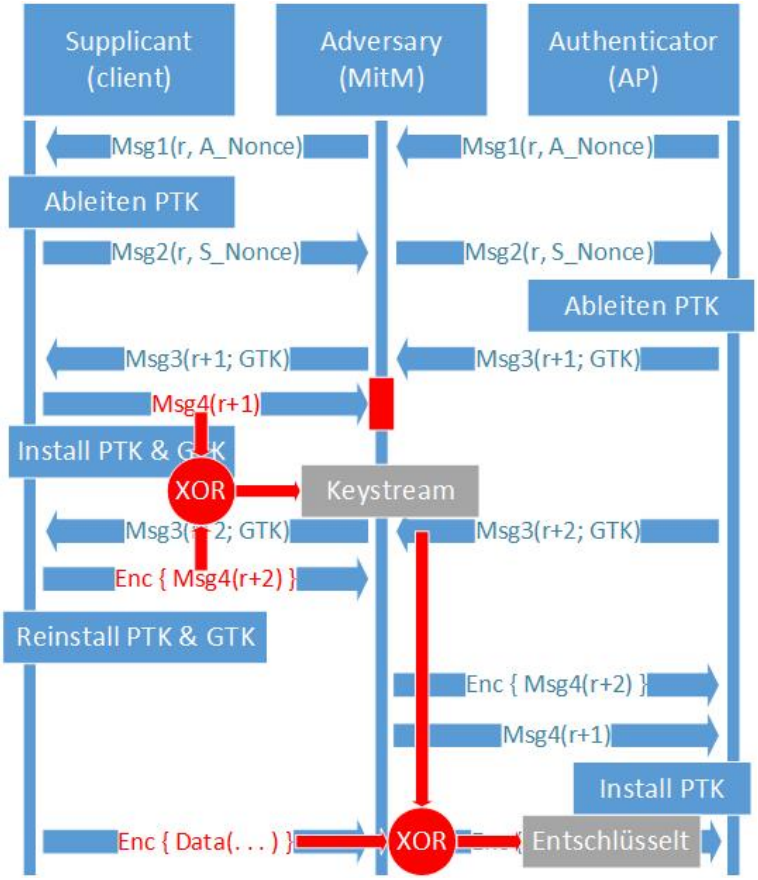

Abbildung 3.4: Entschlüsseln von Nachrichten

4 Gefahrenpotential und Angriffsszenarien

Da der WPA2 Standard das Angriffsziel von KRACK ist, sind praktisch alle WLAN-fähigen Geräte betroffen. Also vom Router über Smartphones und Desktoprechner bis zu Smarthome-Geräten kann alles angegriffen werden. Allerdings ist der Angriff auf die WLAN-Reichweite begrenzt. Das heißt in Normalfall auf 50 bis 100 Meter, also lokal sehr begrenzt. Außerdem sind die sicherheitsrelevanten Daten, die normale WLAN-Nutzer senden, wie Login-Daten, über die TLS-Verschlüsselung, die für HTTPS-Verbindungen zum Einsatz kommt, gesichert. Sind die Daten, die gesendet werden, vor der WPA2-Verschlüsselung schon durch andere Protokolle wie HTTPS oder Ende-zu Ende-Verschlüsselungsverfahren gesichert, ist deren Sicherheit durch KRACK nicht gefährdet.[10]

Durch KRACK wird das Sicherheits-Niveau sozusagen auf den Stand von offenen Hotspots reduziert. KRACK könnte daher eher zu gezielten Angriffen durch erfahrene Hacker genutzt werden. Die Möglichkeiten, wie in den Datenverkehr eingegriffen werden kann, hängt dabei vom verwendeten Verschlüsselungsalgorithmus ab. Unter WPA2 kommen dabei TKIP, CCMP und GCMP zum Einsatz. Das Galois/Counter Mode Protokol, kurz GCMP, wurde mit der 802.11ad Erweiterung als weiterer Verschlüsselungsalgorithmus in den WPA2 Standard aufgenommen.[15] Alle drei Protokolle verwenden eine Stromchiffre, um Nachrichten zu verschlüsseln.

Wird TKIP zur Verschlüsselung eingesetzt, lassen sich Nachrichten entschlüsseln und sogar fälschen. Dazu wird mit Hilfe der wiederverwendeten Nonce ein vollständiges TKIP-Paket einschließlich seines MIC-Feldes entschlüsselt. Mit dem Michael-Algorithmus kann aus der Klartext-Nachricht und dem entschlüsselten MIC-Wert der MIC-Schlüssel wiederhergestellt werden.[15] So können Nachrichten gefälscht werden, deren Absender das angegriffene Gerät ist.

Wird CCMP zur Verschlüsselung eingesetzt, sind praktische Angriffe auf die Wiedergabe und Entschlüsselung von Nachrichten beschränkt. Es sind Papers vorhanden, die sich mit dem Fälschen von Nachrichten bei sich wiederholenden Nonces befassen, allerdings sind diese Angriffe nur theoretisch und lassen sich nicht dazu nutzen, in der Praxis beliebige Nachrichten zu fälschen.[1](Verweis 66)

Wird GCMP zur Verschlüsselung eingesetzt, sind die Möglichkeiten verheerend. Ein Angreifer kann Nachrichten in einer bestimmten Kommunikationsrichtung wiederholen, entschlüsseln und fälschen. Die konkrete Richtung hängt dabei davon ab, welche Seite bei dem Handshake angegriffen wurde.

Durch Störsignale, durch die die Nachricht vier verloren geht, kann KRACK auch spontan auftreten, ohne dass ein Angreifer anwesend ist. Zumindest dann, wenn der Client die wiederholt gesendete Nachricht drei unverschlüsselt akzeptiert. Dies könnte ein Angreifer nutzen, um seinen Angriff zu tarnen. Wenn er nur selektiv einige der Nachrichten Nummer vier abfängt, ist sein Angriff kaum von zufälliger Hintergrundinterferenz zu unterscheiden.

Das größte Gefahrenpotential geht von der „All-Zero Encryption Key“ Schwachstelle aus. Diese ist im WLAN-Treiber „wpa_supplicant“ vorhanden, der bei Linux und bei Android-Geräten und auch bei Android Wear zum Einsatz kommt. Bei der Entwicklung des Treibers wurde auch die Bemerkung im 802.11-Standard umgesetzt, die indirekt vorschlägt, den TK aus dem Speicher zu löschen, nachdem er installiert wurde. Dies wurde so umgesetzt, dass er mit Nullen überschrieben wird. Dies führt dazu, dass ,wenn die Nachricht drei erneut gesendet wird, der gelöschte Schlüssel, der in dem Fall nur noch aus Nullen besteht, installiert wird. Somit ist die daraus resultierende Verschlüsselung unzureichend und lässt sich trivial knacken.

5 Lösungen und Hersteller-Updates

Der einfachste und sicherste Schutz vor KRACK ist zumindest für sensible Daten, wie Online-Banking und Online-Shopping mit Bezahlvorgängen, auf das Nutzen von WLAN zu verzichten und statt dessen über LAN das Internet zu nutzen. Wenn das nicht möglich ist, wie zum Beispiel bei Smartphones, sollte darauf geachtet werden, dass die Daten zusätzlich verschlüsselt sind, zum Beispiel durch die Nutzung von HTTPS.

Die Lücke, die KRACK in den 802.11i-Zusatz ausnutzt, ist zum Glück nur eine ungenaue beziehungsweise missverständliche Formulierung und kein Fehler in Funktionsprinzip von WPA2. Zum Schließen der Lücke ist nur eine Anpassung der Formulierung im Standard notwendig und nicht die Entwicklung eines neuen Standards. Laut der Webseite der Entdecker von KRACK, soll eine Anpassung des WLAN-Standards erfolgen, um explizit den Angriff zu verhindern. Die Anpassung des Standards soll mit älteren WPA2-Implementierungen abwärtskompatibel sein. Allerdings gibt es auf der Seite keine Informationen zu dem Zeitpunkt, wann dies geschieht. Vielmehr heißt es sinngemäß, dass die Zukunft zeigen wird, ob und wie der Standard aktualisiert wird.[2] Allerdings müssen die Änderungen des Standards auch in die zahlreichen Implementierungen übernommen und diese in Form von Updates auf die Geräte gebracht werden. Hier kommen die Hersteller ins Spiel, die diese Updates liefern müssen. Das Problem dabei ist die Vielzahl an Geräten, die mittlerweile über WLAN kommunizieren können. Viele der Gräte sind schon älter oder sind günstige No-Name Produkte. Bei ihnen wird sich die Bereitschaft der Hersteller, Updates für diese Produkte zu liefern, in Grenzen halten. Bei einigen Gräten fehlt auch schlicht und einfach die Möglichkeit, Updates einzuspielen. Daher wird vermutlich bei vielen Geräten die Sicherheitslücke niemals geschlossen.[11]

Auf der Seite der Wi-Fi Alliance heißt es, dass sie die globalen Zertifizierungslabore aufgefordert hat, die Sicherheit der Implementierungen zu testen. Dafür hat sie ein Tool zur Erkennung der Schwachstelle bereitgestellt. Außerdem schreibt sie, dass sie die Gerätehersteller ausführlich über diese Sicherheitslücke und die Möglichkeit diese zu schließen informiert hat. Auch hat die Wi-Fi Alliance die Hersteller zur Zusammenarbeit aufgefordert, um die notwendige Updates schnell bereitzustellen.[19]

Neben den Sicherheits-Updates, die die Lücken in WPA2 schließen sollen, bringt die baldige Einführung von WPA3 eine weitere Lösung für das Sicherheitsproblem. Mit einer Einführung ist ab 2019 zu rechnen. Neben einer besseren usability soll WPA3 auch die Sicherheit in WLAN erhöhen. Eine Angriff wie KRACK sollte dann nicht mehr möglich sein.[20]

6 Zusammenfassung und Fazit

Zusammenfassend kann gesagt werden, dass KRACK zwar ein ernstes Problem ist, aber kein GAU. KRACK ist auf die WLAN Reichweite beschränkt und kein Angriff, der übers Internet ausgeführt werden kann. Auch sind die wichtigen Daten wie das Online-Banking und Anmeldevorgänge durch die TLS-Verschlüsselung von HTTPS gesichert. Daher sollte verstärkt auf gesicherte Verbindungen geachtet werden.

Was KRACK neben den Lücken im WPA2 auch noch verdeutlicht, sind die Gefahren, die von nicht ausreichend präzise formulierten beziehungsweise mehrdeutigen Standards ausgehen. Ein besser ausgearbeiteter Standard hätte die Lücke verhindert. Die Verfahren an sich sind sicher, wenn sie richtig angewendet werden. Eine weitere Sache, die KRACK verdeutlicht, ist, dass formale Beweise keine Garantie für Sicherheit sind. Bei WPA2 spiegelt das Modell des Vier-Wege-Handshakes, das in formalen Beweisen verwendet wird, die Realität nicht vollständig wieder. Was dazu führt, dass es in der Realität Wege gibt, die an dem Beweis vorbei führen. Das Lesen von echtem Code hätte offenbaren können, dass Schlüssel neu installiert werden können. Allerdings ist, sobald ein Protokoll formal verifiziert ist, die Bereitschaft der Gemeinschaft zum Prüfen der tatsächliche Implementierungen eher gering. Somit kann ein formaler Beweis auch kontraproduktiv sein, da sich zu sehr auf ihn verlassen wird.

Zum Schluss steht dann noch die Frage im Raum, wer die Schuld an der Sicherheitslücke trägt. Ein Großteil der Schuld trifft, laut Sicherheitsforschern wie Matthew Green, nicht die Hersteller sondern den WPA2-Standard selbst und somit die IEEE, unter deren Regie er entwickelt wurde. Der Standard ist nicht oder nur sehr schwer zugänglich, da die IEEE ihre Standards unter Verschluss hält und Zugriff nur gegen Gebühren gewährt. Dies erschwert es unabhängigen Testern, Sicherheitslücken zu finden und offen zu legen.[9]

7 Verzeichnisse

7.1 Abbildungsverzeichnis

7.2 Literaturverzeichnis

[1] Vanhoef, Mathy; Piessens, Frank: *Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2.* In: mathyvanhoef.com URL: https://papers.mathyvanhoef.com/ccs2017.pdf (letzter Abruf am 12.08.2018)

[2] Vanhoef, Mathy: *Breaking WPA2 by forcing nonce reuse.* In: Key Reinstallation Attacks URL: https://www.krackattacks.com/ (letzter Abruf am 12.08.2018)

[3] Schirrmacher, Dennis; Schmidt, Jürgen: *WLAN ist angeKRACKt.* In: heise online URL: https://www.heise.de/ct/ausgabe/2017-23-WPA2-Luecke-KRACK-analysiert-und-eingeschaetzt-3869577.html (letzter Abruf am 12.08.2018)

[4] Eilers, Carsten: *WEP, WPA, WPA2 - WLAN-Schutz, aber richtig!.* In: ceilers-news.de URL: https://www.ceilers-news.de/serendipity/7-WEP,-WPA,-WPA2-WLAN-Schutz,-aber-richtig!.html (letzter Abruf am 12.08.2018)

[5] Schirrmacher, Dennis; Schmidt, Jürgen: *WLAN ist angeKRACKt.* In: heise online URL: https://www.heise.de/ct/ausgabe/2017-23-WPA2-Luecke-KRACK-analysiert-und-eingeschaetzt-3869577.html (letzter Abruf am 12.08.2018)

[6] Eilers, Carsten: *WLAN-Sicherheit 9 - Die Schlüssel von WPA2, Teil 1.* In: ceilers-news.de URL: https://www.ceilers-news.de/serendipity/908-WLAN-Sicherheit-9-Die-Schluessel-von-WPA2,-Teil-1.html (letzter Abruf am 12.08.2018)

[7] Eilers, Carsten: *WLAN-Sicherheit 11 - Der Counter-Mode/CBC-MAC von WPA2.* In: ceilers-news.de URL: https://www.ceilers-news.de/serendipity/912-WLAN-Sicherheit-11-Der-Counter-ModeCBC-MAC-von-WPA2.html (letzter Abruf am 12.08.2018)

[8] Vanhoef, Mathy: *Key Reinstallation Attacks: Breaking the WPA2 Protocol.* In: blackhat.com URL: https://www.blackhat.com/docs/eu-17/materials/eu-17-Vanhoef-Key-Reinstallation-Attacks-Breaking-The-WPA2-Protocol.pdf (letzter Abruf am 12.08.2018)

[9] Schmidt, Jürgen: *KRACK - so funktioniert der Angriff auf WPA2.* In: heise online URL: https://www.heise.de/security/artikel/KRACK-so-funktioniert-der-Angriff-auf-WPA2-3865019.html (letzter Abruf am 12.08.2018)

[10] Böck, Hanno; Beuth, Patrick: *Krack klingt schlimmer, als es ist.* In: Zeit Online URL: https://www.zeit.de/digital/datenschutz/2017-10/wlan-sicherheit-wpa2-krack-verschluesselung (letzter Abruf am 12.08.2018)

[11] Olivia von Westernhagen: *KRACK: Hersteller-Updates und Stellungnahmen.* In: heise online URL: https://www.heise.de/security/meldung/KRACK-Hersteller-Updates-und-Stellungnahmen-3863455.html (letzter Abruf am 12.08.2018)

[12] Dominik Blunk, Dr. Andreas Steffen: *WLAN-Hacking en passant.* In: heise online URL: https://www.heise.de/security/artikel/WEP-Verschluesselung-271122.html (letzter Abruf am 12.08.2018)

[13] Magnus, Nils: *Sslstrip täuscht HTTPS-Verbindung vor.* In: linux community URL: http://www.linux-community.de/nachrichten/sslstrip-taeuscht-https-verbindung-vor/ (letzter Abruf am 12.08.2018)

[14] Joos, Thomas: *Erste Schritte mit Wireshark.* In: IP Insider URL: https://www.ip-insider.de/erste-schritte-mit-wireshark-a-631469/ (letzter Abruf am 12.08.2018)

[15] Wikipedia Gemeinschaft: *Galois/Counter Mode.* In: wikipedia URL: https://de.wikipedia.org/wiki/Galois/Counter_Mode (letzter Abruf am 12.08.2018)

[16] *Security Analysis of Michael: the IEEE 802.11i Message Integrity Code.* In: University of Wollongong. URL: https://www.uow.edu.au/ jennie/WEB/WEB05/Michael.pdf (letzter Abruf am 12.08.2018)

[17] von Hoesslin, Christian *Hotspot 2.0 bringt neue Umsatzströme.* In: Computerwoche URL: https://www.computerwoche.de/a/hotspot-2-0-bringt-neue-umsatzstroeme,3065498 (letzter Abruf am 12.08.2018)

[18] Donner, Andreas *Was ist eine MAC-Adresse?.* In: IP Insider URL: https://www.ip-insider.de/was-ist-eine-mac-adresse-a-665074/ (letzter Abruf am 12.08.2018)

[19] *Security Update October 2017* . In: Wi-Fi Alliance URL: https://www.wi-fi.org/security-update-october-2017 (letzter Abruf am 12.08.2018)

[20] Zivadinovic, Dusan *WPA3 schützt vor WLAN-Einbrüchen und koppelt Geräte ohne Display an.* In: heise.de URL: https://www.heise.de/newsticker/meldung/WPA3-schuetzt-vor-WLAN-Einbruechen-und-koppelt-Geraete-ohne-Display-an-4092137.html (letzter Abruf am 12.08.2018)