Hochschule Wismar
Fakultät für Ingenieurwissenschaften
Bereich Elektrotechnik und Informatik

Bachelor-Thesis

ANALYSE UND SYNTHESE WPA2/WPA3

Eingereicht am:
von: Waldemar Stiefvater

Matrikelnummer:

Betreuer: Herr Prof. Dr.-Ing. habil. Andreas Ahrens
Zweite Gutachterin: Frau Prof. Dr.-Ing. Antje Raab-Düsterhöft

Aufgabenstellung

Ziel dieser Arbeit ist die Darstellung der grundlegenden Unterschiede und die Erörterung der Schwachstellen der Standards WPA2 und WPA3. Der Schwerpunkt bildet hierbei der seit 2018 implementierte Standard WPA3. Es werden insbesondere die Bereiche Aufbau des Standards, eingesetzte Verschlüsselungsmethoden und -verfahren, sowie die Abwärtskompatibilität beleuchtet. Abschließend werden die Erkenntnisse in einer praktischen Verifikation untersucht; Schwerpunkt des praktischen Teils bilden hierbei die Performanceunterschiede im „reinen“ WPA2 bzw. WPA3 Betrieb, sowie die Nutzung bestehender bzw. bereits bekannter Sicherheitslücken im Transition Mode.

Kurzreferat

Im Jahr 2018 wurde resultierend aus einer schwerwiegenden Attacke auf den Standard WPA2, der neue Standard WPA3 veröffentlicht. Mit dieser Arbeit sollen die grundlegenden Unterschiede und die Schwachstellen der beiden Standards erörtert werden; Schwerpunkte bilden hierbei die Ausführungen zum Standard WPA3. Die Erkenntnisse werden darüber hinaus in einer praktischen Verifikation verprobt. Zusammenfassend soll diese Arbeit die Vorzüge des „neuen“ WPA3-Standards hervorheben, die Nutzer bezüglich der Schwachstellen sensibilisieren und zu einer Umrüstung der eingesetzten Netzwerkgeräte animieren. Schwachstellen wurden in beiden WPA Standards identifiziert. Durch die vorhandene Abwärtskompatibilität bietet selbst der neue Standard WPA3 eine schwerwiegende Angriffsfläche. Mit Blick auf die hiervon theoretisch betroffenen Endgeräte ist das Ausmaß dieser Schwachstelle enorm und steht in keinem Verhältnis zu den Vorteilen des Transition Modes. Mit geeigneten Gegenmaßnahmen können die Risiken der Bedrohungen jedoch erheblich reduziert werden.

Abstract

Based on a critical attack on the WPA2 standard, the new WPA3 standard was published in 2018. The aim of this thesis is to discuss the fundamental differences and vulnerabilities of both standards. The main focus of this work lies on the explanations of the WPA3 standard. Furthermore, the results will be tested and evaluated in a practical verification. In summary, this work should highlight the opportunities of the new standard, make the users aware of the possible vulnerabilities and encourage them to adapt the used network devices. Vulnerabilities have been identified in both WPA standards. Due to the existiting downward compatibility, even the WPA3 standard provides a target for attacks. With reference to the theoretically affected devices the extent of this vulnerability is great and bears no relation to the advantage of the transition mode. The risks of the identified threats can be significantly reduced by suitable countermeasures.

Inhalt

1 Einleitung

Der derzeit am meist verbreitetste WLAN-Standard WPA2 steht und fällt mit der Komplexität des genutzten Passworts. Jährlich werden die beliebtesten Passwörter von verschiedenen IT-Sicherheitsfirmen veröffentlicht und zeigen aufs Neue, dass ein Großteil der Nutzer sich nicht die Mühe macht die standardmäßig gesetzten Passwörter zu ändern. Die Frequenz der Passwortänderung ist ebenfalls ein weiterer Kritikpunkt dieser Veröffentlichungen. Ändern sowohl Privat- als auch Firmennutzer das genutzte Passwort über einen längeren Zeitraum nicht, bietet dies Angreifern ausreichend Zeit die abgefangen Hashwerte offline zu entschlüsseln und sich somit Zugang zum gewünschten Netzwerk zu verschaffen.

Resultierend aus der KRACK-Attacke im Jahr 2017 hat die WiFi-Alliance den Standard WPA2 aktualisiert. Angriffspunkt dieser Attacke bildete der 4-Wege Handshake. Der 4-Wege Handshake und die WPA2 Verschlüsselung AES-CCMP sind gem. IEEE 802.11 standardisiert. Diese einzelnen Komponenten wurden zwar unabhängig voneinander geprüft und gelten jeweils als sicher; die kombinierte Anwendung beider Verfahren im WPA2 Standard wurde jedoch nie auf mögliche Sicherheitslücken verifiziert. Die Veröffentlichung der KRACK-Attacke zeigte die Schwachstellen dieser Kombinationsmöglichkeit erstmals auf und setzte die WiFi-Alliance bei der Veröffentlichung des Standards WPA3 unter Zugzwang.

Durch den Standard WPA3 ergeben sich erhebliche Verbesserung hinsichtlich des Authentifizierungsvorgangs mittels SAE sowie der Verschlüsselungsmethoden (ECDH) und der Robustheit der Nachrichtenpakete mittels PMF. Das eingesetzte SAE-Verfahren überträgt beispielsweise den Sitzungsschlüssel nicht mehr über die genutzte WLAN-Verbindung. Es sind damit keinerlei Rückschlüsse auf den eingesetzten Schlüssel mehr möglich. Diese Aktualisierung basiert auf einer Kombination des verwendeten Diffie-Hellmann Verfahrens mit der Elliptischer-Kurven-Kryptografie. Zusätzlich beruht der Standard WPA3 auf der Nutzung von PMF zur Integritätssicherung.

Die Kompatibilität zu nicht WPA3 fähigen Geräten wird durch den Transition Mode sichergestellt. Hierdurch kann in einem BSS sowohl WPA2 als auch WPA3, mit identischer SSID und Passwort, angewandt werden. Durch die notwendige Abwärtskompatibilität für ältere Netzwerkgeräte im Transition Mode hat die WiFi-Alliance jedoch eine neue Angriffsfläche geschaffen, welche selbst mit neueren Geräten und Betriebssystemen weiterhin Bestand hat. Die Öffnung des neuen Standards für nicht WPA3 kompatible Geräte stellt damit eine der großen Schwachpunkte der Aktualisierung dar.

Die Passwortkomplexität und der Änderungsrhythmus des genutzten Passworts sind damit immer noch eine Schwachstelle des Standards WPA2 und des WPA3 Standards im Transition Mode. Diese Schwachstellen werden im WPA3 only Modus zwar nicht gänzlich ausgemerzt; die Nutzung eines alten Passwortes hat für mögliche Angreifer jedoch keinen Mehrwert, da dieses nach einer gewissen Zeit die Gültigkeit verliert und somit wertlos ist. Des Weiteren erfolgten im neuen WLAN-Standard WPA3 diverse Änderungen bzw. Aktualisierungen im Bereich der Verschlüsselung sowie dem Schlüsselaustausch, was den Standard sowohl im privaten als auch im geschäftlichen Bereich zur besseren Wahl macht. Im Bereich des Transition Modes ist der Standard WPA3 jedoch weiterhin durch die Downgrade Attacke angreifbar. Die Ausschöpfung der Vorteile des WPA3 Standards ist im Transition Mode somit nicht vollumfänglich möglich.

Die in der Arbeit herausgearbeiteten Schwachstellen der Standards bzw. Modi sollen praktisch verifiziert werden. Aufgrund nicht kompatibler Hardware wird auf die Darstellung einzelner Schwachstellen (EAP-PWD) im reinen WPA3-Standard verzichtet.

Zusammenfassend soll die Arbeit somit die Vorzüge des „neuen“ WPA3-Standards hervorheben, die Nutzer sensibilisieren und zu einer Umrüstung animieren.

2 Eigenschaften, Gemeinsamkeiten und Unterschiede von WPA2/WPA3

In den folgenden Unterkapiteln werden die theoretischen Grundlagen der Arbeit näher erläutert. Hierbei werden die Standards WPA2 sowie WPA3 im Hinblick auf Eigenschaften, Gemeinsamkeiten sowie den wesentlichen Unterschiede miteinander verglichen.

2.1 WPA2

Der im Jahr 2004 veröffentlichte Standard Wi-Fi Protected Access 2 (WPA2) löste den Standard WPA ab und brachte mit dem genutzten Advanced Encryption Standard (AES) wesentliche Verbesserungen im Bereich der Verschlüsselung mit sich. Zur Authentifizierung wird bei WPA2 der Pre-Shared Key (PSK) genutzt; als Fallback für ältere Geräte kann auch zusätzlich auf das Temporal Key Integration Protocol (TKIP), zurückgegriffen werden. WPA2 setzt auf das Counter-Mode/CBC-MAC Protocol (CCMP), welches zur Sicherstellung der Vertraulichkeit dient. Hierbei sind nur autorisierte Netzwerkbenutzer zum Empfang von Daten ermächtigt. [1, S. 61] Mittels Cipher Block Chaining Message Authentication Code (CBC-MAC) wird die Integrität der Nachrichten gewährleistet. [2]

2.1.1 Authentifizierung

Zur Authentifizierung eines Clients mit einem Access Point (AP) wird, vor allem im WPA2 Personal Modus, die Methode des Pre-Shared Keys (PSK) verwendet. Hierbei wird basierend auf dem bekannten Passwort, welches beim AP für das zur Verfügung gestellte WLAN gesetzt ist, sowie dem veröffentlichtem Service Set Identifier (SSID), ein PSK gebildet. In der Abbildung 1 wird beispielhaft ein PSK für das WLAN „WPA-PSK“ mit dem Passwort bzw. der Passphrase „Password123!“ gebildet. [3]

```
waldemar@Waldemars-MBP Resources % ./airport --psk --password=Password123! --ssid=WPA-PSK
c5819c843fea021fe525a013d217142546d458d435d207b4056c6795c1fd3498
```

Abbildung 1: Bildung PSK (Quelle: eigene Darstellung)

Um eine Verbindung zu einem Access-Point herzustellen, wird ein 4-Wege-Handshake seitens des Clients (Supplicant) und dem Access-Point (AP) durchgeführt.

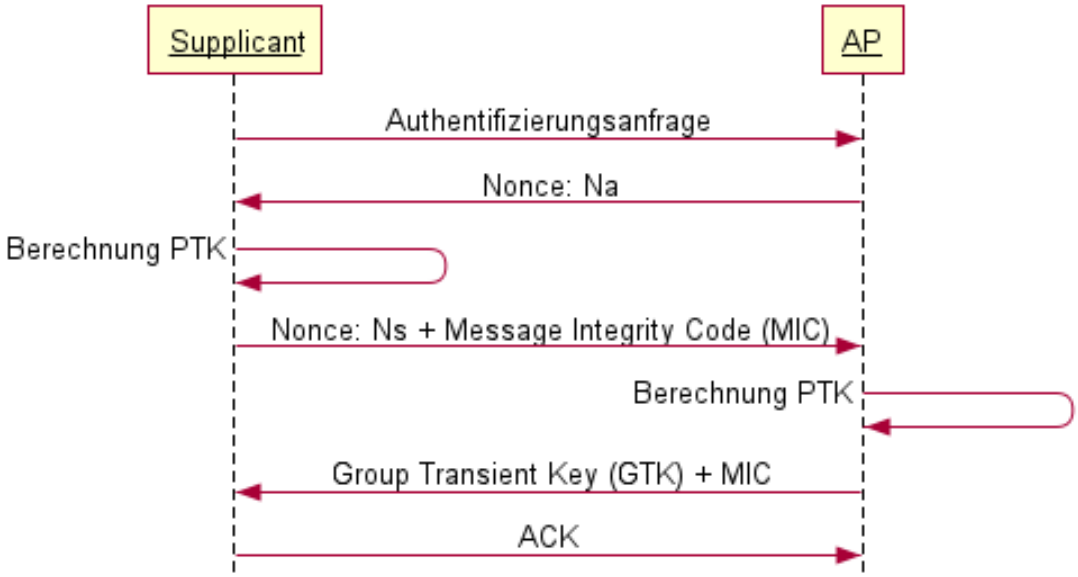

Abbildung 2: 4-Wege Handshake (Quelle: https://bit.ly/3xNSiOe)

Folgende Werte sind hierbei entscheidend:

- Nonce (Number used once) vom Access-Point (Na) - eine Zufallszahl
- Nonce vom Client (Ns) - ebenfalls eine Zufallszahl
- Message Integrity Code (MIC)
- Pairwise Transient Key (PTK)
- Group Transient Key (GTK)
- Nonce group (Ng), eine Zufallszahl

Zunächst sendet der Client eine Authentifizierungsanfrage und erhält im ersten Schritt des 4-Wege-Handshakes die Zufallszahl Na vom AP zurück. Anschließend berechnet der Client, mit Hilfe einer eigenen Zufallszahl Ns, den PTK und übermittelt dem AP im zweiten Schritt seine Zufallszahl Ns und einen

MIC. Dies dient der Sicherung der Authentizität und Integrität. Im weiteren Verlauf berechnet der AP ebenfalls den PTK, welcher zur Verschlüsselung zwischen Client und AP bei der Unicast-Kommunikation verwendet wird. Um eine Multicast-Kommunikation zwischen dem Client und anderen Clients zu gewährleisten muss der GTK, welcher sich aus einem zufälligen Group Master Key (GMK) ableiten lässt, im dritten Schritt vom AP an den Client übermittelt werden. Zum Abschluss des 4-Wege-Handshake Verfahrens, bestätigt der Client im vierten Schritt den Erhalt. Bei Verlassen der Gruppe durch einen Client muss ein Austausch des GTK erfolgen. [4]

Der Wert PTK wird dabei wie folgt berechnet:

PTK = PMK + Na + Ns + SupplicantMacAdresse + APMacAdresse

Der verwendete PMK (Pairwise Master Key) setzt sich aus der SSID sowie dem verwendeten Passwort bzw. der Passphrase zusammen und ist somit identisch mit dem PSK aus Abbildung 1:

```
SSID: WPA-PSK
Passphrase: Password123!
Pairwise Master Key (PMK): c5819c843fea021fe525a013d217142546d458d435d207b4056c6795c1fd3498
```

Abbildung 3: Bildung PMK (Quelle: eigene Darstellung)

Der Wert GTK errechnet sich nach folgendem Schema:

GTK = GMK + Ng + APMacAdresse

Der verwendete GMK wird hierbei nicht zur Authentifizierung verwendet, enthält keine spezifischen Informationen über den AP und ist eine reine Zufallszahl. [5]

Im Bereich des WPA2 Enterprise Modus wird zur Authentifizierung oft auf einen RADIUS (Remote Authentication Dial In User Service) Dienst bzw. Server zurückgegriffen und mittels Extensible Authentication Protocol (EAP) umgesetzt; hierbei werden gem. IEEE 802.1x folgende Funktionen abgedeckt:

- Zugangskontrolle
- Authentifizierung, Autorisierung und Accounting (AAA)
- Bandbreitenzuweisung (QoS)

- Single Sign-on (SSO)

Der Einsatz eines RADIUS Servers wird im Standard IEEE 802.1x nicht vorgeschrieben, in der praktischen Umsetzung der AAA-Überprüfung jedoch oft verwendet. [6]

Grundsätzlich wird während des Authentifizierungsvorgangs ein Client (Supplicant) mittels eines Authentication Server (RADIUS) am Access-Point (Authenticator) zum Netzwerkzugang authentifiziert. Die Authentifizierung am Radius Server selbst kann auf verschiedene Arten ablaufen. Hierbei kann der RADIUS-Server als Verwalter von Benutzer-Zugangsdaten oder als weiteres Bindeglied bzw. Vermittler zu einem LDAP-Server (Lightweight Directory Access Protocol) dienen. Der LDAP-Server verwaltet hierbei sämtliche Benutzer und Netzwerkgeräte. [7]

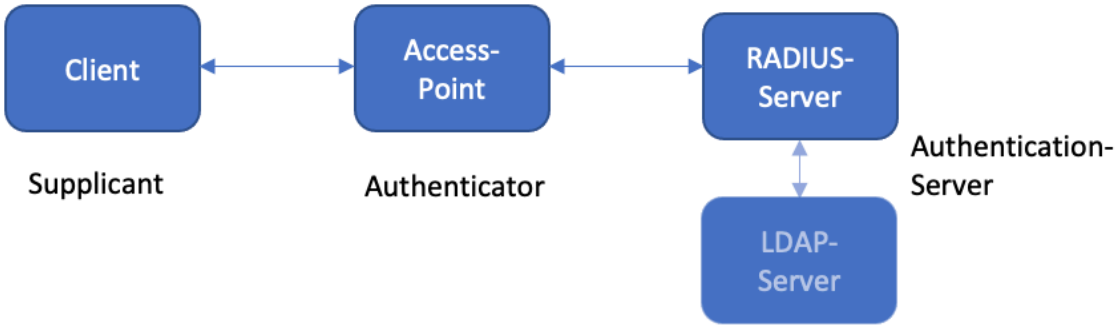

Abbildung 4: RADIUS Authentifizierung (Quelle: eigene Darstellung)

Die in der Abbildung 4 dargestellte Verbindung zwischen dem Client und dem Access-Point findet mittels Extensible Authentication Protocol Over LAN (EAPOL), sowie mittels EAP-Paketen zwischen dem Access-Point und dem RADIUS-Server, statt. [8] Hierbei ermöglicht das Extensible Authentication Protocol (EAP) den Verbindungsaufbau erst nach einer erfolgreichen Authentifizierung. Der Authentifizierungsprozess innerhalb EAP läuft unverschlüsselt ab. Darüber hinaus werden keine dynamischen Schlüssel unterstützt und der Nutzername wird im Klartext übermittelt. Die ausschließliche Nutzung von EAP im WLAN Einsatz führt damit zu einer Erhöhung des Risikos für man-in-the-middle Attacken. Eine Erhöhung der Sicherheit im WLAN, kann durch die Variante der EAP-TLS (Transport Layer Security) mittels einer

gegenseitigen Authentifizierung durch Zertifikate, welche im Client und Authentifizierungsserver gespeichert werden und einem Schlüsselmanagement, gewährleistet werden. Die öffentlichen Schlüssel des Clients und des RADIUS-Servers finden in der Chiffrierung des Sitzungsschlüssels (Session Keys) Verwendung; im Anschluss hieran folgt der beidseitige Austausch, um mittels Sitzungsschlüssel die Nutzerdaten zwischen Access-Point und Client zu verschlüsseln. Da der Session Key durch den öffentlichen Schlüssel chiffriert wurde, kann dieser dementsprechend nur mit dem privaten Schlüssel der Gegenseite, welcher niemals zwischen dem Client und dem Netzwerk ausgetauscht wird, dechiffriert werden. Im Vergleich zum Personal Mode stellt das Betreiben einer Zertifizierungsstelle sowie die Verteilung der Zertifikate an die jeweiligen Endgeräte einen zusätzlichen Aufwand im Enterprise Mode dar. [9, S. 388]

Das symmetrische Verschlüsselungsverfahren Advanced Encryption Standard (AES) findet, mit dem Unterschied in der Schlüssellänge, sowohl bei WPA2 als auch bei WPA3 Verwendung und wird deshalb im Folgenden näher erläutert.

2.1.2 AES Verschlüsselung

Der Advanced Encryption Standard wurde im Jahr 2000 vom National Institute of Standards and Technology (NIST) veröffentlicht. Dabei handelt es sich um ein symmetrisches Verschlüsselungsverfahren, welches von Joan Daemen und Vincent Rijmen entwickelt wurde.

Da es sich um ein symmetrisches Verfahren handelt, wird sowohl zum Ver- als auch zum Entschlüsseln derselbe Schlüssel verwendet. Der AES ist ein Blockchiffre, deren Blockgröße von der Schlüsselgröße abhängig ist. Bei WPA2 beträgt diese 128Bit; bei WPA3-Enterprise ist die Schlüsselgröße mind. 192Bit lang.

Bei dem Verfahren wird zunächst ein Tabellenblock mit vier Zeilen erzeugt und in Abhängigkeit der Schlüssellänge die Anzahl der Spalten gewählt. Pro Zelle werden je acht Bit gesetzt (bei 128Bit vier Spalten, bei 192Bit dementsprechend sechs Spalten).

Der Tabellenblock bei einer Schlüssellänge von 128Bit ist wie folgt ausgestaltet:

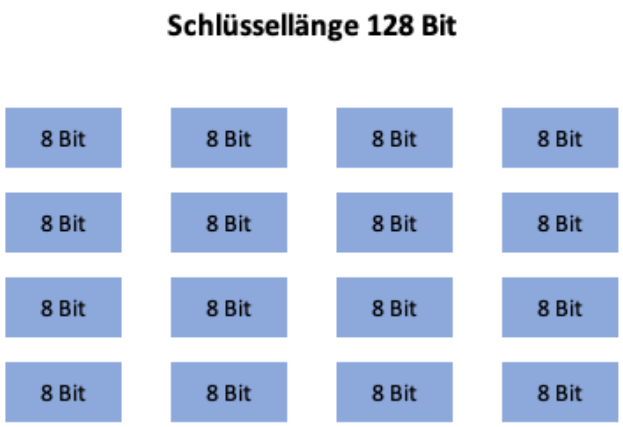

Abbildung 5: AES Tabellenblock 128Bit (Quelle: eigene Darstellung)

Im Anschluss werden mehrere Arten von Transformationen des Tabellenblocks durchgeführt:

- Substitution
- Shift Row
- Mix Column
- Key Addition

Bei der Substitution wird jedes Byte bzw. jede Zelle mit einer Substitutionsbox (S-Box) verschlüsselt. Dabei gibt die S-Box mittels einer Regel vor, wie ein Byte durch einen anderen Wert zu ersetzen ist. In der Abbildung wird jedes Byte durch a i j dargestellt, welche durch die Substitution mit der S-Box als Bytes b i j abgebildet werden.

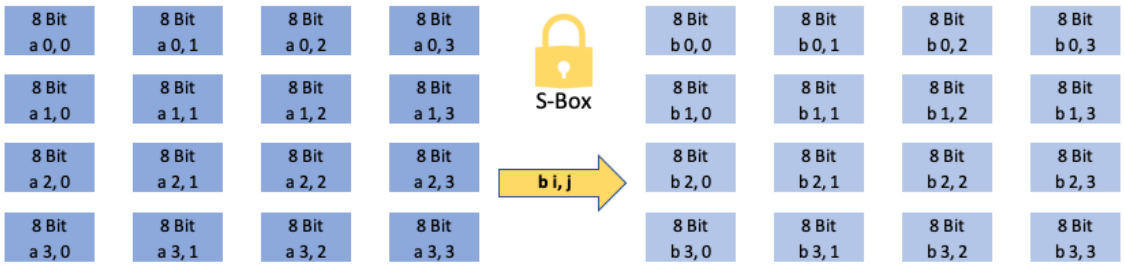

Abbildung 6: AES Substitution (Quelle: eigene Darstellung)

Bei dem Shift Row werden die Zeilen der Tabelle nach links verschoben. Die dabei überlaufenden Zellen werden rechts an die jeweilige Zeile angehängt. Als Beispiel wird in der Abbildung die erste Zeile um null, die zweite um eine, die dritte um zwei, sowie die vierte Zeile um drei Spalten nach links verschoben.

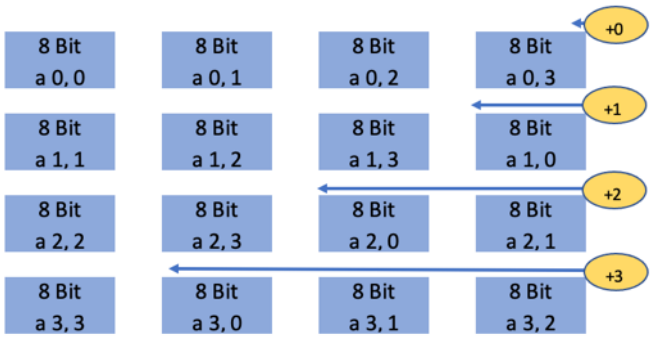

Abbildung 7: AES Shift Row (Quelle: eigene Darstellung)

Beim Mix Column wird jede Spalte mit einer bestimmten Matrix multipliziert. Hierbei werden die Zellen der Tabelle jedoch nicht als Zahlen betrachtet, sondern als Polynome; somit handelt es sich mathematisch um eine Multiplikation in einem Galois Feld. Jede Spalte wird somit als vier-elementiger-Vektor gesehen und mit einer 4 x 4 Matrix (c(x)) multipliziert, was zu einem neuen Vektor führt.

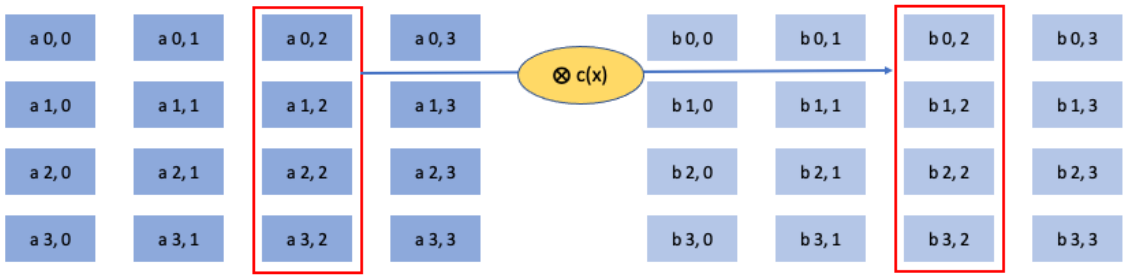

Abbildung 8: AES Mix Column (Quelle: eigene Darstellung)

Bei der Key Addition wird jeder Block bit-weise mit einem Rundenschlüssel, der aus dem Eingabeschlüssel generiert wird, mittels des XOR-Operators verknüpft.

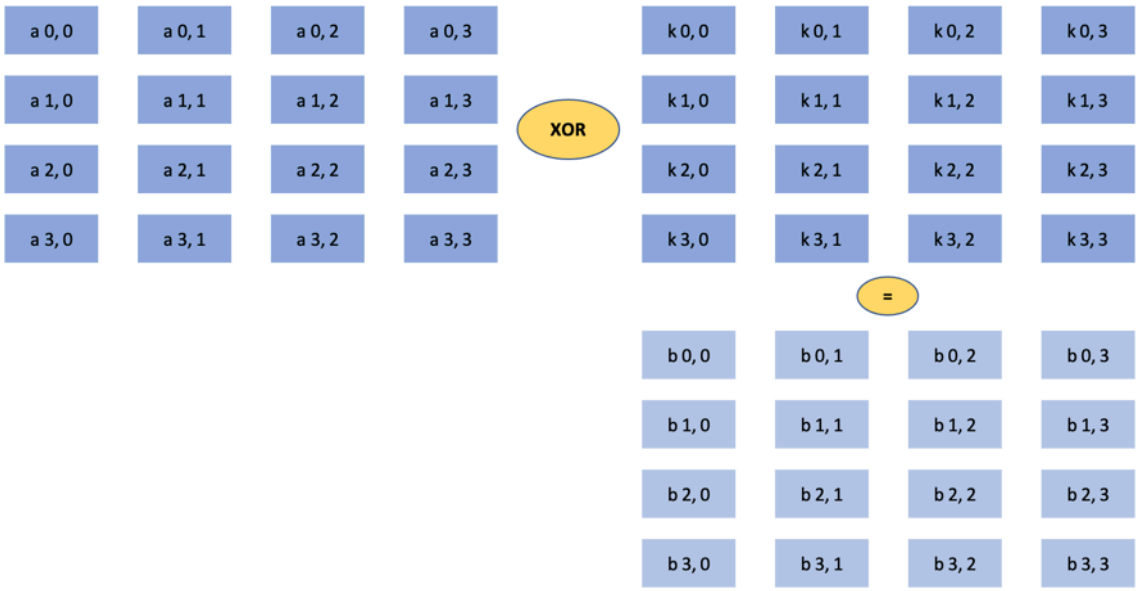

Abbildung 9: AES Key Addition (Quelle: eigene Darstellung)

Es ist gängige Praxis die vier Transformationsschritte mehrmals hintereinander in Runden durchzuführen. Die Transformationsschritte sind umkehrbar.

2.1.3 Schwachstellen WPA2

Wie bei anderen Standards gibt es auch bei WPA2 vielerlei Angriffsmöglichkeiten und somit auch Schwachstellen. Die folgenden Schwachstellen stechen im Hinblick auf WPA2 und dem darauffolgenden Standard WPA3 heraus.

Die Schwachstelle „Hole 196“ wurde auf der DEFCON 2010 vorgestellt und ist nach der Seite 196 des Standard IEEE 802.11i (Revision 2007) benannt. Der vorgenannte Standard schreibt bei einer Unicast-Verbindung zwischen Client und Access Point und unter Verwendung des Pairwise Transient Key (PTK) vor, dass Fälschungen der MAC-Adresse und Manipulation der Daten erkannt werden. Im Gegensatz hierzu werden bei den Broadcast-Verbindungen zwischen dem Access Point und allen Clients, welche hierbei den Group Transient Key (GTK) verwenden, keine Schutzmechanismen im Hinblick auf MAC-Adress- oder Daten-Manipulationen vorgeschrieben. [10]

Diese Schwachstelle bildet die Grundlage für diverse Angriffe, wie dem Address Resolution Protocol (ARP) poisoning mittels man-in-the-middle Attacken, oder dem Einschleusen von Schadcode an autorisierten WLAN-Geräten. Darüber hinaus können auch Störungen mittels denial-of-service (DoS) Attacken und somit das Außergefecht setzen von bestimmten Clients herbeigeführt werden. Im Gegensatz zu dem vorher beschriebenen APR-Poisoning, bei dem der Angreifer mittels gefälschter Angaben versucht hat den APR-Cache des Opfers zu kompromittieren und die Daten über sich weiterzuleiten, muss hier der Angreifer „aus dem Inneren“ heraus agieren, da der GTK erst für authentifizierte Nutzer verfügbar ist. Die Vorteile für den Angreifer ergeben sich aus einem getarnten APR-Poisoning, da der angegriffene Client als Schnittstelle dient und der Angreifer nicht direkt mit dem Netzwerkgerät interagiert und dadurch keine möglichen Alarme bei einem Intrusion Detecion System (IDS) auslösen kann. Zur Vorbeugung und Erkennung von solchen Angriffen können Wireless IDS eingesetzt werden. Grundsätzlich wird diese Art von Angriff jedoch als gering eingestuft, da weder der PTK noch die Verschlüsselung an sich in Gefahr sind. [11, S. 63]

Eine weitaus höhere Gefahr für WPA2 stellt die Key Reinstallation AttaCK (KRACK) dar, welche von Mathy Vanhoef und Frank Piessens im Jahr 2017 auf der Black Hat USA Konferenz vorgestellt wurde. Der Angriff richtet sich gegen den 4-Wege Handshake und ist sowohl im Personal als auch im Enterprise Modus anwendbar. Basis des Angriffs bildet die Aufforderung die bereits genutzten Schlüssel bzw. den derzeit genutzten Schlüssel neu zu installieren. Dies geschieht auf Grundlage von manipulierten und wiederholten Handshake Nachrichten. [12, S. 2] Wie bereits im Kapitel 2.1.1 beschrieben, tauschen der Access-Point und der Client zur Schlüsselerstellung ihre Noncen aus. Laut Standard werden die Noncen auf Null zurückgesetzt, sobald der Austausch des PTK erfolgt ist. Der Austausch ist zwar gesichert und lässt sich grundsätzlich nicht knacken, jedoch kann ein Angreifer in den Austausch eingreifen und den Empfang so stören, dass Teile des Austausches nicht ankommen. Dies erfolgt mittels man-in-the-middle Position, in dem der Angreifer den AP klont und auf einen anderen Kanal umleitet (z.B. ursprünglicher AP auf Kanal 6, geklonter AP auf Kanal 1).

Der Angreifer kann damit, wie in der folgenden Abbildung dargestellt, den vierten Schritt (ACK) vom Client zum Access-Point abfangen und nicht an den AP übermitteln lassen.

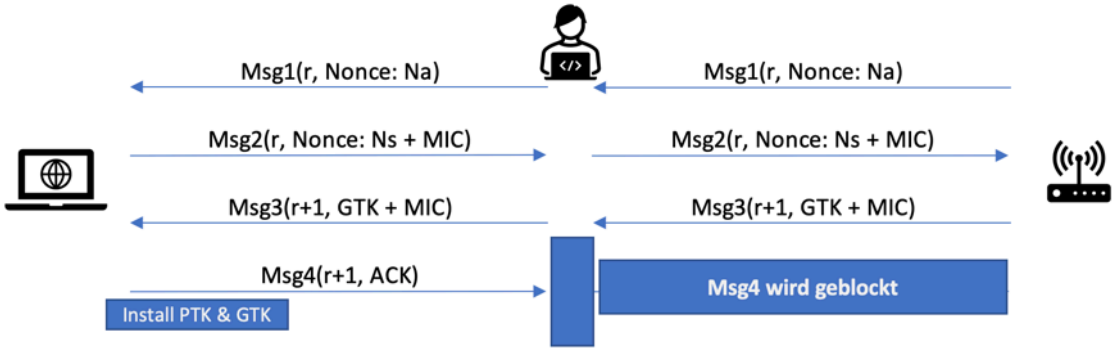

Abbildung 10: Blockierung der Msg4 durch Angreifer (Quelle: eigene Darstellung)

Dies hat zur Folge, dass der Client bereits mit der Übertragung der verschlüsselten Daten beginnt und diese an den AP sendet. Wird innerhalb einer vorgesehenen Zeitspanne kein Acknowledge (ACK) vom Client an den AP übermittelt, sendet der AP die dritte Nachricht erneut. Diese wird vom Angreifer diesmal weitergeleitet und der Client realisiert die vorzeitige Übermittlung der Daten.

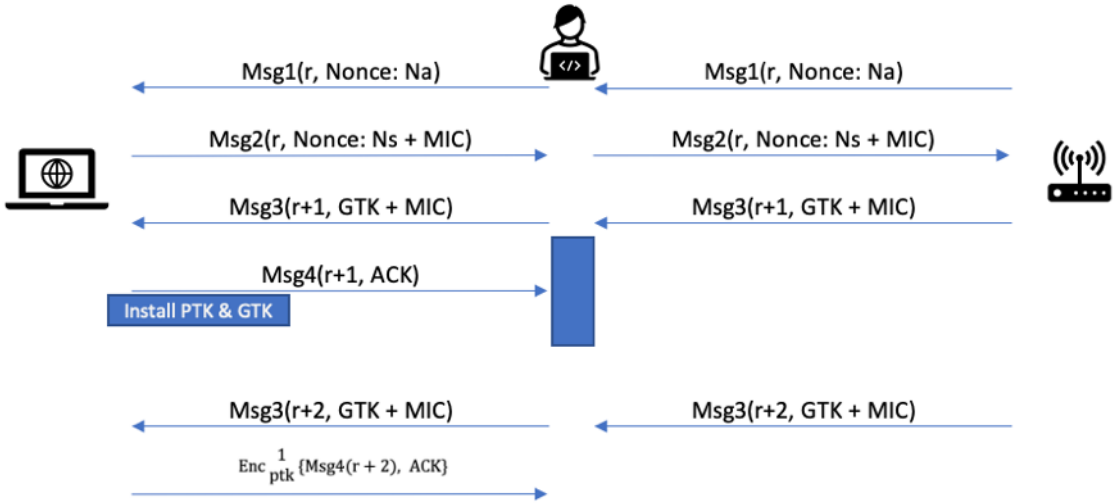

Abbildung 11: Weiterleitung der erneuten Msg3 durch Angreifer (Quelle: eigene Darstellung)

Laut dem Standard IEEE 802.11 ist eine erneute Übermittlung der vierten Nachricht analog zur vorherigen Übermittlung der Nachricht 4 durchzuführen. Es wurde jedoch festgestellt, dass die erneute Übermittlung der vierten Nachricht

bereits verschlüsselt erfolgt, da der Client den PTK bereits installiert hat. [13, S. 8] Nichtsdestotrotz vollzieht der Client die (namensgebende) Key Reinstallation, eine Re-Installierung des (gleichen) PTK; hierbei werden die Client Daten mit der identischen Nonce, wie in den Schritten zuvor, verschlüsselt. [11, S. 69] Dieser Sachverhalt führt zu zwei Problemen. Einerseits wurde der identische Schlüssel bereits für die Verschlüsselung der vierten Nachricht genutzt. Andererseits werden die Nonce-Zähler gem. IEEE Standard nach Neuinstallation wieder auf Null zurückgesetzt. Übermittelt der Client nun eine verschlüsselte Nachricht, wird sowohl der gleiche PTK als auch die gleiche Nonce verwendet.

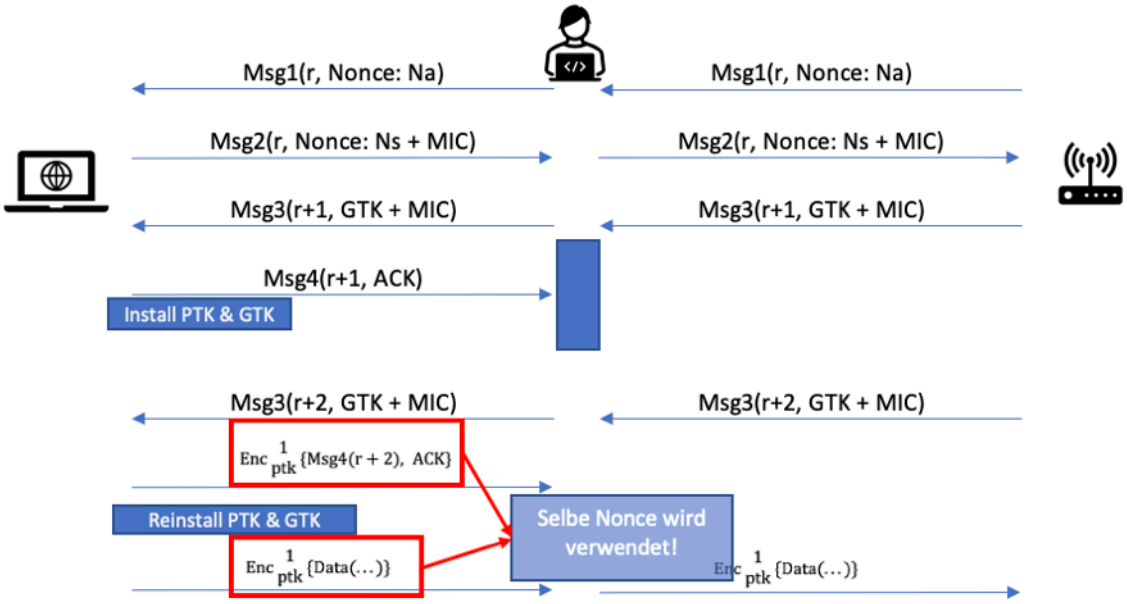

Abbildung 12: Wiederverwendung Nonce (Quelle: eigene Darstellung)

Grundsätzlich gilt bei der im Standard WPA2 verwendeten Verschlüsselung mittels AES-CCMP, dass der Transition Key zusammen mit der Nonce nie mehrmals verwendet werden darf. Eine Missachtung hat zur Folge, dass in beiden Transfers des 4-Wege-Handshake der gleiche Bitstrom zur Verschlüsselung von unterschiedlichen Nachrichten dient. Erhält der Angreifer nun Kenntnis über eine der beiden Nachrichten, kann er mittels XOR-Verknüpfung des bekannten Klartextes und des Chiffretexts den Schlüsselstrom bestimmen.

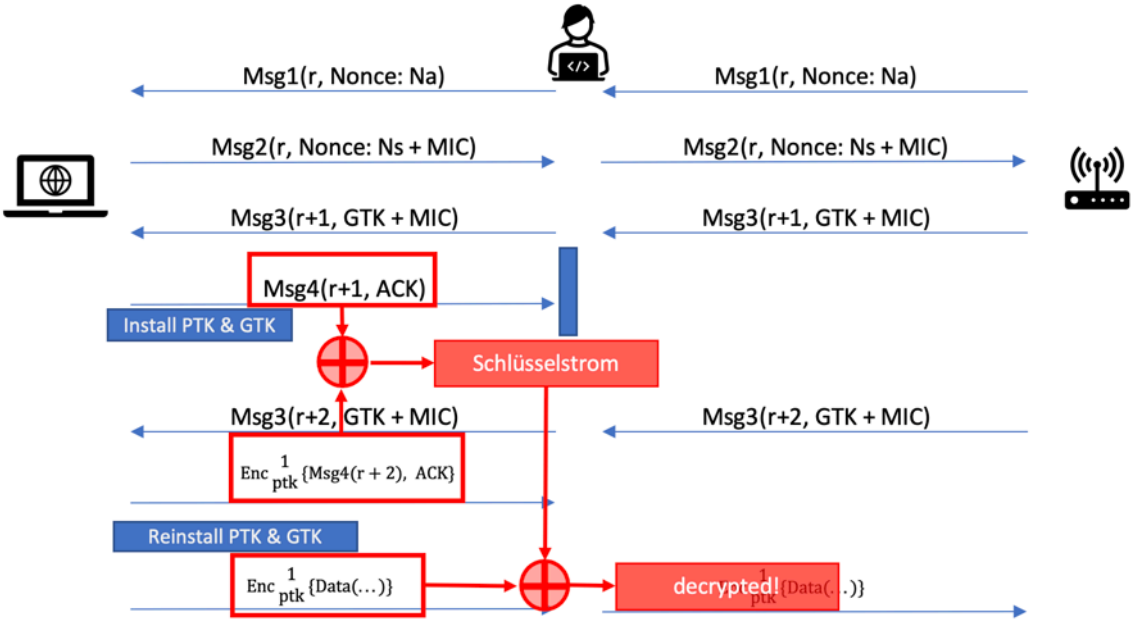

Abbildung 13: Dechiffrierung mittels XOR (Quelle: eigene Darstellung)

Beim KRACK-Angriff wird der Client mittels wiederholter Übermittlung der dritten Nachricht zur Schlüsselerzeugung gezwungen; die Noncen aus Nachricht eins und zwei bleiben jedoch unverändert. Resultierend hieraus ist auch der PTK identisch zum PTK der ersten Übermittlung, da dieser aus dem PMK und den beiden Noncen Na und Ns abgeleitet wird. Der WPA-Standard schreibt vor, dass der Nonce-Zähler bei jeder Key Reinstallation des PTK immer auf den Wert 0 gesetzt wird. Somit sind die Eingangswerte für AES-CCMP identisch und es wird der gleiche Schlüsselstrom erzeugt. [14, S. 108]

Die Auswirkungen der KRACK-Attacke können im praktischen Umfeld sehr vielseitig sein. Windows oder iOS Clients sind grundsätzlich nicht so anfällig wie z.B. Linux oder Android Clients. Das Programm wpa_supplicant (ab Version 2.4), welches für die WLAN-Konfiguration und Verbindung zu einem WLAN gem. WPA-Standard zuständig ist, ist besonders anfällig für eine „all-zero-key“ KRACK Attacke; hierbei wird nicht nur der Nonce-Zähler, sondern der komplette Schlüssel auf Null gesetzt. Die Folge ist, dass sämtlicher Datenverkehr nach der zweiten Nachricht 3 entschlüsselt werden kann.

Bei der „all-zero-key“ KRACK Attacke verhält sich ein Client, in diesem Beispiel ein Android Gerät, in den ersten Schritten des 4-Wege Handshakes zunächst

identisch zu den zuvor genannten Ausführungen. Einziger Unterschied stellt die zusätzliche Komponente des Linux Kernels dar, der hier zwischen dem Gerät und dem Access-Point bzw. dem vorgeschalteten Angreifer einzuordnen ist. Der Kernel ist natürlich physisch im Endgerät verbaut; es handelt sich um eine vereinfachte Darstellung zur besseren Verständlichkeit. Wie bereits in der „normalen“ KRACK Attacke fängt der Angreifer, ohne Wissen des Clients, wieder die vierte Nachricht des 4-Wege Handshakes ab bzw. blockt diese.

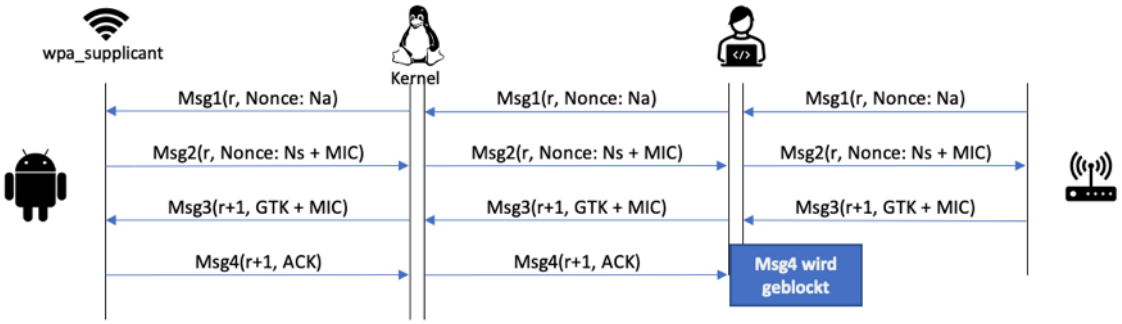

Abbildung 14: Blockierung der Msg4 zero-key (Quelle: eigene Darstellung)

Der ausgehandelte PTK ist bis zu diesem Schritt im Cache des wpa_supplicant gespeichert. Die Konsequenz des vermeintlichen Abschlusses des Handshake Verfahrens ist die Übergabe des PTK vom wpa_supplicant an den Kernel bzw. den Treiber. Dieser übernimmt anschließend die Verschlüsselung der jeweiligen Pakete. Der PTK wird hierauf beim wpa_supplicant bzw. aus dem Speicher gelöscht und beim Kernel bzw. dem Treiber installiert.

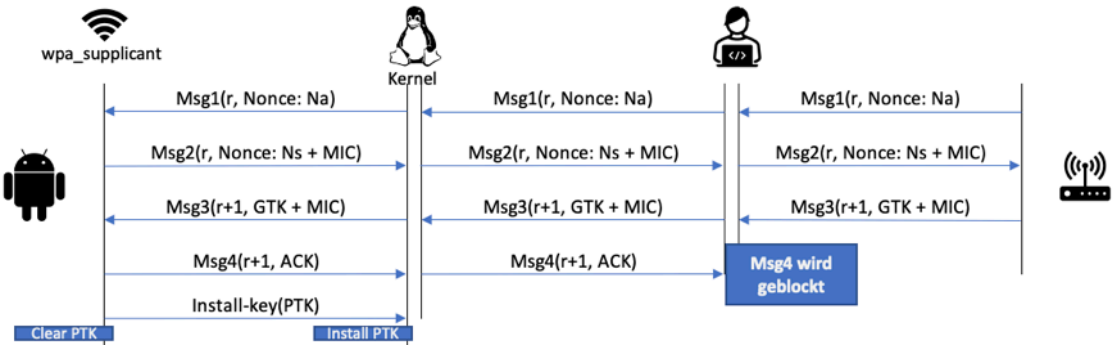

Abbildung 15: Übergabe PTK an den Kernel (Quelle: eigene Darstellung)

Wird nun die Re-Installierung des PTK mittels der KRACK-Attacke durchgeführt, übergibt der wpa_supplicant den identischen Speichersatz, welcher sich zu

diesem Zeitpunkt aus Nullen zusammensetzt, aus dem Speicher an den Kernel. Der „Null-PTK“ wird vom Kernel in den WLAN-Treiber installiert und zur „Verschlüsselung“ verwendet.

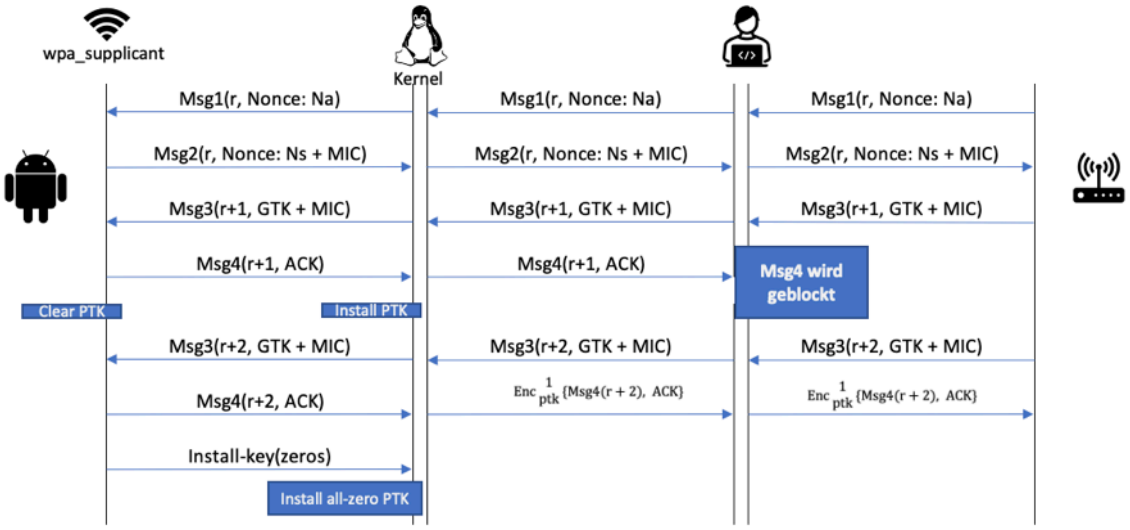

Abbildung 16: Übergabe all-zero PTK an den Kernel (Quelle: eigene Darstellung)

Der aus Nullen bestehende Schlüssel chiffriert die übermittelten Daten; der Schlüssel ist jedoch sehr trivial und kann ohne weiteres entschlüsselt werden. [13, S. 12]

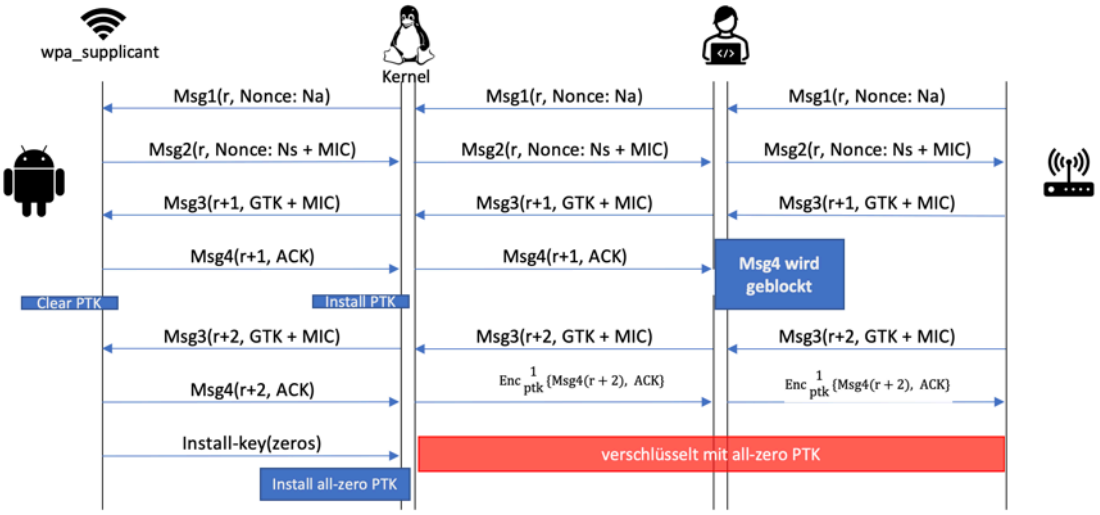

Abbildung 17: Verschlüsselung mit all-zero PTK (Quelle: eigene Darstellung)

Die gravierenden Sicherheitslücken, welche aus der KRACK-Attacke resultierten, hatten die Einführung des neuen Standards WPA3 im Jahr 2018 zur Folge. Auf die Details, wie Aufbau und Verbesserungen zum Vorgänger WPA2, wird in den folgenden Kapiteln eingegangen.

2.2 WPA3

In den folgenden Unterkapiteln wird zunächst der grundsätzliche Aufbau des Standards WPA3 sowie die Funktionsweisen der einzelnen Protokolle und Verfahren näher erläutert.

2.2.1 Voraussetzungen

Um WPA3 nutzen zu können sind verschiedene Voraussetzungen zu erfüllen. Zum einen wird von der WiFi-Alliance eine erfolgreiche Zertifizierung gem. „Wi-Fi CERTIFIED WPA3™“ gefordert. Hauptaugenmerk liegt hierbei auf [15]

- Nutzung der aktuellsten Sicherheitsmethoden
- Nichtverwendung von veralteten Sicherheitsprotokollen (z.B. TKIP)
- Erforderliche Verwendung von Protected Management Frames (PMF)

Die erfolgreiche Zertifizierung gibt die Geräte für die Nutzung von WPA3 frei und ermächtigt den Hersteller zum Führen des Logos auf dem Gerät (oder dessen Verpackung).

Abbildung 18: WiFi Certified Logo (Quelle: https://bit.ly/3hMdrTr)

Darüber hinaus gibt es Voraussetzungen beim genutzten Betriebssystem und der Kompatibilität der (externen) WLAN-Netzwerkkarte. Folgende gängigen Betriebssysteme sind mit deren Version als Mindestanforderung zu sehen [16]:

- Windows 10 ab Version 1903
- MacOS ab Version 10.15 (Catalina)
- iOS bzw. iPadOS ab Version 13
- Android ab Version 10
- Linux ab Kernel Version 3.8 und wpa_supplicant Version 2.9 [17]

Neben den aufgelisteten Vorgaben für WPA3 können bei Benutzung einer „veralteten“ WLAN-Karte Barrieren entstehen. Diese sind Herstellerabhängig und können sowohl am Treiber als auch an der genutzten Hardware liegen.

2.2.2 Dragonfly Protokoll / SAE

Das Dragonfly Protokoll bzw. Simultaneous Authentication of Equals (SAE) verhindert, im Gegensatz zum Pre-Shared Key Verfahren, einen Offline-Wörterbuch Angriff und bietet Perfect Forward Secrecy (PFS) an. Ein kompromittierter Schlüssel stellt hierbei keine Gefahr für vorhergehende Sitzungen dar. SAE nutzt analog zum PSK-Verfahren ebenfalls übereinstimmende Passwörter, welche für jeden Client als Pairwise Master Key (PMK) abgeleitet werden. Trotz der Verwendung eines identischen Passworts für alle Clients, wird für jeden ein eigener PMK generiert bzw. abgeleitet. Im Gegensatz zum PSK-Verfahren, wird der Schlüssel nicht mehr über die WLAN-Verbindung übertragen und lässt somit keine Rückschlüsse auf die jeweiligen PMK zu. [18] Im Rahmen der SEA kommt das Diffie-Hellmann Verfahren mit Elliptischer-Kurven-Kryptografie (Elliptic Curve Cryptography, ECC) zum Einsatz.

Die nachfolgende Darstellung bildet die Schritte gem. SAE-Protokoll inklusive des nachfolgenden 4-Wege Handshake, welcher zur Aushandlung des Session Key dient, ab. Die jeweiligen (vorhergehenden) Schritte sowie die einzelnen Phasen werden im Anschluss näher erläutert.

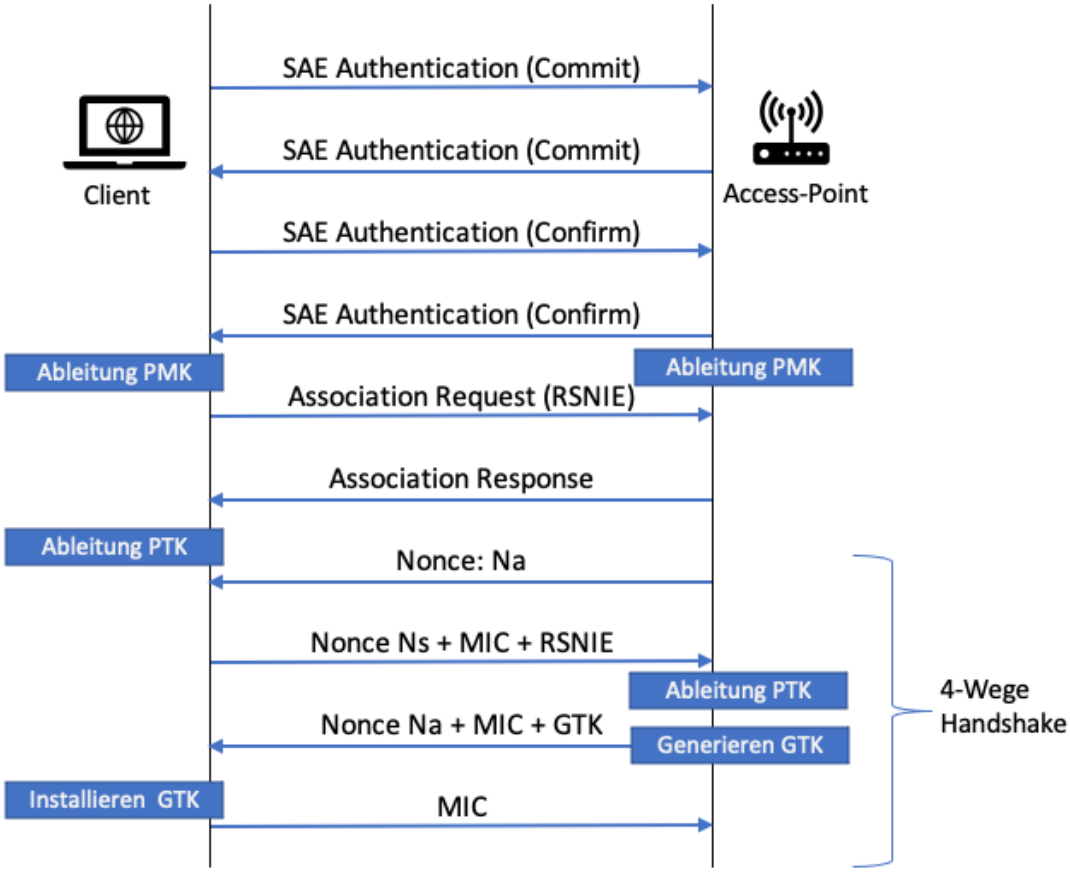

Abbildung 19: Schritte SAE-Protokoll und 4-Wege Handshake (Quelle: eigene Darstellung)

Bevor zwei Teilnehmer, z.B. Client und Access-Point, den Protokoll-Nachrichtenaustausch starten, einigen sich diese auf eine elliptische Kurve. Hierbei handelt es sich um eine ebene Kurve, die durch folgende Gleichung definiert ist [19, S. 30 ff.]:

Voraussetzungen:

$a, b \in K$ *(Feld)*

$4a^3 + 27b^2 \neq 0$

$\mathcal{O}$ als neutrales Element der Gruppe

$$y^2 = x^3 + a_{ec} \cdot x + b_{ec}$$

Beispielhaft wird in folgender Abbildung eine elliptische Kurve mit der Gleichung $y^2 = x^3 + 73$ dargestellt:

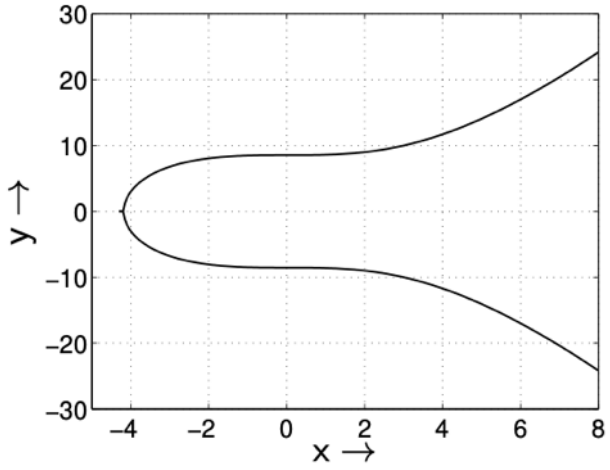

Abbildung 20: Elliptische Kurve (Quelle: Studienbrief Kryptographie II, S. 34)

Im Anschluss werden das Password Element (P) und zwei geheime Zufallswerte (rand r_i und mask m_i) generiert. Dies erfolgt sowohl durch den Client als auch durch den Access-Point. Hierbei gilt:

$1 < rand < r$ und $1 < mask < r$ und $((rand + mask) \bmod r) > 1$

Falls die Summe der zwei Werte rand und mask mod r nicht größer als 1 ist, müssen die Zufallswerte gelöscht und zwei neue Werte generiert werden. Des Weiteren dürfen die bereits genutzten Werte für rand und mask in verschiedenen Protokolldurchläufen nicht noch einmal genutzt werden. [20]

Für die erste Nachricht des SAE-Protokolls muss sowohl der Client als auch der Access-Point folgende Werte berechnen, um diese an den jeweils Anderen übermitteln zu können:

commit-scalar (s_i) = (r_i + m_i) mod r

commit-Element (E_i) = inverse(m_i * P)

Die folgende Darstellung bildet die „Vorphase“ sowie die Commit-Phase, also den Austausch der Authentication-Commit Nachrichten, ab.

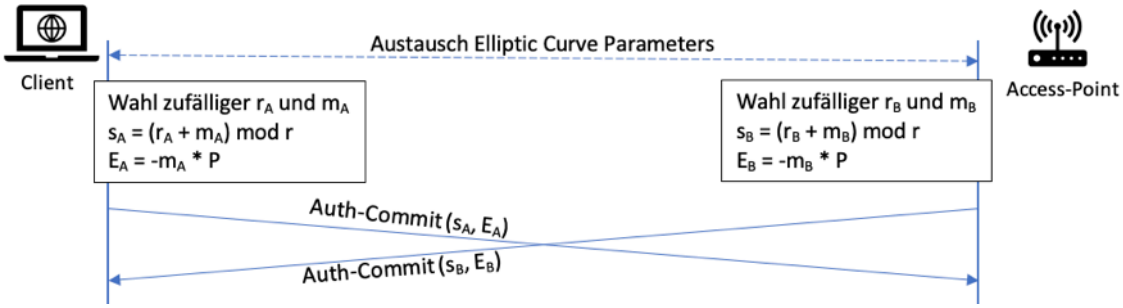

Abbildung 21: Vorphase mit Commit-Phase SAE (Quelle: eigene Darstellung)

Die oben dargestellte Übertragung der jeweiligen Nachrichten kann in Wireshark wie folgt abgebildet werden.

```
  1 0.000000    62:db:79:4a:0d:e4    Synology_ce:6d:36    802.11    128 Authentication, SN=3566, FN=0, Flags=..
  2 0.067451    Synology_ce:6d:36    62:db:79:4a:0d:e4    802.11    128 Authentication, SN=566, FN=0, Flags=...

> Frame 1: 128 bytes on wire (1024 bits), 128 bytes captured (1024 bits)
v IEEE 802.11 Authentication, Flags: ........
    Type/Subtype: Authentication (0x000b)
  > Frame Control Field: 0xb000
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: Synology_ce:6d:36 (00:11:32:ce:6d:36)
    Destination address: Synology_ce:6d:36 (00:11:32:ce:6d:36)
    Transmitter address: 62:db:79:4a:0d:e4 (62:db:79:4a:0d:e4)
    Source address: 62:db:79:4a:0d:e4 (62:db:79:4a:0d:e4)
    BSS Id: Synology_ce:6d:36 (00:11:32:ce:6d:36)
    .... .... .... 0000 = Fragment number: 0
    1101 1110 1110 .... = Sequence number: 3566
v IEEE 802.11 Wireless Management
  v Fixed parameters (6 bytes)
      Authentication Algorithm: Simultaneous Authentication of Equals (SAE) (3)
      Authentication SEQ: 0x0001
      Status code: Successful (0x0000)
      SAE Message Type: Commit (1)
      Group Id: 256-bit random ECP group (19)
      Scalar: 54fa9c4d3eeda9a02936eca6bf4e3a61a58ea79427fc3f78bf0586a4e8430c6a
      Finite Field Element: 63b3a4ac261ef9aad57bbae2630fe6d987f76386ae9954779a51cbcd6102d514f4bc8780…
```

Abbildung 22: Wireshark Authentication 1 (Quelle: eigene Darstellung)

```
  1 0.000000    62:db:79:4a:0d:e4    Synology_ce:6d:36    802.11    128 Authentication, SN=3566, FN=0, Flags=...
  2 0.067451    Synology_ce:6d:36    62:db:79:4a:0d:e4    802.11    128 Authentication, SN=566, FN=0, Flags=....

> Frame 2: 128 bytes on wire (1024 bits), 128 bytes captured (1024 bits)
v IEEE 802.11 Authentication, Flags: ........
    Type/Subtype: Authentication (0x000b)
  > Frame Control Field: 0xb000
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: 62:db:79:4a:0d:e4 (62:db:79:4a:0d:e4)
    Destination address: 62:db:79:4a:0d:e4 (62:db:79:4a:0d:e4)
    Transmitter address: Synology_ce:6d:36 (00:11:32:ce:6d:36)
    Source address: Synology_ce:6d:36 (00:11:32:ce:6d:36)
    BSS Id: Synology_ce:6d:36 (00:11:32:ce:6d:36)
    .... .... .... 0000 = Fragment number: 0
    0010 0011 0110 .... = Sequence number: 566
v IEEE 802.11 Wireless Management
  v Fixed parameters (6 bytes)
      Authentication Algorithm: Simultaneous Authentication of Equals (SAE) (3)
      Authentication SEQ: 0x0001
      Status code: Successful (0x0000)
      SAE Message Type: Commit (1)
      Group Id: 256-bit random ECP group (19)
      Scalar: fe17f81b68beadea59023b024d88bcaa85be5eb9386061b2e28a81adedb1cf0d
      Finite Field Element: e719e6cea3d6adeab0869b03dee11b33c24e56159c7fa92b6e8b3d6ff772b239ef4988c3…
```

Abbildung 23: Wireshark Authentication 2 (Quelle: eigene Darstellung)

Die Werte „Scalar“ und „Finite Field Element“ spiegeln hierbei die jeweiligen s_i sowie E_i Werte aus der vorhergehenden Darstellung wieder. Ergänzend hierzu ist zu erwähnen, dass der Wert für den Authentication Algorithm mit der Nummer

drei gesetzt ist. Die jeweiligen Wertezuweisung können je nach Authentifizierungsmethode variieren:

Tabelle 1: Authentication Algorithm (Quelle: eigene Darstellung)

Algorithm #	Bedeutung
0	Open System
1	Shared Key
2	Fast BSS Transition
3	Simultaneous Authentication of Equals
65535	Vendor Specific Use

In der Aufzeichnung ist der Wert mit der Nummer 3 gesetzt; es wird damit SAE als Authentifizierungsmethode genutzt.

In der anschließenden Confirm-Phase werden die Werte s_i sowie E_i, welche die jeweiligen Parteien übermittelt haben, verifiziert. Hierbei wird zunächst der geheime Punkt K berechnet. Im Anschluss wird die x-Koordinate des Punktes K unter Verwendung einer Hash-Funktion verarbeitet, um den Schlüssel (PMK) κ abzuleiten. Die Handshake Summary wird zusammen mit dem Schlüssel κ mittels HMAC berechnet und bildet den Wert c_i. Dieser wird von beiden Parteien mittels Confirm-Nachrichten ausgetauscht und im Anschluss verifiziert. Schlägt eine der beschriebenen Prüfungen fehl, wird der Handshake abgebrochen.

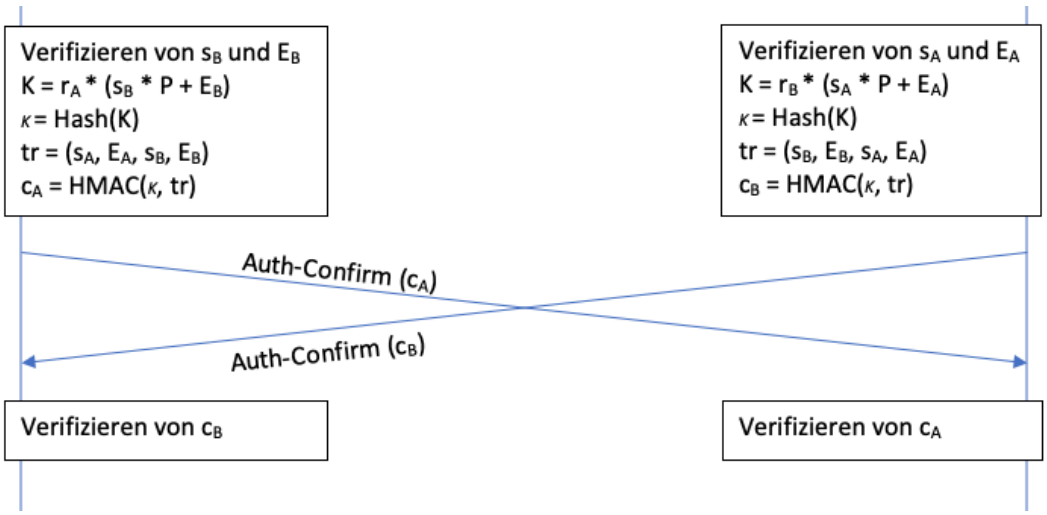

Abbildung 24: Confirm Phase SAE (Quelle: eigene Darstellung)

Die oben dargestellte Übertragung der jeweiligen Nachrichten kann in Wireshark wie folgt nachgestellt werden:

```
  3 0.170988    62:db:79:4a:0d:e4    Synology_ce:6d:36    802.11    64 Authentication, SN=3567, FN=0, Flags=..
  4 0.173290    Synology_ce:6d:36    62:db:79:4a:0d:e4    802.11    64 Authentication, SN=567, FN=0, Flags=...

> Frame 3: 64 bytes on wire (512 bits), 64 bytes captured (512 bits)
v IEEE 802.11 Authentication, Flags: ........
    Type/Subtype: Authentication (0x000b)
  > Frame Control Field: 0xb000
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: Synology_ce:6d:36 (00:11:32:ce:6d:36)
    Destination address: Synology_ce:6d:36 (00:11:32:ce:6d:36)
    Transmitter address: 62:db:79:4a:0d:e4 (62:db:79:4a:0d:e4)
    Source address: 62:db:79:4a:0d:e4 (62:db:79:4a:0d:e4)
    BSS Id: Synology_ce:6d:36 (00:11:32:ce:6d:36)
    .... .... .... 0000 = Fragment number: 0
    1101 1110 1111 .... = Sequence number: 3567
v IEEE 802.11 Wireless Management
  v Fixed parameters (6 bytes)
      Authentication Algorithm: Simultaneous Authentication of Equals (SAE) (3)
      Authentication SEQ: 0x0002
      Status code: Successful (0x0000)
      SAE Message Type: Confirm (2)
      Send-Confirm: 2
      Confirm: 9e694d3831486988ad8b5f205a0fc3e5d1f837fad6347193fd4b44c781e15247
```

Abbildung 25: Wireshark Authentication 3 (Quelle: eigene Darstellung)

```
  3 0.170988    62:db:79:4a:0d:e4    Synology_ce:6d:36    802.11    64 Authentication, SN=3567, FN=0, Flags=..
  4 0.173290    Synology_ce:6d:36    62:db:79:4a:0d:e4    802.11    64 Authentication, SN=567, FN=0, Flags=...

> Frame 4: 64 bytes on wire (512 bits), 64 bytes captured (512 bits)
v IEEE 802.11 Authentication, Flags: ........
    Type/Subtype: Authentication (0x000b)
  > Frame Control Field: 0xb000
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: 62:db:79:4a:0d:e4 (62:db:79:4a:0d:e4)
    Destination address: 62:db:79:4a:0d:e4 (62:db:79:4a:0d:e4)
    Transmitter address: Synology_ce:6d:36 (00:11:32:ce:6d:36)
    Source address: Synology_ce:6d:36 (00:11:32:ce:6d:36)
    BSS Id: Synology_ce:6d:36 (00:11:32:ce:6d:36)
    .... .... .... 0000 = Fragment number: 0
    0010 0011 0111 .... = Sequence number: 567
v IEEE 802.11 Wireless Management
  v Fixed parameters (6 bytes)
      Authentication Algorithm: Simultaneous Authentication of Equals (SAE) (3)
      Authentication SEQ: 0x0002
      Status code: Successful (0x0000)
      SAE Message Type: Confirm (2)
      Send-Confirm: 0
      Confirm: de65436e253c55697b96eb7368d222e36f9c26bd2641676323f1b3b8e8023642
```

Abbildung 26: Wireshark Authentication 4 (Quelle: eigene Darstellung)

Weicht der Wert vom Erwarteten ab, wird auch hier der Handshake abgebrochen und der Confirm-Wert ignoriert. Sollte der Wert der Erwartung entsprechen ist der SAE-Handshake-Vorgang erfolgreich und der ausgehandelte Schlüssel ist κ. [21, S. 2-3]

In den darauffolgenden Association Nachrichten übermittelt der Client mittels Robust Security Network Element (RSNE) Informationen die gewünschte Verschlüsselungsmethode an den Access-Point. Die folgende Abbildung stellt die erste Nachricht vom Client zum Access-Point dar.

```
5 0.180949    62:db:79:4a:0d:e4    Synology_ce:6d:36    802.11    172 Association Request, SN=3568, FN=0, Flags=..
6 0.184621    Synology_ce:6d:36    62:db:79:4a:0d:e4    802.11    200 Association Response, SN=569, FN=0, Flags=..

> Frame 5: 172 bytes on wire (1376 bits), 172 bytes captured (1376 bits)
> IEEE 802.11 Association Request, Flags: ........
v IEEE 802.11 Wireless Management
  > Fixed parameters (4 bytes)
  v Tagged parameters (144 bytes)
    > Tag: SSID parameter set: WPA3_pers
    > Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6, 9, 12, 18, [Mbit/sec]
    > Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
    > Tag: Power Capability Min: 0, Max: 19
    > Tag: Supported Channels
    v Tag: RSN Information
        Tag Number: RSN Information (48)
        Tag length: 38
        RSN Version: 1
      v Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
          Group Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
          Group Cipher Suite type: AES (CCM) (4)
        Pairwise Cipher Suite Count: 1
      v Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
        v Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
            Pairwise Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
            Pairwise Cipher Suite type: AES (CCM) (4)
        Auth Key Management (AKM) Suite Count: 1
      v Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) SAE (SHA256)
        v Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) SAE (SHA256)
            Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
            Auth Key Management (AKM) type: SAE (SHA256) (8)
      v RSN Capabilities: 0x00cc
          .... .... .... ...0 = RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
          .... .... .... ..0. = RSN No Pairwise capabilities: Transmitter can support WEP default key 0 simultaneously with Pairwise key
          .... .... .... 11.. = RSN PTKSA Replay Counter capabilities: 16 replay counters per PTKSA/GTKSA/STAKeySA (0x3)
          .... .... ..00 .... = RSN GTKSA Replay Counter capabilities: 1 replay counter per PTKSA/GTKSA/STAKeySA (0x0)
          .... .... .1.. .... = Management Frame Protection Required: True
          .... .... 1... .... = Management Frame Protection Capable: True
          .... ...0 .... .... = Joint Multi-band RSNA: False
          .... ..0. .... .... = PeerKey Enabled: False
          ..0. .... .... .... = Extended Key ID for Individually Addressed Frames: Not supported
        PMKID Count: 1
      v PMKID List
          PMKID: 53129469a7ac5789823927a90cd6f70c
```

Abbildung 27: Wireshark Association 1 (Quelle: eigene Darstellung)

Der erste markierte Abschnitt bildet die Verschlüsselungsmethode ab. Diese wird mittels der verschiedenen Cipher Suite Types bzw. Selectors unterschieden. In der folgenden Abbildung sind die jeweiligen Selectors gem. IEEE802.11-2016 (table 9.131) dargestellt.

Tabelle 2: Cipher Suite Types (Quelle: eigene Darstellung)

OUI	Suite Type	Bedeutung
00-0F-AC	0	Use Group Cipher Suite
00-0F-AC	1	WEP
00-0F-AC	2	TKIP
00-0F-AC	3	Reserved
00-0F-AC	4	CCMP-128
00-0F-AC	5	WEP-104
00-0F-AC	6	BIP-CMAC-128
00-0F-AC	7	Group address traffic not allowed
00-0F-AC	8	GCMP-128
00-0F-AC	9	GCMP-256
00-0F-AC	10	CCMP-256
00-0F-AC	11	BIP-GMAC-128
00-0F-AC	12	BIP-GMAC-256
00-0F-AC	13	BIP-CMAC-256
00-0F-AC	14-255	Reserved
Other OUI	Any	Vendor Specific

In der Aufzeichnung ist der Organizationally Unique Identifier (OUI) mit 00-0F-AC sowie Type 4 und damit CCMP-128 (Bit) gesetzt.

Auch für die Authentifizierung gibt es verschiedene Typen, welche im IEEE802.11-2016 ebenfalls differenziert werden:

Tabelle 3: Authentification Types (Quelle: eigene Darstellung)

OUI	Suite Type	Authentification Type
00-0F-AC	0	Reserved
00-0F-AC	1	802.1X
00-0F-AC	2	PSK
00-0F-AC	3	FT + 802.1X
00-0F-AC	4	FT + PSK
00-0F-AC	5	802.1X (mit SHA-256)
00-0F-AC	6	PSK (mit SHA-256)
00-0F-AC	7	TDLS
00-0F-AC	8	SAE mit SHA-256
00-0F-AC	9	FT + SAE mit SHA-256
00-0F-AC	10	AP Peer Key Authentication
00-0F-AC	11	802.1X mit Suite B compliant EAP SHA-256
00-0F-AC	12	802.1X mit Suite B compliant EAP SHA-384
00-0F-AC	13	FT + 802.1X mit SHA-384
00-0F-AC	14-255	Reserved
Other OUI	Any	Vendor Specific

In dem Association Request ist der Wert mit OUI 00-0F-AC und dem Typ 8 gesetzt und entspricht damit SAE mit SHA-256.

Des Weiteren ist der Flag bei der Management Frame Protection als erforderlich (required) und fähig (capable) gesetzt. Die Management Frame Protection wird in einem der folgenden Kapiteln näher erläutert.

In der darauffolgenden Association-Response Nachricht bestätigt der Access-Point die Anfrage bei erfolgreichem Abschluss mit dem Status Code „Success“ und bei nicht korrekter Anfrage, beispielsweise falls der Client kein SAE unterstützt und PSK nutzen will, mit dem Status Code „Invalid AKMP“.

```
  5 0.180949    62:db:79:4a:0d:e4                Synology_ce:6d:36   802.11   172 Association Request, SN=3568, FN=0, Flags=..
  6 0.184621    Synology_ce:6d:36                62:db:79:4a:0d:e4   802.11   200 Association Response, SN=569, FN=0, Flags=..

> Frame 6: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits)
v IEEE 802.11 Association Response, Flags: ........
    Type/Subtype: Association Response (0x0001)
  > Frame Control Field: 0x1000
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: 62:db:79:4a:0d:e4 (62:db:79:4a:0d:e4)
    Destination address: 62:db:79:4a:0d:e4 (62:db:79:4a:0d:e4)
    Transmitter address: Synology_ce:6d:36 (00:11:32:ce:6d:36)
    Source address: Synology_ce:6d:36 (00:11:32:ce:6d:36)
    BSS Id: Synology_ce:6d:36 (00:11:32:ce:6d:36)
    .... .... .... 0000 = Fragment number: 0
    0010 0011 1001 .... = Sequence number: 569
v IEEE 802.11 Wireless Management
  v Fixed parameters (6 bytes)
    > Capabilities Information: 0x1431
      Status code: Successful (0x0000)
      ..00 0000 0000 0001 = Association ID: 0x0001
  v Tagged parameters (170 bytes)
    > Tag: Supported Rates 1(B), 2(B), 5.5(B), 6, 9, 11(B), 12, 18, [Mbit/sec]
```

Abbildung 28: Wireshark Association 2 (Quelle: eigene Darstellung)

In dem aufgezeichneten Verbindungsaufbau bestätigt der Access-Point dem Client die erfolgreiche Nutzung von SAE mit SHA-256, welche dieser in der vorhergehenden Nachricht angefragt hat.

Im Anschluss erfolgt, wie bei WPA2, ein 4-Wege Handshake. Einziger Unterschied stellt der genutzte PMK dar, welcher bei WPA3 zuvor durch die SAE generiert und nur zwischen den zwei Parteien (Client und Access-Point) bekannt ist.

Im Verlauf des 4-Wege Handshakes tauschen der Client und Access-Point die jeweiligen Noncen aus. Der aus der SAE abgeleitete PMK wird mittels PMK-Identifier (PMKID) ebenfalls vom Client bzw. Access-Point übermittelt. Zu Beginn übermittelt der Access-Point dem Client in der ersten Nachricht seine Nonce.

```
  7 0.208692    Synology_ce:6d:36    62:db:79:4a:0d:e4    EAPOL    155 Key (Message 1 of 4)
  8 0.210073    62:db:79:4a:0d:e4    Synology_ce:6d:36    EAPOL    173 Key (Message 2 of 4)

Frame 7: 155 bytes on wire (1240 bits), 155 bytes captured (1240 bits)
IEEE 802.11 QoS Data, Flags: ......F.
Logical-Link Control
802.1X Authentication
  Version: 802.1X-2004 (2)
  Type: Key (3)
  Length: 117
  Key Descriptor Type: EAPOL RSN Key (2)
  [Message number: 1]
  Key Information: 0x0088
    .... .... .... .000 = Key Descriptor Version: Unknown (0)
    .... .... .... 1... = Key Type: Pairwise Key
    .... .... ..00 .... = Key Index: 0
    .... .... .0.. .... = Install: Not set
    .... .... 1... .... = Key ACK: Set
    .... ...0 .... .... = Key MIC: Not set
    .... ..0. .... .... = Secure: Not set
    .... .0.. .... .... = Error: Not set
    .... 0... .... .... = Request: Not set
    ...0 .... .... .... = Encrypted Key Data: Not set
    ..0. .... .... .... = SMK Message: Not set
  Key Length: 16
  Replay Counter: 1
  WPA Key Nonce: 076026b0499a00db245409d6f2caeaa9f9f62a24b369d3a221abd887b35ea425
  Key IV: 00000000000000000000000000000000
  WPA Key RSC: 0000000000000000
  WPA Key ID: 0000000000000000
  WPA Key MIC: 00000000000000000000000000000000
  WPA Key Data Length: 22
  WPA Key Data: dd14000fac0453129469a7ac5789823927a90cd6f70c
    Tag: Vendor Specific: Ieee 802.11: RSN PMKID
      Tag Number: Vendor Specific (221)
      Tag length: 20
      OUI: 00:0f:ac (Ieee 802.11)
      Vendor Specific OUI Type: 4
      PMKID: 53129469a7ac5789823927a90cd6f70c
```

Abbildung 29: Wireshark 4-Wege Handshake 1 (Quelle: eigene Darstellung)

In der darauffolgenden zweiten Nachricht übermittelt der Client sowohl die Nonce als auch die MIC mit den (nochmaligen) RSN Informationen. Hierbei ist gut zu erkennen, dass in der RSN Information wieder die Flags bei der Management Frame Protection sowohl bei capable als auch required gesetzt sind.

```
 7 0.208692    Synology_ce:6d:36    62:db:79:4a:0d:e4    EAPOL    155 Key (Message 1 of 4)
 8 0.210073    62:db:79:4a:0d:e4    Synology_ce:6d:36    EAPOL    173 Key (Message 2 of 4)

Key Information: 0x0108
    .... .... .... .000 = Key Descriptor Version: Unknown (0)
    .... .... .... 1... = Key Type: Pairwise Key
    .... .... ..00 .... = Key Index: 0
    .... .... .0.. .... = Install: Not set
    .... .... 0... .... = Key ACK: Not set
    .... ...1 .... .... = Key MIC: Set
    .... ..0. .... .... = Secure: Not set
    .... .0.. .... .... = Error: Not set
    .... 0... .... .... = Request: Not set
    ...0 .... .... .... = Encrypted Key Data: Not set
    ..0. .... .... .... = SMK Message: Not set
  Key Length: 16
  Replay Counter: 1
  WPA Key Nonce: 9f1a4a49fed764dddd5f399ba0cb9432cc43e03312c66e364ea0ec7746850550
  Key IV: 00000000000000000000000000000000
  WPA Key RSC: 0000000000000000
  WPA Key ID: 0000000000000000
  WPA Key MIC: e8a1e9020ca641c38ae55625492ec94b
  WPA Key Data Length: 40
  WPA Key Data: 30260100000fac040100000fac040100000fac08cc00010053129469a7ac5789823927a9…
    Tag: RSN Information
      Tag Number: RSN Information (48)
      Tag length: 38
      RSN Version: 1
      Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
      Pairwise Cipher Suite Count: 1
      Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
        Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
          Pairwise Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
          Pairwise Cipher Suite type: AES (CCM) (4)
      Auth Key Management (AKM) Suite Count: 1
      Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) SAE (SHA256)
        Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) SAE (SHA256)
          Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
          Auth Key Management (AKM) type: SAE (SHA256) (8)
      RSN Capabilities: 0x00cc
        .... .... .... ...0 = RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
        .... .... .... ..0. = RSN No Pairwise capabilities: Transmitter can support WEP default key 0 simultaneously with Pairwise key
        .... .... .... 11.. = RSN PTKSA Replay Counter capabilities: 16 replay counters per PTKSA/GTKSA/STAKeySA (0x3)
        .... .... ..00 .... = RSN GTKSA Replay Counter capabilities: 1 replay counter per PTKSA/GTKSA/STAKeySA (0x0)
        .... .... .1.. .... = Management Frame Protection Required: True
        .... .... 1... .... = Management Frame Protection Capable: True
        .... ...0 .... .... = Joint Multi-band RSNA: False
        .... ..0. .... .... = PeerKey Enabled: False
        ..0. .... .... .... = Extended Key ID for Individually Addressed Frames: Not supported
      PMKID Count: 1
      PMKID List
        PMKID: 53129469a7ac5789823927a90cd6f70c
```

Abbildung 30: Wireshark 4-Wege Handshake 2 (Quelle: eigene Darstellung)

Im dritten Schritt übermittelt der Access-Point, zusammen mit der MIC, wiederum seine Nonce.

```
  9 0.222773   Synology_ce:6d:36   62:db:79:4a:0d:e4   EAPOL   221 Key (Message 3 of 4)
 10 0.224213   62:db:79:4a:0d:e4   Synology_ce:6d:36   EAPOL   133 Key (Message 4 of 4)

> Frame 9: 221 bytes on wire (1768 bits), 221 bytes captured (1768 bits)
> IEEE 802.11 QoS Data, Flags: ......F.
> Logical-Link Control
v 802.1X Authentication
    Version: 802.1X-2004 (2)
    Type: Key (3)
    Length: 183
    Key Descriptor Type: EAPOL RSN Key (2)
    [Message number: 3]
  v Key Information: 0x13c8
      .... .... .... .000 = Key Descriptor Version: Unknown (0)
      .... .... .... 1... = Key Type: Pairwise Key
      .... .... ..00 .... = Key Index: 0
      .... .... .1.. .... = Install: Set
      .... .... 1... .... = Key ACK: Set
      .... ...1 .... .... = Key MIC: Set
      .... ..1. .... .... = Secure: Set
      .... .0.. .... .... = Error: Not set
      .... 0... .... .... = Request: Not set
      ...1 .... .... .... = Encrypted Key Data: Set
      ..0. .... .... .... = SMK Message: Not set
    Key Length: 16
    Replay Counter: 2
    WPA Key Nonce: 076026b0499a00db245409d6f2caeaa9f9f62a24b369d3a221abd887b35ea425
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 99f0170fccf9a96a9edc42025454ed39
    WPA Key Data Length: 88
    WPA Key Data: 15ab2dc7266cb7e4d1832546214c9858c256939eb0674a5e906418af04c8087dfeb67002…
```

Abbildung 31: Wireshark 4-Wege Handshake 3 (Quelle: eigene Darstellung)

Im letzten Schritt des 4-Wege Handshakes übermittelt der Client die MIC und bestätigt die Übertragung. Der Handshake ist damit abgeschlossen.

```
  9 0.222773   Synology_ce:6d:36   62:db:79:4a:0d:e4   EAPOL   221 Key (Message 3 of 4)
 10 0.224213   62:db:79:4a:0d:e4   Synology_ce:6d:36   EAPOL   133 Key (Message 4 of 4)

Frame 10: 133 bytes on wire (1064 bits), 133 bytes captured (1064 bits)
IEEE 802.11 QoS Data, Flags: .......T
Logical-Link Control
802.1X Authentication
  Version: 802.1X-2004 (2)
  Type: Key (3)
  Length: 95
  Key Descriptor Type: EAPOL RSN Key (2)
  [Message number: 4]
v Key Information: 0x0308
    .... .... .... .000 = Key Descriptor Version: Unknown (0)
    .... .... .... 1... = Key Type: Pairwise Key
    .... .... ..00 .... = Key Index: 0
    .... .... .0.. .... = Install: Not set
    .... .... 0... .... = Key ACK: Not set
    .... ...1 .... .... = Key MIC: Set
    .... ..1. .... .... = Secure: Set
    .... .0.. .... .... = Error: Not set
    .... 0... .... .... = Request: Not set
    ...0 .... .... .... = Encrypted Key Data: Not set
    ..0. .... .... .... = SMK Message: Not set
  Key Length: 16
  Replay Counter: 2
  WPA Key Nonce: 0000000000000000000000000000000000000000000000000000000000000000
  Key IV: 00000000000000000000000000000000
  WPA Key RSC: 0000000000000000
  WPA Key ID: 0000000000000000
  WPA Key MIC: 7902b6f8edef19a706e802f7907e9dab
  WPA Key Data Length: 0
```

Abbildung 32: Wireshark 4-Wege Handshake 4 (Quelle: eigene Darstellung)

Durch den Einsatz des bereits im SAE abgeleiteten Schlüssels, welcher im anschließenden 4-Wege Handshake verwendet wird um den WPA-Schlüssel (PTK) abzuleiten [14, S. 110], ist diese Methodik trotz analogem Ablauf des 4-Wege Handshakes zu WPA 2, sowohl gegen eine Offline-Wörterbuchattacke

(Handshake Capture und PMKID Hash) als auch gegen eine Deauthentifizierungsattacke, zur Störung des Netzverkehrs, geschützt. [22, S. 17-19]

2.2.3 Perfect Forward Secrecy

Grundsätzlich dient das Perfect Forward Secrecy (PFS) als Schutzmechanismus vor einem nachträglichen Entschlüsseln von Daten bzw. der Ableitung des nachfolgenden Sitzungsschlüssels. Die Umsetzung erfolgt, wie im Kapitel 2.2.2 beschrieben, durch den Diffie-Hellmann Schlüsselaustausch. [23] Da der Client bei jeder (Neu-)Anmeldung am Access-Point den Handshake (sowohl SAE als auch 4-Way) durchlaufen muss, wird auch der Session Key bzw. PTK immer wieder neu abgeleitet. Auf Grund dessen wird dies unter Benutzung von WPA3 als PFS und nicht „nur“ als Forward Secrecy (FS) eingestuft. [24]

2.2.4 Management Frame Protection

Die Management Frame Protection war bereits im Standard WPA2 verfügbar bzw. mit dem Standard IEEE 802.11w abgedeckt; der Schutzmechanismus wurde damit nicht im Rahmen von WPA3 eingeführt. Im Gegensatz zur verbindlichen Nutzung unter WPA3 ist der Einsatz von PMF unter WPA2 jedoch optional seitens Client und Access-Point möglich.

Grundsätzlich schützen die Protected Management Frames (PMF) die Steuerinformationen, welche zwischen Client und Access-Point z.B. beim An- oder Abmelden verwendet werden. Wird diese Funktion nicht genutzt, kann ein Angreifer den Client dazu zwingen die Verbindung mittels Deauthentication-Attacke zu unterbrechen und sich so erfolgreich als man-in-the-middle zwischen Client und Access-Point positionieren. [25] Sämtliche neuen WLAN-Geräte, welche die Zertifizierung gem. WiFi-Alliance durchlaufen, müssen die Funktion PMF unterstützen. [26]

2.3 Zusammenfassung

In der folgenden Tabelle sind die wesentlichen Unterschiede der beiden WPA Standards aus theoretischer Sicht aufgeführt. Durch die Nutzung des Dragonfly Protokolls gestaltet sich der Schlüsselaustausch bei WPA3 wesentlich sicherer und ist somit robuster gegen Angriffe. Eine Verbesserung bringt auch die erforderliche Nutzung der Option PMF, welche Störungen innerhalb des Netzwerks reduziert und so ebenfalls zu einem stabileren Netzwerk beiträgt.

Tabelle 4: Gegenüberstellung WPA2 WPA3 (Quelle: eigene Darstellung)

	WPA2	WPA3
Verschlüsselung	AES 128 CCMP	AES 128 CCMP AES 256 GCMP
Schlüsselaustausch	Pre-shared-Key (PSK) 4-Wege Handshake	Simultaneous Authentication of Equals (SAE) Elliptic Curve Diffie-Hellman (ECDH)
Authentifizierung (Enterprise)	802.1X mit SHA-256	802.1X mit SHA-256 HMAC-SHA384
Protected Management Frame (PMF)	Optional	Erforderlich

3 Verschiedene Modi von WPA3

Wie bereits beim Standard WPA2 gibt es auch bei WPA3 verschiedene Modi. Für den normalen bzw. heimischen Betrieb wird meistens WPA3-Personal verwendet. Im geschäftlichen Bereich wird, wie bereits bei WPA2, durch ein zusätzliches Element (RADIUS Server) die Authentifizierung gem. IEEE 802.1x Standard durchgeführt.

In den folgenden Unterkapiteln wird auf die jeweiligen Eigenschaften der Modi eingegangen.

3.1 WPA3-Personal Mode

Die WiFi-Alliance stellt an den Personal Mode (only) bestimmte Vorgaben, welche sich auf die AKM suite selectors beziehen. Die Vorgaben sind den RSNE Informationen zu entnehmen. Folgende Kriterien sind hierbei als Mindestanforderung definiert: [27, S. 8]

- Ein AP muss mindestens 00-0F-AC:8 in seinem Basic Service Set (BSS) gesetzt haben
    - SAE mit SHA-256
- Ein Client muss ebenfalls 00-0F-AC:8 in seiner Assoziation wählen
    - SAE mit SHA-256
- AP darf 00-0F-AC:2 sowie 00-0F-AC:6 nicht aktiviert haben
    - PSK
    - PSK (mit SHA-256)
- Client darf 00-0F-AC:2 und 00-0F-AC:6 in seiner Anfrage nicht erlauben
    - PSK
    - PSK (mit SHA-256)

Des Weiteren müssen folgende Werte bei der Management Frame Protection (PMF Verfahren) wie folgt gesetzt sein:

- AP sowohl bei capable als auch required: 1
- Client sowohl bei capable als auch required: 1

Grundsätzlich gilt, dass sowohl WEP als auch TKIP nicht erlaubt sind.

3.2 WPA3-Enterprise Mode

Wie bereits im Personal Mode sind auch im Enterprise Mode (only) formale Vorgaben seitens der WiFi-Alliance vorhanden. Demnach sind folgende Kriterien als Mindestanforderung gesetzt: [27, S. 9-10]

- Ein AP muss mindestens 00-0F-AC:5 in seinem Basic Service Set (BSS) gesetzt haben
    - IEEE 802.1X mit SHA-256
- Ein Client muss ebenfalls 00-0F-AC:5 in seiner Assoziation wählen
    - IEEE 802.1X mit SHA-256
- AP darf 00-0F-AC:1 nicht aktiviert haben
    - IEEE 802.1X (mit SHA-1)
- Client darf 00-0F-AC:1 in seiner Anfrage nicht erlauben
    - IEEE 802.1X (mit SHA-1)

Des Weiteren müssen folgende Werte bei der Management Frame Protection (PMF Verfahren) wie folgt gesetzt sein:

- AP sowohl bei capable als auch required: 1
- Client sowohl bei capable als auch required: 1

Wie bereits im Personal Mode gilt auch hier, dass WEP und TKIP nicht erlaubt sind.

Ein Einsatz des WPA3-Enterprise 192-bit Modus erhöht einige der oben genannten Anforderungen dementsprechend. Demnach gilt bei WPA3-Enterprise 192-bit:

- PMF muss sowohl bei AP als auch beim Client mit capable und required mit Wert 1 gesetzt sein
- Zulässige EAP Cipher Suites sind:
    - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
    - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
    - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

Wie bereits im Personal Mode, können sämtlich genannten Parameter bei einer Aufzeichnung des Datenverkehrs visualisiert werden. Im folgenden Beispiel wurde WPA3-Enterprise im 192-bit Modus unter Einsatz eines Radius Server (FreeRADIUS) mit EAP-TLS umgesetzt. Die Parameter für PMF sind u.a. im Beacon bzw. Broadcast Frame des Access-Points sowie im Association Request vom Client ersichtlich.

```
1 0.000000   Synology_ce:6d:36   Broadcast   802.11   320 Beacon frame, SN=3542, FN=0, Flags=........, BI=100, SSID=WPA3_ent

Tag: RSN Information
    Tag Number: RSN Information (48)
    Tag length: 26
    RSN Version: 1
  v Group Cipher Suite: 00:0f:ac (Ieee 802.11) GCMP (256)
      Group Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
      Group Cipher Suite type: GCMP (256) (9)
    Pairwise Cipher Suite Count: 1
  v Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) GCMP (256)
    v Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) GCMP (256)
        Pairwise Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
        Pairwise Cipher Suite type: GCMP (256) (9)
    Auth Key Management (AKM) Suite Count: 1
  v Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) WPA (SHA384-SuiteB)
    v Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) WPA (SHA384-SuiteB)
        Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
        Auth Key Management (AKM) type: WPA (SHA384-SuiteB) (12)
  v RSN Capabilities: 0x00cc
      .... .... .... ...0 = RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
      .... .... .... ..0. = RSN No Pairwise capabilities: Transmitter can support WEP default key 0 simultaneously with Pairwise key
      .... .... .... 11.. = RSN PTKSA Replay Counter capabilities: 16 replay counters per PTKSA/GTKSA/STAKeySA (0x3)
      .... .... ..00 .... = RSN GTKSA Replay Counter capabilities: 1 replay counter per PTKSA/GTKSA/STAKeySA (0x0)
      .... .... .1.. .... = Management Frame Protection Required: True
      .... .... 1... .... = Management Frame Protection Capable: True
      .... ...0 .... .... = Joint Multi-band RSNA: False
      .... ..0. .... .... = PeerKey Enabled: False
      ..0. .... .... .... = Extended Key ID for Individually Addressed Frames: Not supported
    PMKID Count: 0
    PMKID List
  v Group Management Cipher Suite: 00:0f:ac (Ieee 802.11) BIP (GMAC-256)
      Group Management Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
      Group Management Cipher Suite type: BIP (GMAC-256) (12)
```

Abbildung 33: Wireshark Broadcast Frame AP (Quelle: eigene Darstellung)

```
94 29.639168   6a:f7:6e:62:68:c0     Synology_ce:6d:36    802.11    169 Association Request, SN=2207, FN=0, Flags=........, SSID=WPA3_ent

Tag: RSN Information
    Tag Number: RSN Information (48)
    Tag length: 26
    RSN Version: 1
    Group Cipher Suite: 00:0f:ac (Ieee 802.11) GCMP (256)
        Group Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
        Group Cipher Suite type: GCMP (256) (9)
    Pairwise Cipher Suite Count: 1
    Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) GCMP (256)
        Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) GCMP (256)
            Pairwise Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
            Pairwise Cipher Suite type: GCMP (256) (9)
    Auth Key Management (AKM) Suite Count: 1
    Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) WPA (SHA384-SuiteB)
        Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) WPA (SHA384-SuiteB)
            Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
            Auth Key Management (AKM) type: WPA (SHA384-SuiteB) (12)
    RSN Capabilities: 0x00cc
        .... .... .... ...0 = RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
        .... .... .... ..0. = RSN No Pairwise capabilities: Transmitter can support WEP default key 0 simultaneously with Pairwise key
        .... .... .... 11.. = RSN PTKSA Replay Counter capabilities: 16 replay counters per PTKSA/GTKSA/STAKeySA (0x3)
        .... .... ..00 .... = RSN GTKSA Replay Counter capabilities: 1 replay counter per PTKSA/GTKSA/STAKeySA (0x0)
        .... .... .1.. .... = Management Frame Protection Required: True
        .... .... 1... .... = Management Frame Protection Capable: True
        .... ...0 .... .... = Joint Multi-band RSNA: False
        .... ..0. .... .... = PeerKey Enabled: False
        ..0. .... .... .... = Extended Key ID for Individually Addressed Frames: Not supported
    PMKID Count: 0
    PMKID List
    Group Management Cipher Suite: 00:0f:ac (Ieee 802.11) BIP (GMAC-256)
        Group Management Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
        Group Management Cipher Suite type: BIP (GMAC-256) (12)
```

Abbildung 34: Wireshark Association Request Client (Quelle: eigene Darstellung)

Ein Rückschluss auf die eingesetzte Cipher Suite, in diesem Fall TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, ist u.a. über die übermittelten TLS-Nachrichten möglich.

```
145 31.496202                Synology_ce:6d:36                6a:f7:6e:62:68:c0    TLSv1.2

Frame 145: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
IEEE 802.11 QoS Data, Flags: ....R.F.
Logical-Link Control
802.1X Authentication
Extensible Authentication Protocol
  Code: Request (1)
  Id: 5
  Length: 22
  Type: TLS EAP (EAP-TLS) (13)
> EAP-TLS Flags: 0x80
  EAP-TLS Length: 2000
> [3 EAP-TLS Fragments (2000 bytes): #137(994), #140(994), #145(12)]
v Transport Layer Security
  v TLSv1.2 Record Layer: Handshake Protocol: Server Hello
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 61
    v Handshake Protocol: Server Hello
        Handshake Type: Server Hello (2)
        Length: 57
        Version: TLS 1.2 (0x0303)
      > Random: 9767892e223138e1fd15edf20d07711efb8ed70bfb224f260db4f2e477d4bf1f
        Session ID Length: 0
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
        Compression Method: null (0)
        Extensions Length: 17
      > Extension: renegotiation_info (len=1)
      > Extension: ec_point_formats (len=4)
      > Extension: extended_master_secret (len=0)
  > TLSv1.2 Record Layer: Handshake Protocol: Certificate
  v TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 365
    v Handshake Protocol: Server Key Exchange
        Handshake Type: Server Key Exchange (12)
        Length: 361
      v EC Diffie-Hellman Server Params
          Curve Type: named_curve (0x03)
          Named Curve: secp384r1 (0x0018)
          Pubkey Length: 97
```

Abbildung 35: Wireshark TLS Frame (Quelle: eigene Darstellung)

Wie bereits erwähnt ist für WPA3-Enterprise ebenfalls ein Transition Mode verfügbar. Auf nähere Details wird im weiteren Verlauf dieser Arbeit eingegangen.

3.3 Vergleich Personal und Enterprise Mode

In der folgenden Tabelle sind die wesentlichen Unterschiede der beiden Modi bei WPA3 dargestellt. Besonders erwähnenswert ist hierbei, zum einen die stärkere Verschlüsselung im Enterprise Mode und zum anderen die erforderliche Nutzung eines zusätzlichen Elements, welche zur AAA-Überprüfung (RADIUS) gem. IEEE 802.1X durchgeführt werden muss.

Tabelle 5: Gegenüberstellung WPA3 Personal Enterprise Mode (Quelle: eigene Darstellung)

	Personal	Enterprise
Verschlüsselung	AES 128 CCMP	AES 256 GCMP
Schlüsselaustausch	Simultaneous Authentication of Equals (SAE) Elliptic Curve Diffie-Hellman (ECDH)	
Authentifizierung (Enterprise)	-	802.1X mit SHA-256 HMAC-SHA384
Protected Management Frame (PMF)	Erforderlich	Erforderlich

3.4 Gegenüberstellung WPA2 / WPA3

Die Gegenüberstellung der beiden Standards wird analog zu den bisherigen Ausführungen jeweils in Personal und Enterprise Mode untergliedert.

3.4.1 Personal Mode

In der folgenden Tabelle ist die Gegenüberstellung für den Personal Mode dargestellt.

Tabelle 6: Gegenüberstellung WPA2 WPA3 Personal Mode (Quelle: eigene Darstellung)

	WPA2	WPA3
Verschlüsselung	AES 128 CCMP	AES 128 CCMP
Authentifizierung	Pre-shared-Key (PSK)	Simultaneous Authentication of Equals (SAE)
Protected Management Frame (PMF)	Optional	Erforderlich
Angriffsmöglichkeiten/ Bedrohungen	- Offline Wörterbuch Attacken - De-Authentifizierungs Attacken - KRACK - ARP Spoofing	- Dragonblood
Vorteile	- Kompatibilität noch sehr hoch	- Je nach Konfiguration sicherer als WPA2 - Perfect Forward Secrecy - Schlüssel wird nicht über WLAN übertragen
Nachteile	- Bei schwachen/trivialen Passwörtern und seltener Änderung angreifbar	- Kompatibilität - Wenige Geräte im privaten Sektor verfügbar

Durch den Einsatz von SAE wird den Angreifern die Grundlage von diversen Attacken, bspw. Offline-Wörterbuch- oder KRACK-Attacke, entzogen. Je nach Umfeld könnte die Kompatibilität der Geräte jedoch als Ausschlussfaktor für den Einsatz von WPA3 dienen. Dem kann durch die Anwendung von verschiedenen BSS (je mit WPA2 und WPA3 only) entgegengewirkt werden. [28, S. 22]

3.4.2 Enterprise Mode

Aufbauend auf der Gegenüberstellung im Personal Mode folgen nun Ausführungen zum Enterprise Mode.

Tabelle 7: Gegenüberstellung WPA2 WPA3 Enterprise Mode (Quelle: eigene Darstellung)

	WPA2	WPA3
Verschlüsselung	AES 128 CCMP	AES 256 GCMP
Schlüsselaustausch	PSK	ECDH
Authentifizierung	802.1X mit SHA-256	802.1X mit SHA-256 HMAC-SHA384
Protected Management Frame (PMF)	Optional	Erforderlich

Durch den Schlüsselaustausch bzw. das Ableiten mit dem ECDH ist WPA3 auch im kommerziellen Sektor wesentlich stärker gegen Angriffe, wie z.B. Offline-Wörterbuch Attacken, abgesichert als WPA2. Analog zum Personal Mode ist auch im Enterprise Mode PMF als zwingend erforderliches Muss-Kriterium gesetzt. Die Authentifizierungsmethode ist abhängig von der Konfiguration des IEEE 802.1x AAA- bzw. Radius-Servers und muss sowohl unabhängig von der Konfiguration des WPA3 Access-Points als auch in Kombination betrachtet werden.

4 Abwärtskompatibilität im Transition Mode

Die Kompatibilität zu Geräten, welche noch kein WPA3 unterstützen, wird durch den Transition Mode gewährleistet. Hierbei werden die beiden Standards WPA2, via PSK, und WPA3, via SAE, gleichzeitig vom Netzwerkgerät zur Verfügung gestellt. Im Detail wird dies seitens der WiFi Alliance wie folgt spezifiziert: [29, S. 6]

- Grund für den Einsatz des WPA3-Personal Transition Mode ist die nicht vorhandene Abwärtskompatibilität vom WLAN-Protokoll SAE.
- WPA3-Personal Transition Mode unterstützt sowohl WPA2 als auch WPA3 Geräte, jeweils im Personal Mode, welche im selben Basic Service Set (BSS) und der gleichen SSID ein identisches Passwort verwenden.
- WPA3-Enterprise Transition Mode unterstützt ebenfalls sowohl WPA2 als auch WPA3 Geräte; dabei ist zu beachten, dass PMF als capable und die Flags bei MFPC auf 1 bzw. bei MFPR auf 0 (standardmäßig) gesetzt werden.

Seitens der WiFi Alliance besteht die ausdrückliche Empfehlung einer strikten Trennung der Bereiche WPA2 und WPA3. Des Weiteren sollten unterschiedliche SSID’s sowie verschiedene Passwörter (im Personal Mode) genutzt werden.

4.1 Personal Transition Mode

Wie bereits bei den Modi Personal und Enterprise, legt die WiFi-Alliance auch für die jeweiligen Transition Modi (Personal und Enterprise) diverse Vorgaben fest. Diese sind für den Personal Transition Mode: [27, S. 8]

- Bei den AKM suite selectors müssen 00-0F-AC:2 (PSK) und 00-0F-AC:8 (SAE mit SHA-256) seitens des Access-Points aktiviert sein und vom Client bei der Assoziation gewählt werden (je nach Support der Hardware/Software).
- Die Einstellungen für die Management Frame Protection müssen sowohl beim AP als auch beim Client mit capable 1 und required 0 gesetzt sein,

um die Kompatibilität von (älteren) Geräten sicherzustellen.

- Des Weiteren darf der Access-Point WPA mit der Version 1, WEP sowie TKIP nicht im selben BSS zulassen, in dem WPA3-Personal betrieben wird.
- Bei einer Verbindung zum AP, welcher sowohl SAE als auch PSK verwendet, sollte der Client vorzugsweise SAE nutzen.
- Bei der Verwendung der AKM suite selector mit den Feldern 00-0F-AC:2 (PSK) sowie 00-0F-AC:6 (PSK mit SHA-256) sollte der WPA3-Personal Transition Mode beim AP standardmäßig aktiviert werden.
- Wenn die PMF zwischen Client und AP in den vorhergehenden Schritten nicht verhandelt wurden, muss der AP die Assoziation für SAE abweisen; stellt der Client wiederum die PMF in den vorherigen Schritten zur Verfügung, muss SAE anstatt PSK verwendet werden.

Diese Vorgaben können innerhalb des Nachrichtenaustausches zwischen Client und AP nachvollzogen werden. Eine Visualisierung erfolgte mit dem Programm Wireshark. In der folgenden Abbildung ist zu erkennen, dass der AP im Transition Mode sowohl PSK als auch SAE als Authentifizierungsmethode anbietet.

```
1 0.000000   Synology_ce:6d:36   Broadcast   802.11   325 Beacon frame, SN=2189, FN=0, Flags=........, BI=100, SSID=WPA3_transition

Tag: RSN Information
  Tag Number: RSN Information (48)
  Tag length: 24
  RSN Version: 1
  Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
    Group Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
    Group Cipher Suite type: AES (CCM) (4)
  Pairwise Cipher Suite Count: 1
  Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
    Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
      Pairwise Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
      Pairwise Cipher Suite type: AES (CCM) (4)
  Auth Key Management (AKM) Suite Count: 2
  Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) PSK 00:0f:ac (Ieee 802.11) SAE (SHA256)
    Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) PSK
      Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
      Auth Key Management (AKM) type: PSK (2)
    Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) SAE (SHA256)
      Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
      Auth Key Management (AKM) type: SAE (SHA256) (8)
  RSN Capabilities: 0x008c
    .... .... .... ...0 = RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
    .... .... .... ..0. = RSN No Pairwise capabilities: Transmitter can support WEP default key 0 simultaneously with Pairwise key
    .... .... .... 11.. = RSN PTKSA Replay Counter capabilities: 16 replay counters per PTKSA/GTKSA/STAKeySA (0x3)
    .... .... ..00 .... = RSN GTKSA Replay Counter capabilities: 1 replay counter per PTKSA/GTKSA/STAKeySA (0x0)
    .... .... .0.. .... = Management Frame Protection Required: False
    .... .... 1... .... = Management Frame Protection Capable: True
    .... ...0 .... .... = Joint Multi-band RSNA: False
    .... ..0. .... .... = PeerKey Enabled: False
    ..0. .... .... .... = Extended Key ID for Individually Addressed Frames: Not supported
```

Abbildung 36: Wireshark Broadcast Frame WPA3 Transition Mode (Quelle: eigene Darstellung)

In der nächsten Abbildung unterstützt der Client kein WPA3 und greift somit sowohl auf den PSK als auch auf die „Nichtaktivierung“ der PMF zurück.

```
18 13.549899   MurataMa_08:4f:73     Synology…  802.11    173 Association Request, SN=170, FN=0, Flags=........, SSID=WPA3_transition

Tag: RSN Information
    Tag Number: RSN Information (48)
    Tag length: 20
    RSN Version: 1
    Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
        Group Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
        Group Cipher Suite type: AES (CCM) (4)
    Pairwise Cipher Suite Count: 1
    Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
        Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
            Pairwise Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
            Pairwise Cipher Suite type: AES (CCM) (4)
    Auth Key Management (AKM) Suite Count: 1
    Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) PSK
        Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) PSK
            Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
            Auth Key Management (AKM) type: PSK (2)
    RSN Capabilities: 0x0000
        .... .... .... ...0 = RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
        .... .... .... ..0. = RSN No Pairwise capabilities: Transmitter can support WEP default key 0 simultaneously with Pairwise key
        .... .... .... 00.. = RSN PTKSA Replay Counter capabilities: 1 replay counter per PTKSA/GTKSA/STAKeySA (0x0)
        .... .... ..00 .... = RSN GTKSA Replay Counter capabilities: 1 replay counter per PTKSA/GTKSA/STAKeySA (0x0)
        .... .... .0.. .... = Management Frame Protection Required: False
        .... .... 0... .... = Management Frame Protection Capable: False
        .... ...0 .... .... = Joint Multi-band RSNA: False
        .... ..0. .... .... = PeerKey Enabled: False
        ..0. .... .... .... = Extended Key ID for Individually Addressed Frames: Not supported
```

Abbildung 37: Wireshark Client ohne WPA3 Support (Quelle: eigene Darstellung)

In der nachfolgenden Abbildung ist ein anderer Client (seitens Software und/oder Hardware) WPA3-fähig; dementsprechend wird SAE und PMF genutzt.

```
25 42.865356   56:4b:f0:0a:96:6d     Synology…  802.11    188 Association Request, SN=557, FN=0, Flags=....R..., SSID=WPA3_transition

Tag: RSN Information
    Tag Number: RSN Information (48)
    Tag length: 38
    RSN Version: 1
    Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
        Group Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
        Group Cipher Suite type: AES (CCM) (4)
    Pairwise Cipher Suite Count: 1
    Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
        Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
            Pairwise Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
            Pairwise Cipher Suite type: AES (CCM) (4)
    Auth Key Management (AKM) Suite Count: 1
    Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) SAE (SHA256)
        Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) SAE (SHA256)
            Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
            Auth Key Management (AKM) type: SAE (SHA256) (8)
    RSN Capabilities: 0x00cc
        .... .... .... ...0 = RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
        .... .... .... ..0. = RSN No Pairwise capabilities: Transmitter can support WEP default key 0 simultaneously with Pairwise key
        .... .... .... 11.. = RSN PTKSA Replay Counter capabilities: 16 replay counters per PTKSA/GTKSA/STAKeySA (0x3)
        .... .... ..00 .... = RSN GTKSA Replay Counter capabilities: 1 replay counter per PTKSA/GTKSA/STAKeySA (0x0)
        .... .... .1.. .... = Management Frame Protection Required: True
        .... .... 1... .... = Management Frame Protection Capable: True
        .... ...0 .... .... = Joint Multi-band RSNA: False
        .... ..0. .... .... = PeerKey Enabled: False
        ..0. .... .... .... = Extended Key ID for Individually Addressed Frames: Not supported
```

Abbildung 38: Wireshark Client mit WPA3 Support (Quelle: eigene Darstellung)

4.2 Enterprise Transition Mode

Im Enterprise Transition Mode sind darüber hinaus folgende Kriterien vorgeschrieben: [27, S. 9]

- Wie bereits im Personal Mode, darf der Access-Point WPA mit der Version 1, WEP sowie TKIP nicht im selben BSS zulassen, in dem WPA3-Enterprise betrieben wird
- Bei den AKM suite selectors sollten mindestens 00-0F-AC:1 (IEEE 802.X mit SHA-1) sowie 00-0F-AC:5 (IEEE 802.X mit SHA-256) aktiviert sein
- Die beiden Selectoren (00-0F-AC:1, 00-0F-AC:5) müssen vom Client ebenfalls in den AKM suite selectors gewählt sein

Auch hier könnte mit dem Programm Wireshark der Nachrichtenfluss zwischen Client und Access-Point, sowohl unter Benutzung PSK als auch SAE, visualisiert werden. Da die für die Arbeit genutzte Hardware für den Access-Point die Funktion WPA3-Enterprise Transition Mode leider nicht unterstützt, wird jedoch auf eine Darstellung verzichtet.

5 Schwachstellenanalyse WPA und praktische Verifikation

5.1 Schwachstellenanalyse Transition Mode

Wie bereits bei der WPA2 Schwachstelle KRACK war Mathy Vanhoef bei der im Jahr 2019 festgestellten Schwachstelle im Dragonfly Protokoll ebenfalls beteiligt. Zusammen mit Eyal Ronen hat dieser ein Whitepaper mit Details sowie Programmen veröffentlicht, um Geräte auf die von ihnen entdeckte Schwachstelle zu testen.

Eine der identifizierten Attacken basiert auf dem Downgrade der genutzten Authentifizierungsmethode. Wie bereits in den Vorkapiteln näher erläutert, stellt ein Access-Point im Transition Mode sowohl SAE als auch PSK als Authentifizierungsmethode zur Verfügung, um die Kompatibilität zu älteren Geräten zu gewährleisten. Für beide Methoden wird ein identisches Passwort verwendet. Der Angreifer beabsichtigt den Client zu der PSK-Methode zu leiten, um im Anschluss aus dem abgefangenen Nachrichtenverlauf des 4-Wege Handshakes mit einer Offline-Wörterbuchattacke das genutzte Passwort zu knacken. Der Angriff basiert hierbei nicht auf einer man-in-the-middle-Position, sondern resultiert aus dem Duplizieren des tatsächlichen Access-Points durch einen fraudulenten AP. Hierfür ist lediglich der Service Set Identifier (SSID) des originären AP notwendig. Die AP unterscheiden sich lediglich im unterstützten Authentifizierungsverfahren; der „betrügerische“ AP unterstützt mit Absicht nur PSK und gibt diesen als einzige Möglichkeit dem Client vor. Der Client verbindet sich mit dem fraudulenten AP; realisiert jedoch spätestens bei der zweiten Nachricht des PSK 4-Wege Handshakes, dass dieser nicht korrekt ist, da die RSNE Informationen mit den bisherigen Informationen nicht übereinstimmen und bricht die Verbindung ab. Die Angreifer können zu diesem Zeitpunkt jedoch bereits mit den ersten beiden Nachrichten des 4-Wege Handshake eine Offline-Wörterbuch Attacke starten.

Je nach Konfiguration des Access-Points im Transition Mode kann das Passwort trivial gesetzt sein, da mit WPA3 Personal (only) die Passwortlänge bzw. das

Passwort selbst für den Sitzungsschlüssel nicht relevant ist. Diese Auffassung wird seitens der WiFi-Alliance ebenfalls über verschiedene Kanäle vermittelt. [28, S. 16] Nähere Details zum durchgeführten Downgrade Angriff sind im praktischen Teil enthalten.

5.2 Praktische Verifikation

Für den praktischen Aufbau wurden folgende Komponenten verwendet:

Tabelle 8: Komponenten für praktische Verifikation (Quelle: eigene Darstellung)

Access-Point/Router	FRITZ!Box SL WLAN für den Bereich WPA2 Personal Mode; Firmware-Version 09.04.34
	Synology MR2200ac für die Bereiche WPA3 Personal, Enterprise sowie Transition Mode; SRM (Firmware) 1.2.4-8081
Clients/Betriebssysteme	Apple iPhone 12 mit iOS 14.6
	Samsung Galaxy S4 mit Android 5.0.1
	Raspberry Pi 3b mit Kali Linux
RADIUS Server	Ubuntu 20.04.2 LTS
	FreeRADIUS 3.0.20
	OpenSSL 1.1.1.f

Für die Durchführung der praktischen Verifikation der Sicherheitslücken, müssen die jeweiligen Geräte und die Software installiert und konfiguriert werden. Beim FRITZ!Box Router SL WLAN war dies nicht weiter umständlich. Zu Beginn wurde das Gerät auf Werkseinstellungen zurückgesetzt und im Anschluss als Standalone-Gerät (ohne Anschluss an das Internet oder andere Netzwerkgeräte) konfiguriert.

Beim Synology Router wurde je nach Modi eine andere Konfiguration vorgenommen. Grundsätzlich wurde das Gerät an ein bestehendes Netzwerk angeschlossen, um eine Weiterleitung zum RADIUS Server, welcher als virtuelle Maschine (VM) auf einem weiteren Gerät gehostet wurde, zu gewährleisten. Da die genutzten Netzwerkgeräte bzw. deren WLAN-Schnittstellen nur das 2.4GHz-Netz unterstützen, wurde dies bei der Konfiguration ebenfalls berücksichtigt.

Die Konfigurationen der beiden Router sind Anhang 1 zu entnehmen.

Die dargestellte IP-Adresse des Synology Routers im Enterprise Mode entspricht der des genutzten RADIUS-Servers. Die Konfiguration des RADIUS-Servers besteht zunächst aus einer Basisinstallation von Ubuntu 20.04.2 LTS (Liveserver). Diese wurde „headless“ und somit ohne das grafische Interface (GUI) durchgeführt. Im Anschluss erfolgte die Installation des FreeRADIUS (mit dem LDAP-Modul zur Nutzerverwaltung) sowie des OpenSSL Servers, welche für den späteren Einsatz von EAP-TLS benötigt werden. Um eine Authentifizierung mittels EAP-TLS durchführen zu können, wurden sowohl ein Server-Zertifikat als auch die jeweiligen Nutzer-Zertifikate mittels OpenSSL erstellt. Bei der Konfiguration des FreeRADIUS-Servers wurden die jeweiligen Server Zertifikatsdateien eingebunden und die Client Zertifikate an das Client Gerät (iPhone) verteilt und installiert. Die Zertifikate sind beim genutzten Gerät in einem Profil gespeichert:

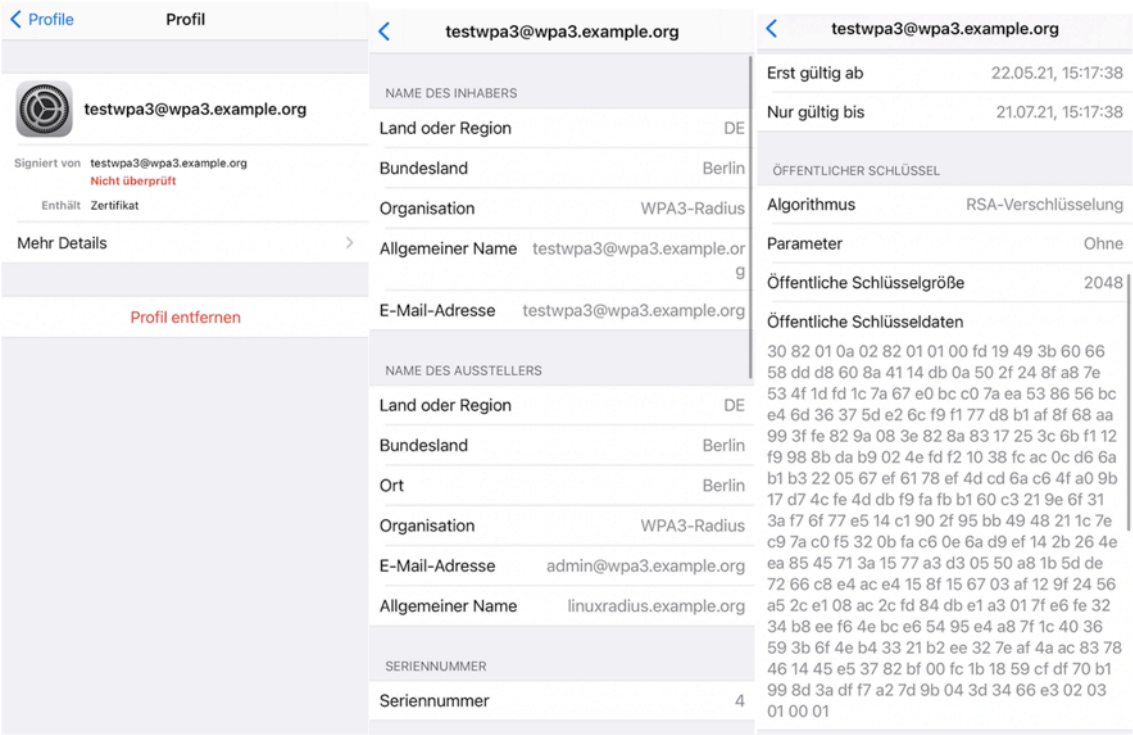

Abbildung 39: Einbindung der Zertifikatsdatei am Client (Quelle: eigene Darstellungen)

Die Konfiguration des EAP-Moduls von FreeRADIUS setzt voraus, dass sich ausschließlich Nutzer, welche folgende Bedingungen erfüllen, durch den RADIUS Server authentifiziert werden:

- Nutzung von EAP-TLS (Zertifikat)
- Nutzer hat einen aktiven LDAP-Account
- Nutzer ist in der LDAP-Gruppe „wpa3user“

Sollte eine der oben genannten Bedingungen nicht erfüllt sein, wird die Anfrage abgelehnt. Dies führt zum Abbruch des Anmeldevorgangs beim WLAN.

5.3 Scoringsystem

Um die einzelnen Schwachstellen miteinander vergleichen zu können, gibt es verschiedene Methoden bzw. Messverfahren, um das Risiko und die Eintrittswahrscheinlichkeit und somit das Ausmaß einer Schwachstelle darzustellen.

5.3.1 Common Vulnerability Scoring System

Das Common Vulnerability Scoring System (CVSS) wurde im Jahr 2005 als Entwurf von dem National Infrastructure Advisory Council (NIAC) vorgestellt und liegt mit der aktuellen Version 3.1 in der Verantwortlichkeit des Forum of Incident Response and Security Teams (FIRST). Das CVSS wird unter anderem für die Bewertung von Common Vulnerabilities and Exposures (CVE) Meldungen der MITRE Datenbank verwendet. In der IT-Sicherheitsbranche hat sich das CVSS als Quasi-Standard durchgesetzt und findet bei vielen großen Soft- und Hardwarehersteller wie HP, Symantec oder Microsoft bei der Veröffentlichung bzw. Deklarierung von Sicherheitslücken in Systemen oder Software, Verwendung. [30, S. 362]

Ein CVSS-Eintrag wird in drei verschiedene Metrik-Gruppen untergliedert. Die Base Metric Group bildet hierbei die wesentlichen und technischen Merkmale einer Schwachstelle, welche unabhängig der Umgebung und des zeitlichen Faktors existieren, ab. In der Temporal Metric Group werden wiederum die zeitlichen oder umgebungsabhängigen Faktoren dargestellt; je nachdem ob eine Schwachstelle bzw. der Schadcode veröffentlicht ist oder ein Hersteller bereits einen Patch veröffentlich hat, verändern sich die Metrik-Gruppen mit der Zeit. Die

Environmental Metric Group bündelt die Einflüsse in der vorhandenen Umgebung, welche sich je nach Unternehmen oder Institution unterscheiden und sich im Laufe der Zeit ebenfalls verändern können bzw. angepasst werden müssen. Innerhalb der Metric Groups sind verschiedene Vektor-Werte mit den zutreffenden Kategorien („None“, „Low“, „Medium“, „High“ oder „Critical“) zu wählen; diese spiegelt am Schluss den Schweregrad der Schwachstelle von 0,0 bis 10,0 wieder.

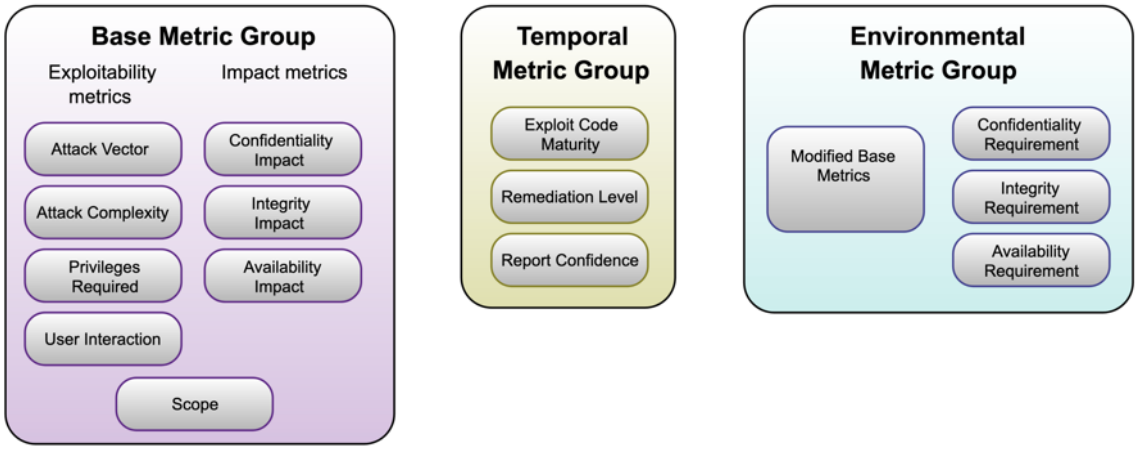

Abbildung 40: CVSS Metric Groups (Quelle: https://bit.ly/3ijsOBT)

Es besteht die Möglichkeit eine Schwachstellenmeldung mit einem CVSS-Rechner abzubilden und abhängig von den Metric Groups Temporal und Environmental auf die gegebene Situation anzupassen. In einer Sicherheitsmeldung der verschiedenen Stellen wie z.B. des Computer Emergency Response Team (CERT) wird zunächst nicht der Vektor, bestehend aus den Metric Groups oder dem Schweregrad angegeben, sondern die CVE-Nummer im Format CVE-YYYY-NNNNN (Jahr und eine fünfstellige fortlaufende Nummer), welche auf die zentrale MITRE-Datenbank verweist. Hierbei sind der CVSS-Vektor und die CVE-Nummer bzw. der Eintrag in der Datenbank unabhängig voneinander zu betrachten. Das CVSS dient lediglich zur Schweregradermittlung.

Beispielhaft wird in der folgenden Abbildung der Base Metric Score für die Schwachstelle CVE-2017-9494 angegeben (in der Version 3.1).

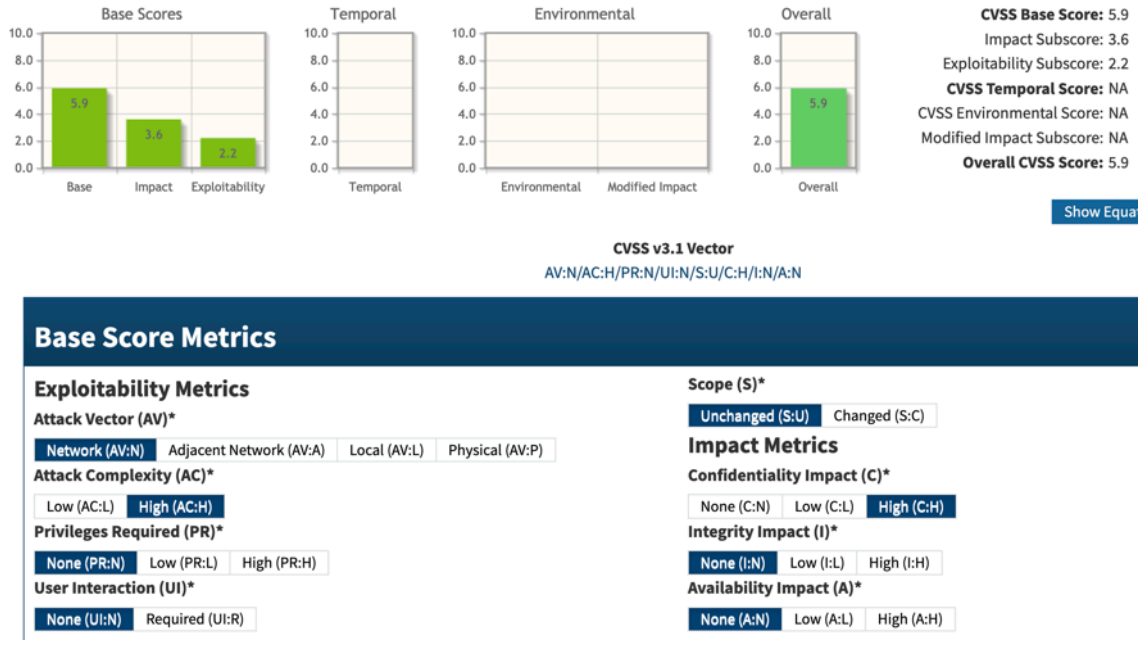

Abbildung 41: NIST Bewertung CVE-2019-9494 (Quelle: https://bit.ly/36KOGki)

Die Werte für die Temporal und Environmental Groups sind noch nicht gesetzt, da die CVE-Meldungen immer nur den Base Score abdecken.

Der Vektor für die Schwachstelle CVE-2019-9494 ist somit AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N.

5.3.2 DREAD Modell

Das DREAD Modell ist Bestandteil der Microsoft Treat-Modeling-Vorgehensweise und bildet mit den fünf Buchstaben gleichzeitig die beinhalteten Metriken wie folgt ab:

- Damage Potential
- Reproducibility
- Exploitability
- Affected Users
- Discoverability

Zu jeder Metrik wird bei der Analyse ein numerischer Wert zwischen 1 (gering) und 3 (hoch) zugewiesen und am Schluss der Gesamtwert gebildet. Dieser kann dementsprechend zwischen 5 und 15 betragen. [30, S. 385]

Hierbei werden Bedrohungen mit einem Rating von 12-15 als High, 8-11 als Medium und 5-7 als Low eingestuft. Um die Werte für die jeweiligen Metriken richtig einzuschätzen hat Microsoft Beschreibungen der Einstufungen als Hilfestellung im Prozess definiert:

	Rating	High (3)	Medium (2)	Low (1)
D	Damage potential	The attacker can subvert the security system; get full trust authorization; run as administrator; upload content.	Leaking sensitive information	Leaking trivial information
R	Reproducibility	The attack can be reproduced every time and does not require a timing window.	The attack can be reproduced, but only with a timing window and a particular race situation.	The attack is very difficult to reproduce, even with knowledge of the security hole.
E	Exploitability	A novice programmer could make the attack in a short time.	A skilled programmer could make the attack, then repeat the steps.	The attack requires an extremely skilled person and in-depth knowledge every time to exploit.
A	Affected users	All users, default configuration, key customers	Some users, non-default configuration	Very small percentage of users, obscure feature; affects anonymous users
D	Discoverability	Published information explains the attack. The vulnerability is found in the most commonly used feature and is very noticeable.	The vulnerability is in a seldom-used part of the product, and only a few users should come across it. It would take some thinking to see malicious use.	The bug is obscure, and it is unlikely that users will work out damage potential.

Abbildung 42: DREAD Metriken (Quelle: https://bit.ly/3ipyYjE)

Die Methode soll am Beispiel der Bedrohung „Angreifer erlangte Anmeldedaten durch Netzwerk Monitoring“ verdeutlicht werden. Es werden dementsprechend die Werte gesetzt, die Bedrohung bewertet und hieraus mögliche Gegenmaßnahmen abgeleitet.

Tabelle 9: DREAD Bewertung für Angriffsfall (Quelle: eigene Darstellung)

Bedrohung	D	R	E	A	D	Gesamt	Rating
Angreifer erlangte Anmeldedaten durch Netzwerk Monitoring	3	3	2	2	2	12	High

Tabelle 10: DREAD Gegenmaßnahme für Angriffsfall (Quelle: eigene Darstellung)

Bedrohung Nr	1
Beschreibung	Angreifer erlangte Anmeldedaten durch Netzwerk Monitoring
Angriffsziel	WebAnwendung 1, Nutzerzugriff
Risiko Rating	High
Genutzte Methode	Netzwerk Monitoring Tool
Gegenmaßnahmen	Nutzen von SSL um verschlüsselte Kommunikation sicherzustellen

Die einzelnen Metriken können je nach Umgebung oder Sachverhalt (z.B. Anzahl der betroffenen Clients) durch eine unterschiedliche Gewichtung stärker oder schwächer gewertet werden. Bei mehrfachem Scoring, z.B. vor und nach geeigneten Risikominderungsmaßnahmen, ist zur besseren Vergleichbarkeit die Verwendung derselben Gewichtung ratsam.

5.3.3 Analyse Scoringsysteme

Das DREAD-Modell ist im Gegensatz zu CVSS ein wesentlich einfacheres Modell zur Risikobewertung. Durch den weit verbreiteten Einsatz des CVSS-Modells handelt es sich, wie bereits erwähnt, um einen Quasi-Standard im IT-Sicherheitsbereich. Bei kleineren Sicherheitslücken bzw. Schwachstellen von nicht öffentlichem Interesse, werden jedoch häufig keine Meldungen seitens NIST oder CERT veröffentlicht. Verpflichtende Regelungen zur Anwendung der beiden Modelle existieren nicht. Die für die Bewertung Verantwortlichen können damit unabhängig über den Einsatz von CVSS oder eines anderen Modells wie DREAD zur Risikobewertung entscheiden.

5.4 Schwachstelle KRACK

Eine Veröffentlichung der benötigten Skripte bzw. des Schadcodes für die Key-Reinstallation Attacke erfolgte durch die Verantwortlichen nicht. Es wurden lediglich Programme veröffentlicht, die eine Möglichkeit der Überprüfung der Anfälligkeit der eigenen Geräte ermöglichen. Die erweiterte Attacke „all-zero-key“ kann jedoch je nach Gerät nachgestellt bzw. analysiert werden.

In der praktischen Evaluierung wurden mittels dem eingesetzten Samsung Galaxy S4 die zero-key-Attacke erfolgreich durchgeführt.

Abbildung 43: Praktischer Aufbau WPA2 KRACK all-zero-key Attacke (Quelle: eigene Darstellung)

Wie der nachfolgenden Abbildungen zu entnehmen ist, wird zunächst die man-in-the-middle Position zwischen dem Client und dem originären Access-Point aufgebaut.

```
[18:16:53] Real channel : 10:a5:d0:08:4f:73 -> 3e:94:ed:c7:20:a4: Null(seq=3971, sleep=0)
[18:16:53] Real channel : 10:a5:d0:08:4f:73 -> 3e:94:ed:c7:4e:da: Auth(seq=3972, status=0)
[18:16:53] Client 10:a5:d0:08:4f:73 is connecting on real channel, injecting CSA beacon to try to correct.
[18:16:53] Injected 1 CSA beacon pairs (moving stations to channel 1)
[18:16:53] Injected 1 CSA beacon pairs (moving stations to channel 1)
[18:16:53] Real channel : 3e:94:ed:c7:4e:da -> 10:a5:d0:08:4f:73: Auth(seq=1398, status=0) -- MitM'ing
[18:16:53] Rogue channel: 10:a5:d0:08:4f:73 -> 3e:94:ed:c7:4e:da: Null(seq=3974, sleep=0)
           Established MitM position against client 10:a5:d0:08:4f:73 (moved to state 2)
[18:16:53] Real channel : 10:a5:d0:08:4f:73 -> 3e:94:ed:c7:4e:da: ReassoReq(seq=3973)
[18:16:53] Rogue channel: 10:a5:d0:08:4f:73 -> 3e:94:ed:c7:4e:da: Null(seq=3975, sleep=0)
```

Abbildung 44: KRACK all-zero-key man-in-the-middle Position (Quelle: eigene Darstellung)

Im Anschluss erfolgt die eigentliche Attacke und das erfolgreiche Zurücksetzen des Schlüssels auf Null.

```
[18:16:54] Real channel : 3e:94:ed:c7:4e:da -> 10:a5:d0:08:4f:73: EAPOL-Msg3(seq=1,replay=2) -- MitM'ing
           Not forwarding EAPOL msg3 (1 unique now queued)
[18:16:54] Real channel : 3e:94:ed:c7:4e:da -> 10:a5:d0:08:4f:73: EAPOL-Msg3(seq=1,replay=2) -- MitM'ing
           Not forwarding EAPOL msg3 (1 unique now queued)
[18:16:56] Rogue channel: 3e:94:ed:c7:4e:da -> 30:cd:a7:a0:8f:8b: ProbeResp(seq=49)
[18:16:56] Rogue channel: 3e:94:ed:c7:4e:da -> 30:cd:a7:a0:8f:8b: ProbeResp(seq=50)
[18:16:56] Rogue channel: 3e:94:ed:c7:4e:da -> 30:cd:a7:a0:8f:8b: ProbeResp(seq=51)
[18:16:56] Rogue channel: 3e:94:ed:c7:4e:da -> 30:cd:a7:a0:8f:8b: ProbeResp(seq=52)
[18:16:56] Rogue channel: 3e:94:ed:c7:4e:da -> 30:cd:a7:a0:8f:8b: ProbeResp(seq=53)
[18:16:56] Real channel : 3e:94:ed:c7:4e:da -> 10:a5:d0:08:4f:73: EAPOL-Msg3(seq=2,replay=3) -- MitM'ing
           Got 2nd unique EAPOL msg3. Will forward both these Msg3's seperated by a forged msg1.
           ==> Performing key reinstallation attack!
[18:16:56] Real channel : 30:cd:a7:a0:8f:8b -> 3e:94:ed:c7:4e:da: Auth(seq=3434, status=0)
[18:16:56] Injected 1 CSA beacon pairs (moving stations to channel 1)
[18:16:56] Injected 1 CSA beacon pairs (moving stations to channel 1)
[18:16:56] Rogue channel: 10:a5:d0:08:4f:73 -> 3e:94:ed:c7:4e:da: Null(seq=3978, sleep=0)
[18:16:56] Rogue channel: 10:a5:d0:08:4f:73 -> 3e:94:ed:c7:4e:da: Action(seq=3979) -- MitM'ing
[18:16:56] Real channel : 3e:94:ed:c7:4e:da -> 30:cd:a7:a0:8f:8b: Disas(seq=0)
[18:16:56] Rogue channel: 10:a5:d0:08:4f:73 -> 3e:94:ed:c7:4e:da: EAPOL-Msg4(seq=744,replay=2)
[18:16:56] Rogue channel: 10:a5:d0:08:4f:73 -> 3e:94:ed:c7:4e:da: Null(seq=3980, sleep=0)
[18:16:56] Real channel : 3e:94:ed:c7:4e:da -> 10:a5:d0:08:4f:73: EAPOL-Msg3(seq=2,replay=3) -- MitM'ing
[18:16:56] Rogue channel: 10:a5:d0:08:4f:73 -> 3e:94:ed:c7:4e:da: EncryptedData(seq=745, IV=1)
[18:16:56] Real channel : 3e:94:ed:c7:4e:da -> 10:a5:d0:08:4f:73: EAPOL-Msg3(seq=2,replay=3) -- MitM'ing
[18:16:56] Rogue channel: 10:a5:d0:08:4f:73 -> 3e:94:ed:c7:4e:da: Null(seq=3981, sleep=0)
[18:16:56] Real channel : 3e:94:ed:c7:4e:da -> 10:a5:d0:08:4f:73: EAPOL-Msg3(seq=2,replay=3) -- MitM'ing
[18:16:56] Rogue channel: 10:a5:d0:08:4f:73 -> 3e:94:ed:c7:4e:da: EncryptedData(seq=746, IV=1)
           SUCCESS! Nonce and keystream reuse detected (IV=1).
[18:16:56] Real channel : 3e:94:ed:c7:4e:da -> 10:a5:d0:08:4f:73: EAPOL-Msg3(seq=2,replay=3) -- MitM'ing
[18:16:56] Rogue channel: 10:a5:d0:08:4f:73 -> 3e:94:ed:c7:4e:da: Null(seq=3982, sleep=0) -- MitM'ing
[18:16:56] Real channel : 30:cd:a7:a0:8f:8b -> 3e:94:ed:c7:4e:da: Auth(seq=3434, status=0)
[18:16:56] Injected 1 CSA beacon pairs (moving stations to channel 1)
[18:16:56] Injected 1 CSA beacon pairs (moving stations to channel 1)
```

Abbildung 45: KRACK all-zero-key Zurücksetzen des Schlüssels (Quelle: eigene Darstellung)

Ab diesem Zeitpunkt wird der Datenverkehr vom Angreifer unverschlüsselt empfangen und an den originären Access-Point durchgeschleust.

Das genutzte Gerät ist zwar bereits seit 2013 auf dem Markt und es wurden seitdem ca. 80 Millionen Stück weltweit verkauft; ein vergleichbares Gerät ist zum aktuellen Stand relativ preiswert zu erwerben und mit Nutzung des LTE-Netzes noch immer aktuell. [31] Die Sicherheitslücke beschränkt sich nicht nur auf dieses Modell, sondern ist für alle Android Geräte mit dem Programm wpa_supplicant ab Version 2.4 identisch anwendbar. Die Bedrohung ist zwar relativ hoch, jedoch bleibt die Attacke spätestens bei einer (vorherigen) Neuverbindung der Internetseiten nicht unbemerkt. Der Browser zeigt einen Wechsel von https zu http an, da der Angriff eine Durchschleusung von gesicherten Verbindungen nicht abbilden kann.

Die KRACK-Attacke wurde in verschiedene CVEs unterteilt; die betreffende Schwachstelle bezüglich des PTK wurde als CVE-2017-13077 veröffentlicht und mit einem Wert von 6,8 als Medium eingestuft:

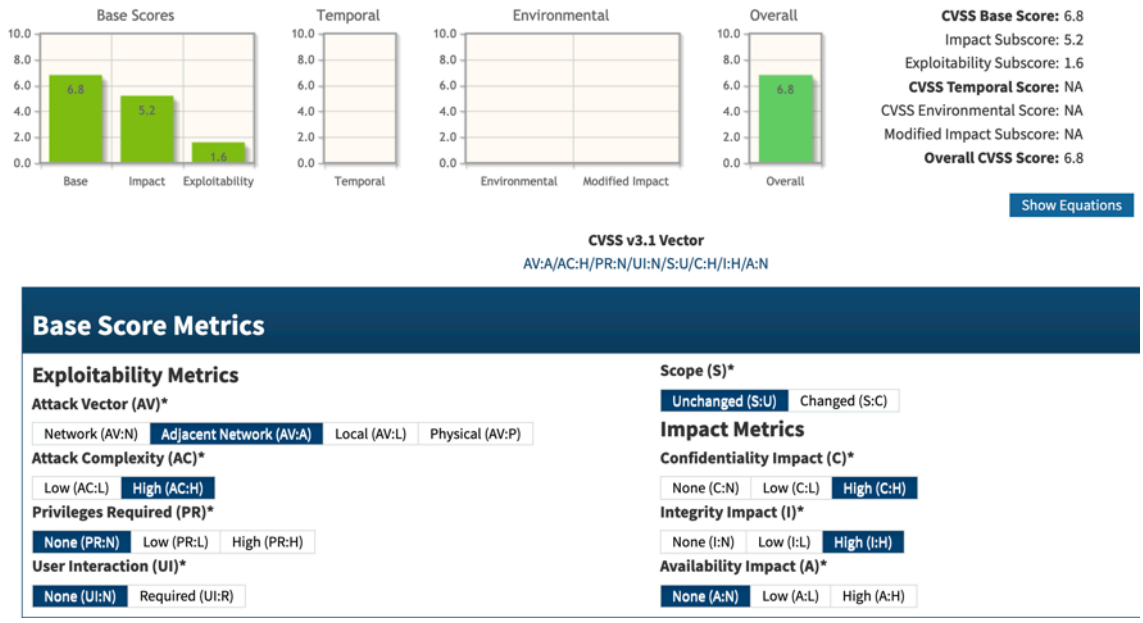

Abbildung 46: NIST Bewertung CVE-2017-13077 (Quelle: https://bit.ly/3iy5Maq)

Eine Spezifizierung für die umgesetzte zero-key-Attacke erfolgte nicht.

5.5 Schwachstelle Dragonblood

Bei der bereits im Theorieteil beschriebenen Schwachstelle Dragonblood konnte eine Downgrade Attacke erfolgreich in der Praxis umgesetzt werden. Hierbei bildete der Angreifer durch einen „bösen Zwilling“ einen weiteren Access-Point, mit dem Unterschied der unsichereren und ausschließlichen Authentifizierungsmethode des Pre-Shared Keys, ab.

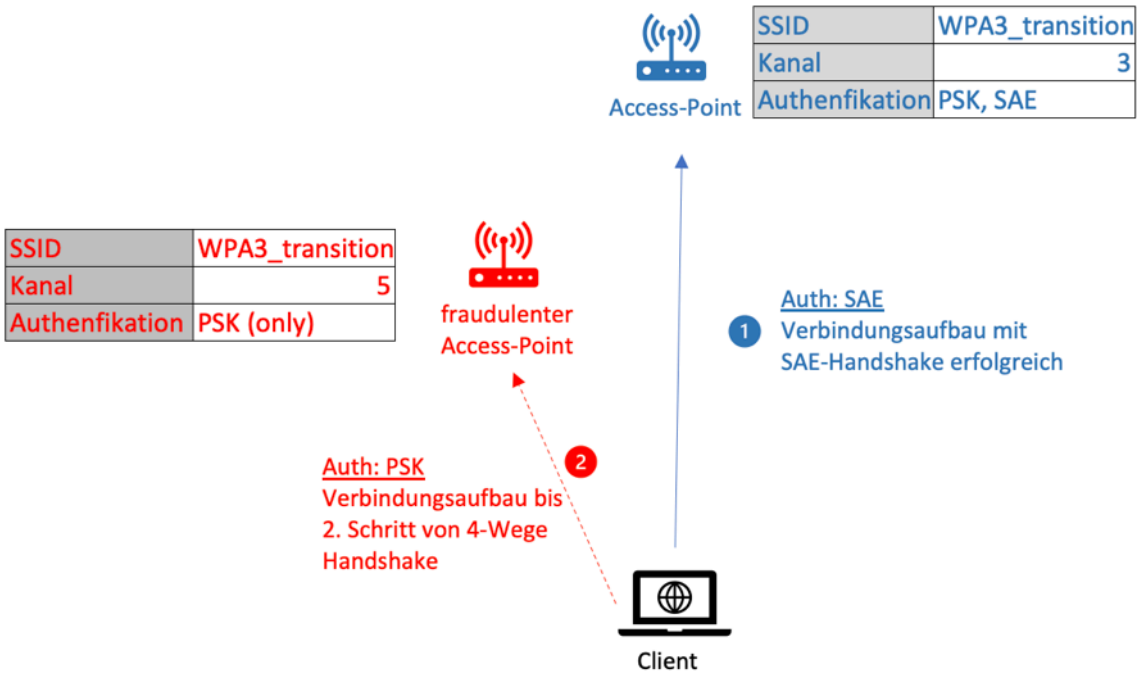

Abbildung 47: Praktischer Aufbau WPA3-Transition Downgrade Attacke (Quelle: eigene Darstellung)

Wesentliche Merkmale des Angriffs sind die Reichweite und die Signalstärke aus Sicht des Clients. Sollten diese Kriterien beim fraudulenten Access-Point besser bzw. stärker ausgeprägt sein, wird dieser durch den Client in Betracht gezogen und somit bis zum zweiten Schritt des 4-Wege Handshakes als AP bevorzugt. Zur besseren Darstellung des Verbindungsaufbaus erfolgt die Verbindung mittels iNet wireless deamon (iwd) bzw. dem Client-Programm iNet wireless client (iwctl). Dieses stellt zunächst die Verbindung mit den originären Access-Point her.

```
debian@debian:~$ sudo iwctl
[iwd]# station list
                            Devices in Station Mode
--------------------------------------------------------------
  Name                State          Scanning
--------------------------------------------------------------
  wlx00c0ca991420     disconnected   scanning

[iwd]# station wlx00c0ca991420 scan
[iwd]# station wlx00c0ca991420 get-networks
                               Available networks
--------------------------------------------------------------
    Network name                      Security  Signal
--------------------------------------------------------------
    Honeypot                          psk       ****
  > WPA3_transition                   psk       ****
    UPC5E25CCD_EXT                    psk       ****
    UPC1643967                        psk       ****
    WLAN-CE9893                       psk       ****

[iwd]# station wlx00c0ca991420 connect WPA3_transition
Type the network passphrase for WPA3_transition psk.
Passphrase: ***********
```

Abbildung 48: Verbindungsaufbau mit iwctl (Quelle: eigene Darstellung)

Im Anschluss liest der Angreifer die jeweiligen Daten für den Angriff aus, um sicherzugehen, dass der Client sich erfolgreich mit dem originären Access-Point verbunden hat (4-Wege Handshake abgeschlossen). In den folgenden zwei Abbildungen sind die Broadcast Nachricht vom Access-Point und zweite Nachricht des 4-Wege Handshakes dargestellt. Der originäre Access-Point bietet hierbei sowohl PSK als auch SAE als Verfahren an. Des Weiteren authentifiziert sich der Client via SAE am Access-Point.

```
1 0.000000   Synology_ce:6d:36   Broadcast   802.11   325 Beacon frame, SN=1948, FN=0, Flags=........, BI=100, SSID=WPA3_transition

ag: RSN Information
  Tag Number: RSN Information (48)
  Tag length: 24
  RSN Version: 1
> Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
  Pairwise Cipher Suite Count: 1
> Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
  Auth Key Management (AKM) Suite Count: 2
  Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) PSK 00:0f:ac (Ieee 802.11) SAE (SHA256)
    > Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) PSK
    > Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) SAE (SHA256)
  RSN Capabilities: 0x008c
      .... .... .... ...0 = RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
      .... .... .... ..0. = RSN No Pairwise capabilities: Transmitter can support WEP default key 0 simultaneously with Pairwise key
      .... .... .... 11.. = RSN PTKSA Replay Counter capabilities: 16 replay counters per PTKSA/GTKSA/STAKeySA (0x3)
      .... .... ..00 .... = RSN GTKSA Replay Counter capabilities: 1 replay counter per PTKSA/GTKSA/STAKeySA (0x0)
      .... .... .0.. .... = Management Frame Protection Required: False
      .... .... 1... .... = Management Frame Protection Capable: True
      .... ...0 .... .... = Joint Multi-band RSNA: False
      .... ..0. .... .... = PeerKey Enabled: False
      ..0. .... .... .... = Extended Key ID for Individually Addressed Frames: Not supported
```

Abbildung 49: Wireshark Broadcast Frame Transition (Quelle: eigene Darstellung)

```
33 37.531492   ca:13:b2:f8:34:01   Synology_ce:6d:…   EAPOL   155 Key (Message 2 of 4)

Tag: RSN Information
  Tag Number: RSN Information (48)
  Tag length: 20
  RSN Version: 1
> Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
  Pairwise Cipher Suite Count: 1
> Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
  Auth Key Management (AKM) Suite Count: 1
  Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) SAE (SHA256)
    Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) SAE (SHA256)
      Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
      Auth Key Management (AKM) type: SAE (SHA256) (8)
  RSN Capabilities: 0x0080
      .... .... .... ...0 = RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
      .... .... .... ..0. = RSN No Pairwise capabilities: Transmitter can support WEP default key 0 simultaneously with Pairwise key
      .... .... .... 00.. = RSN PTKSA Replay Counter capabilities: 1 replay counter per PTKSA/GTKSA/STAKeySA (0x0)
      .... .... ..00 .... = RSN GTKSA Replay Counter capabilities: 1 replay counter per PTKSA/GTKSA/STAKeySA (0x0)
      .... .... .0.. .... = Management Frame Protection Required: False
      .... .... 1... .... = Management Frame Protection Capable: True
      .... ...0 .... .... = Joint Multi-band RSNA: False
      .... ..0. .... .... = PeerKey Enabled: False
      ..0. .... .... .... = Extended Key ID for Individually Addressed Frames: Not supported
```

Abbildung 50: Wireshark Client Auth mit SAE (Quelle: eigene Darstellung)

Daraufhin startet der Angreifer den fraudulenten Access-Point und wartet auf den Verbindungsversuch des Clients, um bis zum zweiten Schritt des 4-Wege Handshakes die Informationen auszutauschen. In der folgenden Abbildung ist zu erkennen, dass sich sowohl PMF als auch die Authentifizierungsmethode hin zu PSK statt SAE geändert hat.

```
557 39.267303  Raspberr_49:de:9b  Broadcast  802.11   216 Beacon frame, SN=1652, FN=0, Flags=........, BI=100, SSID=WPA3_transition
  > Multicast Cipher Suite: 00:50:f2 (Microsoft Corp.) TKIP
    Unicast Cipher Suite Count: 2
  v Unicast Cipher Suite List 00:50:f2 (Microsoft Corp.) AES (CCM) 00:50:f2 (Microsoft Corp.) TKIP
    > Unicast Cipher Suite: 00:50:f2 (Microsoft Corp.) AES (CCM)
    > Unicast Cipher Suite: 00:50:f2 (Microsoft Corp.) TKIP
    Auth Key Management (AKM) Suite Count: 1
  v Auth Key Management (AKM) List 00:50:f2 (Microsoft Corp.) PSK
    v Auth Key Management (AKM) Suite: 00:50:f2 (Microsoft Corp.) PSK
        Auth Key Management (AKM) OUI: 00:50:f2 (Microsoft Corp.)
        Auth Key Management (AKM) type: PSK (2)
```

Abbildung 51: Wireshark fraudulente AP mit PSK (Quelle: eigene Darstellung)

```
1783 77.933487  fe:8d…  Raspberr…  EAPOL    157 Key (Message 2 of 4)
    Type: WPA Information Element (0x01)
    WPA Version: 1
  > Multicast Cipher Suite: 00:50:f2 (Microsoft Corp.) TKIP
    Unicast Cipher Suite Count: 1
  v Unicast Cipher Suite List 00:50:f2 (Microsoft Corp.) AES (CCM)
    > Unicast Cipher Suite: 00:50:f2 (Microsoft Corp.) AES (CCM)
    Auth Key Management (AKM) Suite Count: 1
  v Auth Key Management (AKM) List 00:50:f2 (Microsoft Corp.) PSK
    v Auth Key Management (AKM) Suite: 00:50:f2 (Microsoft Corp.) PSK
        Auth Key Management (AKM) OUI: 00:50:f2 (Microsoft Corp.)
        Auth Key Management (AKM) type: PSK (2)
```

Abbildung 52: Wireshark Verbindungsaufbau Client mit fraudulenten AP (Quelle: eigene Darstellung)

Mit dem teilweise abgefangenen 4-Wege Handshake startet der Angreifer nun eine Offline-Wörterbuch Attacke und erhält so das genutzte Passwort für das WLAN-Netzwerk.

```
                      Aircrack-ng 1.5.2

[00:00:46] 62255/9822769 keys tested (1318.05 k/s)

Time left: 2 hours, 3 minutes, 25 seconds                 0.63%

                    KEY FOUND! [ Password123 ]


Master Key     : 70 15 40 2C 4E 05 50 3A AA 8C 31 99 A3 DE 42 1D
                 0C 15 65 D3 45 9B AC AA 62 1C 61 DB A0 0F DC 40

Transient Key  : 95 AF 7E 0B EE 15 14 B6 B7 8D AF 80 A4 D3 2E EE
                 55 64 39 34 BC E8 13 71 58 8B 95 9F 5B AB 73 C3
                 6A 44 C9 7C 7F D7 5F D1 41 44 15 9E 98 7D B1 9E
                 8E F1 92 DA 5C 62 EA 90 36 91 C7 D9 6F D1 3F 63

EAPOL HMAC     : 59 8F AF A4 2F DC 76 A3 31 88 A8 75 67 F4 9F E2
```

Abbildung 53: Offline-Wörterbuch Attacke mit Aircrack-ng (Quelle: eigene Darstellung)

Je nach Komplexität des genutzten Passworts und der Qualität der genutzten Wörterbuch-Datei, kann der Vorgang unterschiedlich lange dauern.

Die praktische Verifikation der Downgrade Attacke wurde ebenfalls mit den Clients (Samsung Galaxy S4 und iPhone 12) erfolgreich durchgeführt. Details zum Verbindungsaufbau sind der Anlage 2 zu entnehmen.

Die dargestellte Schwachstelle wurde vom CERT unter der ID871675 veröffentlicht. Neben der Dragonblood Schwachstelle wurden im Dragonfly Protokoll weitere Lücken hinsichtlich EAP-PWD festgestellt; diese sind auf Grund nicht kompatibler Hardware nicht Bestandteil der praktischen Verifikation. [32]

5.6 Bewertung der WPA Schwachstellen

Trotz der hohen Sicherheit des SAE Verfahrens bzw. des Dragonfly Handshakes ist die Gefahr hoch, dass sich Angreifer, resultierend aus schwachen Passwörtern im Transition Mode, mit einem Downgrade Angriff relativ leicht Zugang zu vermeintlich sicheren WPA3-Netzwerken verschaffen können. Diese Art von Angriff wird von einem Intrusion Detection System nicht wahrgenommen, da sich der Angreifer „nur“ durch die Kommunikation mit dem Client bemerkbar macht. Die dargestellte Downgrade Attacke konnte sowohl mit einem Samsung Galaxy S4 als auch mit einem Apple iPhone 12 reproduziert werden. Da das eingesetzte Samsung Galaxy S4 die bereits erwähnten Mindestvorrausetzungen für WPA3 nicht erfüllt, handelt es sich hierbei um keine originäre Downgrade Attacke. Grund dafür ist, dass das Gerät nur die Methode PSK als Authentifizierungsverfahren zulässt und somit nicht auf die Nutzung eines anderen Verfahrens gezwungen werden kann. Das neuere mobile Endgerät Apple iPhone 12 ist hingegen mit iOS 14.6 WPA3 fähig. Diese praktische Verifikation kann damit als „echte“ Downgrade Attacke bezeichnet werden, da das mobile Endgerät zur Nutzung von PSK anstatt von SAE gezwungen werden konnte. Durch den Transition Mode im WPA3 Standard können somit die ersten Teile des 4-Wege Handshakes sowohl bei den neueren als auch bei den älteren Endgeräten abgefangen und mittels Offline-Wörterbuch Angriff dechiffriert werden. Durch den Einsatz des Transition Modes und dessen Abwärtskompatibilität ist somit keine Abhängigkeit von verschiedenen Endgeräten bzw. Betriebssystemen erkennbar.

Gemäß aktuellen Erhebungen befinden sich im Jahr 2021 weltweit rund 4,3 Milliarden Smartphones im Gebrauch. [33] Die Marktanteile der mobilen Betriebssysteme werden durch Android (69,8 %) und iOS (29,8 %) dominiert. [34] Eine Aufteilung in WPA3 kompatible Betriebssysteme kann anhand der jeweiligen Versionen erfolgen. Bei iOS ist die Kompatibilität ab einer Version 13 oder höher sichergestellt; diese Vorrausetzung erfüllen derzeit rund 93 % der iOS-Geräte. [35] Für Android-Geräte gilt die Mindestvoraussetzung des Android OS 10; derzeit erfüllen rund 51 % der Geräte diese Anforderung. [36] Zusammenfassend bedeutet dies, dass im mobilen Sektor ca. 2,7 Milliarden Endgeräte WPA3 unterstützen und rund 1,6 Milliarden Endgeräte nicht WPA3-kompatibel sind und im Transition Mode theoretisch nicht vor eine Downgrade Attacke geschützt sind. Zusätzlich sind natürlich noch weitere Geräte wie Laptops oder Tablets von diesen Auswirkungen betroffen. Das Ausmaß der theoretisch betroffenen Endgeräte im Rahmen der Abwärtskompatibilität ist damit enorm und steht in keinem Verhältnis zu den Vorteilen des Transition Modes.

Eine Verhinderung der Downgrade Attacke kann u.a. durch eine separate Konfiguration der beiden Standards verhindert werden; auf diese Möglichkeit wird im Fazit dieser Arbeit eingegangen.

Die Bewertung beider Schwachstellen wurde, mangels Veröffentlichung einer CVE und eines offiziellen CVSS Vektor, mittels DREAD Verfahren durchgeführt. In der folgenden Tabelle ist der Vergleich beider Schwachstellen mittels DREAD Verfahren dargestellt.

Tabelle 11: Scoring der Bedrohungen mittels DREAD (Quelle: eigene Darstellung)

Nr	Bedrohung	D	R	E	A	D	Gesamt	Rating
1	WPA2-Personal Mode: all-zero-key Attacke auf Android Geräte	3	2	2	2	2	11	Medium
2	WPA3-Personal Transition Mode: Downgrade Attacke; Zwang des Clients zur Nutzung von PSK statt SAE	2	3	3	3	3	14	High
	Gewichtung	1	0,8	0,8	1,6	0,8		

Zur Ermittlung des Scorings der beiden Bedrohungen wurde beim DREAD Verfahren auf eine Gewichtung der Metriken zurückgegriffen.

Die Gewichtung der Metrik A (Affected Users) erfolgte auf Grund der hohen Anzahl der betroffenen Geräte mit einem erhöhten Wert (1,6). Bei der Downgrade Attacke handelt es sich um einen Designfehler im aktuellen Protokoll Standard. Dieser ist bisher durch die Hersteller der Endgeräte, anders als bei KRACK-Attacke, noch nicht durch ein Update ausgemerzt.

Zur Verhinderung der betrachteten Bedrohungen konnten folgende Gegenmaßnahmen identifiziert werden:

Tabelle 12: Ableitung von Gegenmaßnahmen Bedrohung Nr. 1 (Quelle: eigene Darstellung)

Bedrohung Nr	1
Beschreibung	WPA2-Personal Mode: all-zero-key Attacke auf Android Geräte
Angriffsziel	Auslesen des Datenstroms
Risiko Rating	Medium
Genutzte Methode	man-in-the-middle; fraudulenter AP; Netzwerkanalysetools
Gegenmaßnahmen	Update der Clientsoftware sowie Firmware der Netzwerkgeräte; Sensibilisierung der Nutzer (z.B. Browsersicherheit mit HTTPS)

Tabelle 13: Ableitung von Gegenmaßnahmen Bedrohung Nr. 2 (Quelle: eigene Darstellung)

Bedrohung Nr	2
Beschreibung	WPA3-Personal Transition Mode: Downgrade Attacke; Zwang des Clients zur Nutzung von PSK statt SAE
Angriffsziel	Auslesen der 4-Wege Handshake Nachrichten
Risiko Rating	High
Genutzte Methode	fraudulenter AP; Netzwerkanalysetools
Gegenmaßnahmen	Trennung der BSS in WPA2- und WPA3-Personal; Passwortkomplexität erhöhen (vor allem beim WPA2 BSS)

Mit Blick auf die identifizierten Risikominimierungsmaßnahmen ergibt sich folgende neue Bewertung mittels DREAD Verfahren. Zur besseren Vergleichbarkeit ist die Gewichtung bei der zweiten Evaluierung unverändert.

Tabelle 14: Scoring der Bedrohungen nach Gegenmaßnahmen (Quelle: eigene Darstellung)

Nr	Bedrohung	D	R	E	A	D	Gesamt	Rating
1	WPA2-Personal Mode: KRACK all-zero-key Attacke auf Android Geräte	2	1	2	1	2	7,6	Low
2	WPA3-Personal Transition Mode: Downgrade Attacke; Zwang des Clients zur Nutzung von PSK statt SAE	2	1	1	3	3	10,8	Medium
	Gewichtung	1	0,8	0,8	1,6	0,8		

In der Bewertung wird davon ausgegangen, dass sich bei der ersten Bedrohung die Anzahl der Geräte durch ein Update des Herstellers deutlich reduziert und sich somit auch die Reproduzierbarkeit schwächer darstellt. Das Schadenspotenzial sinkt, da die übertragenen Informationen nicht mehr mit einem trivialen Null-Schlüssel „verschlüsselt“ werden. Die Metriken D (Schadenspotenzial), R (Reproduzierbarkeit) sowie A (Ausnutzbarkeit) werden deshalb mit einem niedrigeren Wert angesetzt; im Vergleich zur ersten Evaluation führt dies mit einem Low Rating zu einer Ratingverbesserung.

Im Rahmen der Evaluation der zweiten Bedrohung bleibt die erhöhte Einstufung der betroffenen Nutzer unverändert bestehen, da durch die aufgeführten Gegenmaßnahmen keine Änderung des Standard-Designs erfolgt. Die Reproduzierbarkeit wird in der zweiten Evaluation mit einem geringen Risiko eingestuft. Durch die Verbesserung in den Bereichen der Passwortkomplexität sowie der Trennung der jeweiligen Standards in separierte BSS sinkt das Risiko eines möglichen Angriffs erheblich. Die Metrik E (Ausnutzbarkeit) wurde ebenfalls mit einem geringen Risiko eingestuft, da durch die Gegenmaßnahmen kein Transition Mode verfügbar und eine „originäre“ Downgrade Attacke damit nicht mehr eins zu eins abbildbar ist. Auf Grund der niedrigeren Einstufung der Metriken R und E ergibt sich im Vergleich zur ersten Evaluation für die zweite Bedrohung ein Medium Rating und damit ebenfalls eine Ratingverbesserung.

6 Fazit und Ausblick

Der Standard WPA3 bietet durch die individuellen Sitzungsschlüssel, welche für jeden Client unterschiedlich sind, sowie durch die wesentlichen Aktualisierungen durch das Dragonfly Protokoll, erhebliche Verbesserungen in der WLAN-Sicherheit. Diese Verbesserungen sind durch die Nutzung des gemischten Modus (Transition Mode) leider nur optional gesetzt und können, wie in der praktischen Analyse aufgezeigt, von Angreifern umgangen werden. Wie bereits zu Beginn erwähnt, gestaltet sich die Sicherstellung einer Abwärtskompatibilität, mit mehreren Standards und deren genutzten Protokollen, als schwierig. Mit Blick auf die aus der Abwärtskompatibilität resultierende Anzahl der für eine Downgrade Attacke anfälligen Endgeräte ist das Ausmaß sehr hoch und steht somit in keinem Verhältnis zu den Vorteilen des Transition Modes. Mit geeigneten Gegenmaßnahmen können die Risiken der Bedrohung jedoch erheblich reduziert werden. Eine Empfehlung seitens der WiFi-Alliance ist, die jeweiligen Standards WPA2 und WPA3 in einzelne und von sich getrennte BSS zu konfigurieren und somit die Vorteile von WPA3, ohne die erörterte Schwachstelle einer Downgrade Attacke, vollends auszuschöpfen. [29] Ist eine Nutzung von getrennten BSS nicht möglich, muss zwingend ein starkes Passwort verwendet werden, da sonst die Gefahr von Downgrade- und darauffolgende Offline-Wörterbuch Attacken besteht.

Ein Update des IEEE 802.11 Standards bezüglich weiterer Flags im Protokollaustausch würde darüber hinaus eine weitere Möglichkeit zur Verhinderung einer Downgrade Attacke darstellen. Bei Aufnahme zusätzlicher Flags können diese Rückschlüsse auf den zuvor genutzten Authentifizierungsstandard geben und somit eine Herabstufung verhindern.

Eine weitere Verbesserung der Sicherheit hinsichtlich Downgrade Attacken birgt eine Implementierung des Verbindungsaufbaus gem. trust-on-first-use (TUFU) Prinzip innerhalb der Verbindungssoftware, wie z.B. wpa_supplicant oder iwd. Dies bewirkt, dass bei der nächsten Verbindung zur identischen SSID keine schwächere Einstellung beim Verbindungsaufbau genutzt werden kann.

Dieses Verfahren wird bereits bei einer bzw. der ersten SSH-Verbindung mit einem SSH-Server genutzt, indem der Benutzer den öffentlichen Schlüssel des Servers zum Verbindungsaufbau akzeptiert und somit dem Server vertraut. Bei einer Änderung des Schlüssels muss der Benutzer den Schlüssel erneut akzeptieren, spätestens an dieser Stelle sollte der Benutzer Verdacht schöpfen und sich fragen, ob der Server noch immer vertrauenswürdig ist. Ein solcher Mechanismus wäre bei den genutzten WPA3-Access-Points eine Möglichkeit die Integrität der jeweiligen Geräte gegenüber dem Client bzw. dem Benutzer zu wahren und mögliche fraudulente Access-Points durch eine Warnmeldung bzw. neue Akzeptierung des Schlüssels zu erkennen bzw. als Gefahr einzustufen.

Weitere Maßnahmen, wie z.B. das Updaten der verwendeten Geräte sowie die Sensibilisierung von den Benutzern ist zwar eine Standardprozedur, stellt jedoch ein wichtiger Bestandteil der Prävention von Attacken dar. Vor allem nach der Entdeckung der KRACK-Attacke waren die Hersteller seitens des CERT und der jeweiligen nationalen Behörden dahingehend angewiesen die Sicherheitslücke durch jeweilige Updates zu schließen. Wie bereits in der praktischen Verifikation dargestellt ist dies bei manchen, vor allem älteren, Geräten nicht so einfach, da der Support von neuerer Software nicht mehr gegeben ist. Die Möglichkeit die Geräte im Netzwerk durch die Programme auf die Sicherheitslücke zu testen, bringt letzten Endes die einzige Gewissheit, ob das genutzten Equipment anfällig ist oder nicht. Falls Geräte betroffen und keine Updates durch den Hersteller mehr vorhanden sind können durch minimale Änderungen in der Konfiguration von Netzwerkgeräten, z.B. das lokale Drucken oder ein Anschluss über LAN anstatt WLAN, die Sicherheit im gesamten Netzwerk verbessert werden.

Darüber hinaus muss vor allem im privaten Umfeld eine Sensibilisierung der Benutzer bezüglich der Passwortstärke und -länge erfolgen. Ein kurzes und nicht komplexes Passwort für das genutzte WLAN erleichtert zwar die Handhabung für die Benutzer; öffnet jedoch sowohl im WPA2 als auch WPA3 Transition Mode Tür und Tor für die Angreifer. Wie bereits erwähnt ist nicht nur die Komplexität des Passwortes, sondern auch der Änderungsrhythmus entscheidend. Eine Kombination aus beiden Kriterien bietet den Benutzern sowohl im privaten als auch im geschäftlichen Umfeld derzeit die höchste Sicherheit.

Literaturverzeichnis

[1] C. Baun, Computernetze kompakt, 5 Hrsg., Wiesbaden: Springer Vieweg, 2020.

[2] J. Scarpati, „WLAN-Sicherheit: Vergleich von WEP, WPA, WPA2 und WPA3,“ 05 2021. [Online]. Available: https://tinyurl.com/nj57k35s. [Zugriff am 04 06 2021].

[3] „Understanding PSK Authentication,“ Juniper Networks, 01 2019. [Online]. Available: https://juni.pr/3ktMdTe. [Zugriff am 03 06 2021].

[4] „WPA/WPA2,“ Kryptowissen, 11 2016. [Online]. Available: https://bit.ly/2UORBFM. [Zugriff am 06 06 2021].

[5] C. Eilers, „WLAN-Sicherheit 10 - Die Schlüssel von WPA2, Teil 2,“ 10 2017. [Online]. Available: https://bit.ly/3wNHxdB. [Zugriff am 06 06 2021].

[6] „IEEE 802.1x / RADIUS,“ Elektronik Kompendium, [Online]. Available: https://bit.ly/3kKKJ7b. [Zugriff am 06 06 2021].

[7] L. Kruse, „802.1x Zugangskontrolle mit EAP und RADIUS in LAN und WLAN Umgebungen,“ 2016. [Online]. Available: https://bit.ly/3eE4t8D. [Zugriff am 06 06 2021].

[8] S. Krecher, „WLAN und LAN sichern mit IEEE 802.1X und Radius,“ 04 2010. [Online]. Available: https://bit.ly/2UXtkgA. [Zugriff am 03 06 2021].

[9] M. Sauter, Grundkurs Mobile Kommunikationssysteme, 4. Auflage Hrsg., Wiesbaden: Vieweg+Teubner Verlag, 2011.

[10] C. Eilers, „“Hole196“ - Eine neue Schwachstelle in WPA2,“ 08 2010. [Online]. Available: https://bit.ly/3Bf60fb. [Zugriff am 21 06 2021].

[11] D. Westhoff, Mobile Security, Wiesbaden: Springer Vieweg, 2020.

[12] D. Fehér und B. Sándor, „Effects of the WPA2 KRACK Attack in Real Environment," 11 2018. [Online]. Available: https://bit.ly/3Bi2mRy. [Zugriff am 06 06 2021].

[13] M. Vanhoef und F. Piessens, „Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2," 2017. [Online]. Available: https://bit.ly/3kvuASU. [Zugriff am 21 06 2021].

[14] J. Schwenk, Sicherheit und Kryptographie im Internet, Wiesbaden: Springer Vieweg, 2020.

[15] „Discover Wi-Fi Security," WiFi-Alliance, [Online]. Available: https://bit.ly/36LpKca. [Zugriff am 04 07 2021].

[16] „WPA3: Die neue WLAN-Verschlüsselung erklärt," AVM, [Online]. Available: https://bit.ly/36FYBaE. [Zugriff am 04 07 2021].

[17] D. Wolski, „WPA3 mit Linux nutzen - so geht's," 05 2021. [Online]. Available: https://bit.ly/36GbYYz. [Zugriff am 04 07 2021].

[18] S. Luber und P. Schmitz, „Was ist SAE?," 11 2019. [Online]. Available: https://bit.ly/3hOtZKB. [Zugriff am 04 07 2021].

[19] A. Ahrens, Studienbrief Kryptographie II, Wismar, 2021.

[20] IEEE, Hrsg., *IEEE 802.11-2016,* New York, Kap. 12.4.5.2.

[21] M. Vanhoef und E. Ronen, „Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd," 2020. [Online]. Available: https://bit.ly/3hKm8gP. [Zugriff am 03 07 2021].

[22] C. Kohlios und T. Hayajneh, „A Comprehensive Attack Flow Model and Security Analysis for Wi-Fi and WPA3," 10 2018. [Online]. Available:

https://bit.ly/3xOAimU. [Zugriff am 03 07 2021].

[23] D. Fox, „Perfect Forward Secrecy (PFS),“ *Datenschutz Datensicherheit - DuD,* Bd. 37, S. 729, 2013.

[24] „PFS - Perfect Forward Secrecy,“ Elektronik Kompendium, [Online]. Available: https://bit.ly/3ewUv9f. [Zugriff am 2021 07 2021].

[25] E. Ahlers, „FAQ WLAN,“ 02 2019. [Online]. Available: https://bit.ly/3igX2Fw. [Zugriff am 04 07 2021].

[26] „What are Protected Management Frames?,“ WiFi-Alliance, [Online]. Available: https://bit.ly/3exaLXQ. [Zugriff am 04 07 2021].

[27] „WPA3 Specifications v3.0,“ WiFi-Alliance, [Online]. Available: https://bit.ly/3ipyHgI. [Zugriff am 04 07 2021].

[28] „The Wi-Fi security evolution,“ WiFi-Alliance, 04 2021. [Online]. Available: https://bit.ly/2UgGjKG. [Zugriff am 04 07 2021].

[29] „WPA3 Security Considerations November 2019,“ WiFi-Alliance, 11 2019. [Online]. Available: https://bit.ly/3zauZyw. [Zugriff am 04 07 2021].

[30] M. Rohr, Sicherheit von Webanwendungen in der Praxis, 2. Auflage Hrsg., Wiesbaden: Springer Vieweg, 2018.

[31] „What made Samsung S4 such a popular mobile phone.,“ RAPIDphonebuyer, [Online]. Available: https://bit.ly/3wL48Yc. [Zugriff am 15 07 2021].

[32] „WPA3 design issues and implementation vulnerabilities in hostapd and wpa_supplicant,“ CERT, 04 2019. [Online]. Available: https://bit.ly/3wLptR9. [Zugriff am 15 07 2021].

[33] „Anzahl der in Gebrauch befindlichen Smartphones weltweit in den Jahren 2019 und 2020 und Prognose bis 2022,“ Statista, 04 2021. [Online].

Available: https://bit.ly/3rtebQp. [Zugriff am 22 07 2021].

[34] „Marktanteile der mobilen Betriebssysteme am Absatz von Smartphones in Deutschland von Januar 2012 bis März 2021," Statista, 05 2021. [Online]. Available: https://bit.ly/3BvrhBg. [Zugriff am 22 07 2021].

[35] „App Store Support," Apple, 06 2021. [Online]. Available: https://apple.co/3eOaFLA. [Zugriff am 22 07 2021].

[36] „Anteile der verschiedenen Android-Versionen an der Internetnutzung von Geräten mit Android OS weltweit im April 2021," Statista, 04 2021. [Online]. Available: https://bit.ly/3wU2ByR. [Zugriff am 22 07 2021].

Abbildungsverzeichnis

Tabellenverzeichnis

Verzeichnis der wichtigen Abkürzungen

AAA	Authentifizierung, Autorisierung und Accounting
ACK	Acknowledge
AES	Advanced Encryption Standard
AP	Access Point
ARP	Address Resolution Protocol
BSS	Basic Service Set
CBC-MAC	Cipher Block Chaining Message Authentication Code
CCMP	Counter-Mode/CBC-MAC Protocol
CERT	Computer Emergency Response Team
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DoS	denial-of-service
DREAD	Damage Potential, Reproducibility, Exploitability, Affected Users, Discoverability
EAP	Extensible Authentication Protocol, Extensible Authentication Protocol
EAPOL	Extensible Authentication Protocol Over LAN
ECC	Elliptic Curve Cryptography
FIRST	Forum of Incident Response and Security Teams
FS	Forward Secrecy
GMK	Group Master Key
GTK	Group Transient Key
IDS	Intrusion Detecion System
IEEE	Institute of Electrical and Electronics Engineers
KRACK	Key Reinstallation AttaCK
LDAP-Server	Lightweight Directory Access Protocol
MIC	Message Integrity Code
NIAC	National Infrastructure Advisory Council
NIST	National Institute of Standards and Technology
Nonce	Number used once
OUI	Organizationally Unique Identifier
PFS	Perfect Forward Secrecy, Perfect Forward Secrecy
PMF	Protected Management Frames
PMK	Pairwise Master Key
PSK	Pre-Shared Key
PTK	Pairwise Transient Key
RADIUS	Remote Authentication Dial In User Service
RSNE	Robust Security Network Element
SAE	Simultaneous Authentication of Equals
S-Box	Substitutionsbox
SSH	Secure Shell
SSID	Service Set Identifier, Service Set Identifier
SSO	Single Sign-on
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security

TUFU	trust-on-first-use
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Networ*k*
WPA	Wi-Fi Protected Access

Anlagenverzeichnis

Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbständig verfasst und keine anderen als die angegebenen Hilfsmittel benutzt habe.
Die Stellen der Arbeit, die anderen Quellen im Wortlaut oder dem Sinn nach entnommen wurden, sind durch Angaben der Herkunft kenntlich gemacht. Dies gilt auch für Zeichnungen, Skizzen, bildliche Darstellungen sowie für Quellen aus dem Internet.

Ich erkläre ferner, dass ich die vorliegende Arbeit in keinem anderen Prüfungsverfahren als Prüfungsarbeit eingereicht habe oder einreichen werde.

Die eingereichte schriftliche Fassung entspricht der auf dem Medium gespeicherten Fassung.

Ort, Datum (Unterschrift)

Anlage 1 - Konfigurationen Router

FRITZ!Box SL WLAN

Funkeinstellungen

Hier können Sie die Einstellungen für das kabellose Funknetz (WLAN) vornehmen.

☑ WLAN aktivieren

Funkkanal auswählen: Kanal 6

Name des Funknetzes (SSID): WPA-PSK

☑ Name des Funknetzes (SSID) bekannt geben

Sendeleistung: 100 %

Modus: g + b

WLAN Sicherheit

Geben Sie an, wie das Funknetzwerk gegen unberechtigte Nutzung und Abhören gesichert wird.

○ **unverschlüsselten Zugang aktivieren**
○ **WEP-Verschlüsselung aktivieren**
◉ **WPA-Verschlüsselung aktivieren**

WPA-Verschlüsselung

Legen Sie fest, mit welchem Kennwort WLAN-Verbindungen gesichert werden. Das Kennwort muss zwischen 8 und 63 Zeichen lang sein und darf Buchstaben und Ziffern enthalten. Die Groß-/Klein-Schreibung wird berücksichtigt.

WPA Modus: WPA2 (CCMP)

WPA-Netzwerkschlüssel: **********

Synology MR2200ac

WPA3-Personal

Name (SSID):	WPA3_pers	Anzeigen
Sicherheitsstufe:	WPA3-Personal	
Passwort:		
Drahtlos-Modus:	b + g + n	
Kanal:	Kanal 3	

☐ USB 3.0-Gerät herabstufen, um Störungen bei 2,4 GHz Signal zu reduzieren

Standardoptionen

Schlüsselrotation:	3600	Sekunden
Kanalbreite:	20/40MHz	
PMF-Support:	Aktiviert - Erforderlich	
Übertragungsleistung:	Hoch	

WPA3-Personal Transition

Name (SSID):	WPA3_transition	Anzeigen
Sicherheitsstufe:	WPA2/WPA3-Personal	
Passwort:		
Drahtlos-Modus:	b + g + n	
Kanal:	Kanal 3	

☐ USB 3.0-Gerät herabstufen, um Störungen bei 2,4 GHz Signal zu reduzieren

Standardoptionen

Schlüsselrotation:	3600	Sekunden
Kanalbreite:	20/40MHz	
PMF-Support:	Aktiviert - Optional	
Übertragungsleistung:	Hoch	

WPA3-Enterprise

Name (SSID):	WPA3_ent	Anzeigen
Sicherheitsstufe:	WPA3-Enterprise	

Daten für Authentifizierungsserver eingeben

IP-Adresse:	192.168.25.202
Portnummer:	1812
Geteiltes Geheimnis:	••••••••••
Drahtlos-Modus:	b + g + n
Kanal:	Kanal 3

☐ USB 3.0-Gerät herabstufen, um Störungen bei 2,4 GHz Signal zu reduzieren

^ Standardoptionen

Schlüsselrotation:	3600	Sekunden
Kanalbreite:	20/40MHz	
PMF-Support:	Aktiviert - Erforderlich	
Übertragungsleistung:	Hoch	

Anlage 2 - Downgrade Clients

Originärer Access-Point

```
1 …  Synology_ce:6d:36  Broadcast          802.11   325  Beacon frame, SN=736, FN=0, Flags=........, BI=100, SSID=WPA3_transition

  Tag: RSN Information
      Tag Number: RSN Information (48)
      Tag length: 24
      RSN Version: 1
    > Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
      Pairwise Cipher Suite Count: 1
    > Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
      Auth Key Management (AKM) Suite Count: 2
    v Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) PSK 00:0f:ac (Ieee 802.11) SAE (SHA256)
      > Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) PSK
      > Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) SAE (SHA256)
    v RSN Capabilities: 0x008c
        .... .... .... ...0 = RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
        .... .... .... ..0. = RSN No Pairwise capabilities: Transmitter can support WEP default key 0 simultaneously with Pairwise key
        .... .... .... 11.. = RSN PTKSA Replay Counter capabilities: 16 replay counters per PTKSA/GTKSA/STAKeySA (0x3)
        .... .... ..00 .... = RSN GTKSA Replay Counter capabilities: 1 replay counter per PTKSA/GTKSA/STAKeySA (0x0)
        .... .... .0.. .... = Management Frame Protection Required: False
        .... .... 1... .... = Management Frame Protection Capable: True
        .... ...0 .... .... = Joint Multi-band RSNA: False
        .... ..0. .... .... = PeerKey Enabled: False
        ..0. .... .... .... = Extended Key ID for Individually Addressed Frames: Not supported
```

Fraudulenter Access-Point

```
557  39.267303  Raspberr_49:de:9b  Broadcast  802.11   216  Beacon frame, SN=1652, FN=0, Flags=........, BI=100, SSID=WPA3_transition

  > Multicast Cipher Suite: 00:50:f2 (Microsoft Corp.) TKIP
    Unicast Cipher Suite Count: 2
  v Unicast Cipher Suite List 00:50:f2 (Microsoft Corp.) AES (CCM) 00:50:f2 (Microsoft Corp.) TKIP
    > Unicast Cipher Suite: 00:50:f2 (Microsoft Corp.) AES (CCM)
    > Unicast Cipher Suite: 00:50:f2 (Microsoft Corp.) TKIP
    Auth Key Management (AKM) Suite Count: 1
  v Auth Key Management (AKM) List 00:50:f2 (Microsoft Corp.) PSK
    v Auth Key Management (AKM) Suite: 00:50:f2 (Microsoft Corp.) PSK
        Auth Key Management (AKM) OUI: 00:50:f2 (Microsoft Corp.)
        Auth Key Management (AKM) type: PSK (2)
```

Samsung Galaxy S4

Verbindung zu originären AP

```
34 … MurataMa_08:4f:73 Synology_ce:6d:36  EAPOL   155 Key (Message 2 of 4)

  Tag: RSN Information
    Tag Number: RSN Information (48)
    Tag length: 20
    RSN Version: 1
    Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
    Pairwise Cipher Suite Count: 1
    Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
    Auth Key Management (AKM) Suite Count: 1
    Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) PSK
      Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) PSK
        Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
        Auth Key Management (AKM) type: PSK (2)
    RSN Capabilities: 0x0000
      .... .... .... ...0 = RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
      .... .... .... ..0. = RSN No Pairwise capabilities: Transmitter can support WEP default key 0 simultaneously with Pairwise key
      .... .... .... 00.. = RSN PTKSA Replay Counter capabilities: 1 replay counter per PTKSA/GTKSA/STAKeySA (0x0)
      .... .... ..00 .... = RSN GTKSA Replay Counter capabilities: 1 replay counter per PTKSA/GTKSA/STAKeySA (0x0)
      .... .... .0.. .... = Management Frame Protection Required: False
      .... .... 0... .... = Management Frame Protection Capable: False
      .... ...0 .... .... = Joint Multi-band RSNA: False
      .... ..0. .... .... = PeerKey Enabled: False
      ..0. .... .... .... = Extended Key ID for Individually Addressed Frames: Not supported
```

Verbindung zum fraudulenten AP

```
5… … 56:4b:f0:0a:96:6d Raspberr_49:de:9b  EAPOL   159 Key (Message 2 of 4)

  Tag: Vendor Specific: Microsoft Corp.: WPA Information Element
    Tag Number: Vendor Specific (221)
    Tag length: 24
    OUI: 00:50:f2 (Microsoft Corp.)
    Vendor Specific OUI Type: 1
    Type: WPA Information Element (0x01)
    WPA Version: 1
    Multicast Cipher Suite: 00:50:f2 (Microsoft Corp.) TKIP
    Unicast Cipher Suite Count: 1
    Unicast Cipher Suite List 00:50:f2 (Microsoft Corp.) AES (CCM)
    Auth Key Management (AKM) Suite Count: 1
    Auth Key Management (AKM) List 00:50:f2 (Microsoft Corp.) PSK
      Auth Key Management (AKM) Suite: 00:50:f2 (Microsoft Corp.) PSK
        Auth Key Management (AKM) OUI: 00:50:f2 (Microsoft Corp.)
        Auth Key Management (AKM) type: PSK (2)
```

iPhone 12

Verbindung zu originären AP

```
… 56:4b:f0:0a:96:6d Synology_ce:6d:36  EAPOL    173 Key (Message 2 of 4)

  Tag: RSN Information
    Tag Number: RSN Information (48)
    Tag length: 38
    RSN Version: 1
  > Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
    Pairwise Cipher Suite Count: 1
  > Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
    Auth Key Management (AKM) Suite Count: 1
  v Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) SAE (SHA256)
    v Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) SAE (SHA256)
        Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
        Auth Key Management (AKM) type: SAE (SHA256) (8)
  v RSN Capabilities: 0x00cc
      .... .... .... ...0 = RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
      .... .... .... ..0. = RSN No Pairwise capabilities: Transmitter can support WEP default key 0 simultaneously with Pairwise key
      .... .... .... 11.. = RSN PTKSA Replay Counter capabilities: 16 replay counters per PTKSA/GTKSA/STAKeySA (0x3)
      .... .... ..00 .... = RSN GTKSA Replay Counter capabilities: 1 replay counter per PTKSA/GTKSA/STAKeySA (0x0)
      .... .... .1.. .... = Management Frame Protection Required: True
      .... .... 1... .... = Management Frame Protection Capable: True
      .... ...0 .... .... = Joint Multi-band RSNA: False
      .... ..0. .... .... = PeerKey Enabled: False
      ..0. .... .... .... = Extended Key ID for Individually Addressed Frames: Not supported
    PMKID Count: 1
  v PMKID List
      PMKID: a310f2ff7e9747cd73425f4fad9d91c6
```

Verbindung zum fraudulenten AP

```
56:4b:f0:0a:96:6d Raspberr_49:de:9b  EAPOL    159 Key (Message 2 of 4)

  v Tag: Vendor Specific: Microsoft Corp.: WPA Information Element
      Tag Number: Vendor Specific (221)
      Tag length: 24
      OUI: 00:50:f2 (Microsoft Corp.)
      Vendor Specific OUI Type: 1
      Type: WPA Information Element (0x01)
      WPA Version: 1
    > Multicast Cipher Suite: 00:50:f2 (Microsoft Corp.) TKIP
      Unicast Cipher Suite Count: 1
    > Unicast Cipher Suite List 00:50:f2 (Microsoft Corp.) AES (CCM)
      Auth Key Management (AKM) Suite Count: 1
    v Auth Key Management (AKM) List 00:50:f2 (Microsoft Corp.) PSK
      v Auth Key Management (AKM) Suite: 00:50:f2 (Microsoft Corp.) PSK
          Auth Key Management (AKM) OUI: 00:50:f2 (Microsoft Corp.)
          Auth Key Management (AKM) type: PSK (2)
```