# Historie und Technologie von WLAN-Standards der IEEE 802.11-Familie in Hinblick auf Angriffsszenarien

Eldin Sabanovic

Hochschule RheinMain, Unter den Eichen 5, 65195 Wiesbaden, Deutschland
eldin.sabanovic@student.hs-rm.de

**Abstract.** In diesem Paper soll die Geschichte, Technologie und Entwicklung der IEEE 802.11-Familie in Bezug auf Angriffsszenarien zusammengefasst werden. Einleitend wird der 802.11-Standard vorgestellt. Hierbei soll anfangs eine Begriffserklärung stattfinden, darauf folgend Informationen über den ersten 802.11-Standard und weshalb dieser in der nicht-kommerziellen, sowie kommerziellen Nutzung eine schnelle Verbreitung erfuhr. Es wird im weiteren auf die technischen Merkmale eingegangen. Dazu gehören die OSI-Schicht und die vereinfachte Migration in bereits bestehende Ethernet-Netzwerke (durch Zugehörigkeit zur "IEEE 802"-Familie). Nach der Einleitung wird mit WEP der erste Versuch einer sicheren Kommunikation beleuchtet, mit Blick auf die Funktion und der dort festgestellten Schwachstellen. Weiter wird auf die in der nächsten Generation durch WPA getroffene Schutzmaßnahmen, mit Hinblick auf die Schwachstellen von WEP eingegangen. Weiter wird Bezug auf die in dieser Generation gefundene Schwachstelle, in einem Feature, im 802.11e-Standard genommen. Danach wird ein genauer Einblick in in die Sicherheitsmaßnahmen von WPA2 genommen. Besonderer Blick liegen auf dem AES-CCMP-Verfahren, folgend eine Auflistung der weiteren Authentifizierungsmöglichkeiten und daraus resultierender Schwachstellen. Da in dieser Generation verschiedene neue Angriffsmethoden, abseits vom Jamming und dem Abhören entwickelt wurden, wird ein genauer Einblick auf verschiedene Angriffsmethoden gegeben und wie diese einen sicheren Betrieb gefährden können. Im weiteren soll WPS kurz vorgestellt werden, worauf dann ein genauer Blick auf die nachfolgende Generation WPA3 folgen soll.

**Keywords:** IEEE-802.11 · WPA2 · Schutzmaßnahmen.

# 1 Einleitung zum 802.11-Standard

Unter 802.11 wird eine Gruppe von Funknetz-Standards, basierend auf dem IEEE 802-Standard bezeichnet. Herausgegeben werden diese durch das Institute of Electrical and Electronic Engineers, kurz "IEEE". Die erste Version wurde im Jahr 1997 veröffentlicht. In dieser wurde der Medienzugriff, sowie die physische Schicht zur Implementierung von Funknetzwerken in verschiedenen Frequenzbändern, wie 2.4 GHz, 5 GHz und 60 GHz, definiert.

Vor dem Jahr 1997 wurden lokale Funknetzwerke selten genutzt. Dies lang an der der fehlenden Standardisierung, der geringen Datenrate, hoher Störanfälligkeit (Fernseher, Kühlschränke, etc.), sowie den geringen Hürden für das mitschneiden von Datenübertragungen.

Durch die Standardisierung, die Protokoll-Transparenz und die fortlaufende Entwicklung des 802.11-Standard haben Funknetzwerke eine weite Verbreitung gefunden und im privaten, sowie teilweise im kommerziellen Umfeld, einen Großteil der kabelgebundenen Netzwerke abgelöst.

## 1.1 Architektur

IEEE 802.11 wurde dahingehend entwickelt, dass Netzwerke den Großteil der Entscheidungen dem Netzwerk-Teilnehmern überlassen. Diese Art der Architektur hat verschiedene Vorteile. Das Netzwerk ist zum einen fehlertolerant, zum anderen treten keine Engpässe auf, wie sie bei einer zentralisierten Architektur auftreten könnten [9]. Durch diese Strukturvorteile ist die Architektur flexibel genug, um sowohl kleine Netzwerke (Heimnetzwerk), als auch große semipermanente (Messe-Netzwerke) oder permanente Netzwerke (Unternehmen) problemlos zu unterstützen.

Zwei Netzwerk-Arten sind im 802.11-Standard definiert:

**Ad-hoc-Netzwerke:** Ein Ad-hoc-Netzwerk wird zur Kommunikation zwischen mehrerer Teilnehmer verwendet. In der Regel wird wird diese Netzwerkart spontan erstellt, um Dateien mit geringer Dateigröße zu übertragen. Ad-hoc-Netzwerke benötigen keine Basisstation zum verbinden und unterstützen keinen Zugriff auf kabelgebundene Architektur.

**Infrastruktur-Netzwerke:** Ein Infrastruktur-Netzwerk wird zur Kommunikation zwischen drahtlosen und kabelgebundenen Teilnehmern genutzt. Die Übertragung von drahtlosen zu kabelgebundenen Teilnehmern erfolgt über eine Basisstation.

### 1.2 Kollisionsvermeidung (CSMA/CA)

"Carrier-sense multiple access with collision avoidance", kurz CSMA/CA ist eine Standardmethode welche die Kommunikation mehrerer Teilnehmer auf einem gemeinsam genutzten und dezentralen Übertragungsmedium steuert.

Grundlegend teilt sich die Methode in folgende Teilkomponenten auf:

**Carrier sense (CS):** Daten dürfen nur versendet werden, wenn das jeweilige Übertragungsmedium (z.b. ein Netzwerkadapter) verfügbar ist.

**Multiple access (MA):** Alle Teilnehmer müssen sich auf ein Protokoll zur Kommunikationssteuerung einigen, um eine faire Verteilung zu gewährleisten.

**Collision avoidance (CA):** Es wird ein Scheduling-Algorithmus genutzt, um Kollisionen zwischen zwei oder mehreren Teilnehmern zu vermeiden.

## 2 WEP

WEP ist ein Verschlüsselungsprotokoll welches zusammen mit dem ersten 802.11-Standard im Jahr 1997 veröffentlicht wurde. Es sollte zum einen den Zugriff der Nutzer steuern, als auch die übertragenen Daten schützen, hinsichtlich Vertraulichkeit und Integrität [3]. Im Jahr 2003 wurde ein Paper veröffentlicht, welches verschiedene Schwachstellen in der Verwendung des RC4-Algorithmus aufzeigte und die Sicherheit des Protokolls nicht mehr gewährleistete [10]. In diesem Kapitel wird nur auf das brechen der Verschlüsselung einer Nachricht eingegangen.

### 2.1 Design der Nachrichtenübertragung

Im WEP-Protokoll findet die Verschlüsselung einer Nachricht über eine einfache XOR-Verknüpfung statt. Benötigt werden ein RC4-Keystream [4], sowie eine Nachricht verknüpft mit ihrem jeweiligen CRC-Hashwert. Zur Erzeugung eines Keystreams, werden der WEP-Schlüssel, sowie ein 24-Bit langer Initialisierungsvektor miteinander verknüpft, wobei zu jeder Nachricht ein neuer Initialisierungsvektor generiert werden muss. Weiter wird die zu übertragende Nachricht mit ihrem jeweiligen CRC-Hash verknüpft. Im nächsten Schritt werden der Keystream und die Nachricht XOR-verknüpft. Als Ergebnis erhält man einen Ciphertext, an dem man noch den jeweiligen Initialisierungsvektor anhängen muss. Die Nachricht ist daraufhin bereit zur Übertragung.

Zur Entschlüsselung werden ein Ciphertext mit dem Initialisierungsvektor und der WEP-Schlüssel des Netzwerks benötigt. Der Initialisierungsvektor und der WEP-Schlüssel werden wie bei der Verschlüsselung in einen RC4-Algorithmus

eingegeben. Da dieser bei gleicher Eingabe immer die gleichen Ausgaben ausgibt, muss nur noch der Ciphertext mit dem Keystream XOR-verknüpft werden. Als Ergebnis erhält man den CRC-Hashwert, sowie die entschlüsselte Nachricht. Optional kann noch eine Integritätsprüfung durchgeführt werden, indem ein neuer CRC-Hashwert der Nachricht erstellt wird und mit dem vorliegenden CRC-Hashwert verglichen wird.

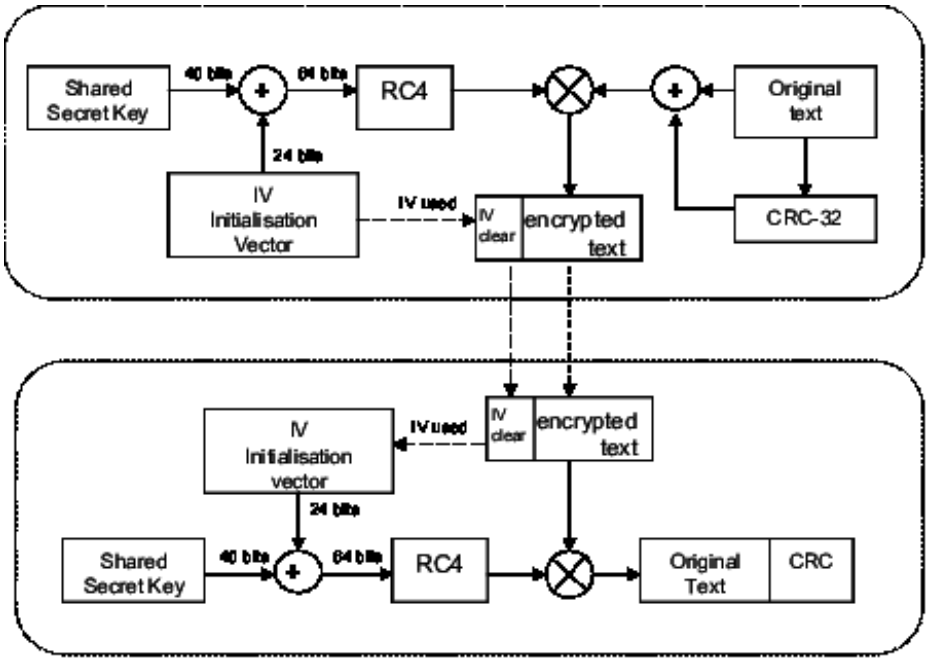


**Fig. 1.** Im oberen Teil der Abbildung wird das Verschlüsseln einer Nachricht dargestellt. im unteren Teile das Entschlüsseln.

### 2.2 Vorstellung der wichtigsten Schwachstellen

Die meisten Angriffsarten auf WEP-Netzwerke erfordern, dass mindestens ein Nutzer aktiv Netzwerkverkehr erzeugt. Eine Schwachstelle ist der Initialisierungsvektor. Zum einen ist eine Größe von 24-Bit zu gering gewählt, als dass es für kryptographische Zwecke ausreichen würde [13]. Zum anderen wird ebendieser Vektor im Klartext an den Ciphertext angehangen, was den RC4-Algorithmus schwächt. Da von jedem Datenpaket 24 Bit direkt ablesbar sind, kombiniert mit den Schwächen der RC4-Implementierung, lässt sich mit relativ wenig abgefangenem Netzwerkverkehr, sowie wenig Rechenzeit der WEP-Schlüssel zurückberechnen [6]. Dies führt dazu, dass sich unautorisierte Nutzer Zugang in gesicherte Bereiche verschaffen könnten. Auch ist es eine Schwachstelle, dass der Initialisierungsvek-

tor durch den Nutzer wiederverwendet werden kann. Es findet keine Prüfung statt, ob der Vektor bereits verwendet wurde, was dazu führt, dass statische Keystreams erstellt werden und damit die Sicherheit der Nachrichten weiter verringern. Weiter können Hersteller, Hintertüren in ihre Firmwares einbauen, welche bei Interesse durch eine Strafverfolgungsbehörde die Sicherheit des Netzwerks signifikant verringern können, indem sie den Initialisierungsvektor als statisch deklarieren. Eine weitere Schwachstelle sind nicht-verschlüsselte CRC-Hashwerte, welche die Integrität der Nachricht nicht zuverlässig nachweisen können, da diese manipulierbar sind.

## 3 WPA

Nachdem verschiedene Schwachstellen im WEP-Verschlüsselungsprotokoll veröffentlicht wurden und sich die Fertigstellung des neuen Standards IEEE-802.11i verzögerte, wurden nicht benötigte Neuerungen entfernt und WPA als neuer Pseudostandard vorgestellt [14]. Dieser sollte eine Zwischenlösung darstellen. Die Veröffentlichung und Zertifizierung fand im Jahr 2003 statt.

Grundlegend hat sich an der Verschlüsselungsarchitektur nichts verändert. Es wurden lediglich dynamische Schlüssel, welche auf dem Temporal Key Integrity Protocol (TKIP) basieren hinzugefügt. Außerdem wurden "Pre-shared keys" (PSK) oder das "Extensible Authentication Protocol" (EAP) zur Authentifizierung von Teilnehmern angeboten. Weitere Neuerungen waren, dass der Initialisierungsvektor auf 48 Bit angehoben wurde, kein statischer WEP-Schlüssel genutzt wurde, sondern für jedes Datenpaket ein neuer Schlüssel generiert wurde. Zuletzt wurde noch ein Message Integrity Check (MIC) eingefügt, welcher eine fortlaufende Paketnummer verschlüsselt. Sollte ein Paket mit ungültiger Paketnummer empfangen werden, wird dies verworfen. Durch diese Neuerungen konnte ein Großteil der vorher möglichen Angriffe abgewehrt werden.

### 3.1 Schwachstellen

Eine Schwachstelle in WPA wären die "Pre-Shared-Keys". Hierbei ist auf die Stärke des Passworts zu achten. Einem Angreifer ist es möglich über eine "Brute Force"-Attacke oder einen Wörterbuchangriff das Passwort zu ermitteln. Hierbei generiert der Angreifer eine Liste von "Pre-Shared-Keys" und versucht sich mit jedem Schlüssel anzumelden. Da hierbei allerdings die Schuld beim Nutzer zu suchen ist und bei Herstellern die den Nutzer nicht auffordern das Standardpasswort zu ändern, ist dies zwar ein Sicherheitsrisiko, allerdings keines welches exklusiv dem WPA-Protokoll zuzuschreiben ist. Ein anderes Sicherheitsrisiko welches allerdings der Kompatibilität geschulden ist, ist dass WPA noch den RC4-Algorithmus genutzt hatte, welcher bereits bekannterweise anfällig auf "Known-Plaintext-Angriffe" war. Da WPA allerdings als Übergangslösung zu sehen war und bereits ein Jahr später (2004) der WPA2-Standard veröffentlicht wurde, ist das Risiko im Nachinein als gering einzustufen. Besonders da akut

gefährdete Einrichtungen dennoch die Möglichkeit zur (zeitweisen) Umstellung auf kabelgebundene Netzwerke hatten.

# 4 WPA2

Das "Wi-Fi Protected Access 2" wurde im Jahr 2004, als Nachfolger von WPA veröffentlicht. Im Gegensatz zu den beiden Vorgängern nutzt WPA den Verschlüsselungsstandard AES, sollte CCMP als Protokoll genutzt werden. Der Fokus auf die Kompatibilität zu vorher genutzter Hardware ist bei dieser Version nicht gegeben [1]. Dies wurde mit Fokus auf bessere Sicherheitsmaßnahmen begründet. Eine einfache Umstellung durch eine Firmware-Aktualisierung wäre zwar möglich, allerdings ist es wahrscheinlich, dass die meiste damalige Hardware zu wenig Rechenleistung geboten hätte, um mit der AES-Verschlüsselung umzugehen.

## 4.1 CCMP

"Counter Mode with Cipher Block Chaining Message Authentication Code Protocol", kurz CCMP, ist ein Protokoll welches in der 802.11i-Norm spezifiziert wurde. Es stellt Methoden zur Authentifizierung, Verschlüsselung und Integritätssicherung zur Verfügung. Es werden 48 Bit lange Initialisierungsvektoren, sowie 128 lange Schlüssel verwendet, basierend auf dem Advanced Encryption Standard.

## 4.2 Authentifizierung über RADIUS-Server

In WPA2 ist es möglich Authentifizierungsanfragen von einer Basisstation, an einen zentralen Authentifizierungsserver weiterzuleiten [2]. Hierbei prüft der "Remote Authentication Dial-In User Service", ob die Authentifizierung erfolgreich war oder nicht und leitet die Antwort an die jeweilige Basisstation zurück. Auch lässt sich der Zugang parametrisieren, sodass privilegierte Nutzer mehr Bandbreite erhalten (Bezahlkunden) oder auf bestimmte Domains zugreifen können (Nutzer-/Admin-Login).

Diese Zentralisierung hat das Sicherheitsrisiko, dass im Fall eines Datenabflussen durch Angreifer, große Mengen an Nutzerdaten zur Kompromittierung weiterer Infrastruktur genutzt werden können. Auch die Wahrscheinlichkeit eines Störfalls oder Sabotage, durch "Denial of Service"-Angriffe oder dem unbeabsichtigten Vergessen eines Backups, falls der Server getauscht werden soll, stellen Risiken dar. Weiter gibt es noch die Gefahr einer Misskonfiguration, sodass unberechtigte Nutzer, Zugang in geschützte Systembereiche bekommen könnten.

### 4.3 Angriffsmethoden

Trotz des hohen Sicherheitsstandards des WPA2-Protokolls sind verschiedene Arten von Angriffen möglich. Diese sind entweder durch das Design des WPA2-Protokolls möglich, zum anderen durch kreative Nutzung anderer Angriffe und "Social engineering"-Methoden.

**Deauthentifizierungsangriff:** Deauthentifizierungsangriffe gehören zur Familie der "Denial-of-service"-Angriffe. Der Angriffszweck besteht darin den Nutzer durch wiederholtes entfernen aus dem Netzwerk zu stören oder weitere Angriffe auf das Zielgerät vorzubereiten. Hierzu wird die MAC-Adresse des Zielgeräts, sowie der Basisstation benötigt. Der Angreifer sendet manipulierte Management-Frames an die Basisstation, um die Verbindung zu schließen. Dieser Angriff ist möglich, da Management-Frames in WPA2-Netzwerkes keine Verschlüsselung nutzen und damit gefälschte Nachrichten versendet und bearbeitet werden können. Gängige Tools für diesen Angriff wären "Aireplay-ng" und "Mdk3".

**Evil-Twin:** Ein "Evil Twin" bezeichnet ein Netzwerk welches einem vorher ausgewähltem Zielnetzwerk nachempfunden ist [5]. Hierbei wählt der Angreifer idealerweise die gleiche oder eine ähnliche SSID, wie beim Zielnetzwerk. Sollte das Zielnetzwerk die Authentifizierung über eine interne Domain verwalten, dann sollte diese bei einem gezielten Angriff kopiert/nachgebaut werden. Idealerweise hat das Netzwerk eine ähnliche Signalstärke, um eine maximal mögliche Vertrauenswürdigkeit auszustrahlen. Manche Angreifer starten am einem weiteren Netzwerkadapter einen Deauthentifizierungsangriff, um Opfer effektiver auf den "Evil Twin" zu locken. Ein bekanntes Tool für diesen Angriff wäre "Fluxion2".

**KRACK:** Der "Key Reinstallation Attack" ist eine im Jahr 2017 veröffentlichte Angriffsmethode, welche eine Schwachstelle im Vier-Wege-Handshake von WPA2-Netzwerks ausnutzt, um den ausgehandelten Schlüssel zwischen Nutzer und Basisstation zu erhalten [11]. Dadurch ist es möglich verschiedene Angriffe auszuführen, wie die Entschlüsselung und Manipulation des Netzwerkverkehrs. Der Angriffsvektor liegt in der clientseitigen Implementierung der 802.11s-Norm. Vorwiegend waren Unix-Geräte betroffen, Geräte mit Windows oder MacOS als Betriebssystem nur teilweise. Windows hat die Lücke eine Woche vor bekanntwerden geschlossen, im Rahmen eines "Responsible Disclosure".

## 5 WPS

"Wi-Fi Protected Setup" ist ein im Jahr 2007 veröffentlichter Standard, um Nutzern mit wenig Sachkenntnis eine einfache Möglichkeit zu bieten, neue Geräte in ihr Heimnetzwerk zu integrieren, ohne die Notwendigkeit ein langes Passwort einzugeben. Im Dezember 2011 wurde eine größere Schwachstelle entdeckt,

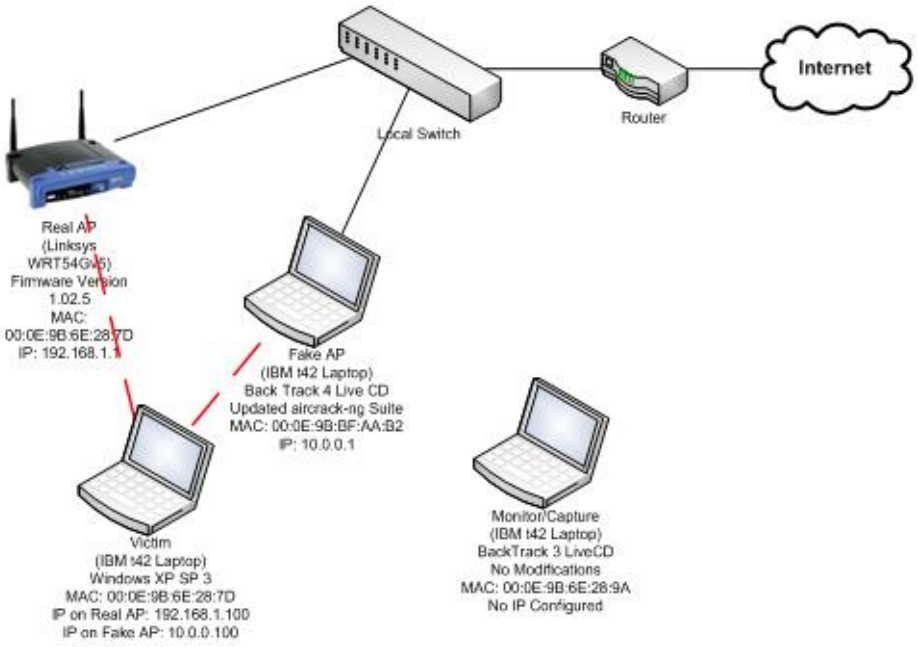


**Fig. 2.** Ein beispielhafter Evil-Twin-Angriff.

wodurch sich der WPS-Pin innerhalb weniger Stunden durch einen "Brute Force"-Angriff" berechnen ließ [8]. Hier wurde ausgenutzt, dass nach einem WPS-Verbin-dungsaufbau die ersten vier Ziffern an den Nutzer übertragen wurden. Nachdem die letzten vier Ziffer gefunden wurden war es daraufhin möglich den WPA/WPA2-Schlüssel im Klartext auszulesen. Als Reaktion sollten Administratoren eines Heimnetzwerks die WPS-Funktion deaktivieren. Fraglich ist, ob regelmäßige Nutzer dieser Funktion die Sachkenntnis hatten, um eine Abschaltung zu bewerkstelligen.

## 6 WPA3

"Wi-Fi Protected Access 3" ist ein, als Reaktion zum KRACK-Angriff, im Juni 2018 verabschiedeter Nachfolger von WPA2. Ziel dieses Standards soll es sein die Sicherung des Netzwerkverkehrs zu vereinfachen, sicherere Authentifizierungsmöglichkeiten einzuführen, sowie die Ausfallsicherheit von kritischer Netzwerken zu verbessern.

### 6.1 SAE - Simultaneous Authentication of Equals

In WPA3 wird zwischen zwei Netzwerkarten unterschieden [7]. Der "Personal-Mode" wurde für den privaten Gebrauch entwickelt, der "Enterprise-Mode"

hingegen für Firmen und größere Netzwerke. In diesem Modus teilt ein Admininistrator jedem Nutzer einen eigenen privaten Authentifizierungsschlüssel zu. Im "Personal-Mode" wurde das "Pre-shared Key"-Verfahren, kurz "PSK" welches häufig in WPA2-Personal-Netzwerken genutzt wurde, durch das "Simultaneous Authentication of Equals"-Verfahren, kurz "SAE" ausgetauscht. Mittels dieses Verfahrens soll die Sicherheit des Schlüsselaustausches bei einem Handshake erhöht werden. Hierbei wird wie in den vorherigen Wifi-Standards ein gemeinsam genutzter Schlüssel verwendet. Aus diesem wird für jede Verbindung ein sogenannter "Pairwise Master Key (PMK)" generiert. Dieser stellt sicher, dass selbst bei einer Kompromittierung des gemeinsamen Schlüssels, jede Klient-Router-Verbindung ihren eigenen Schlüssel besitzt und andere Verbindungen nicht kompromittiert werden können. Weiter werden aus dem PMK, "Pairwise Transient Keys (PTK)" abgeleitet, mit welchen der Netzwerkverkehr für die jeweilige Verbindung verschlüsselt wird.

### 6.2 PMF - Protected Management Frames

Unter "Protected Management Frames (PMF)" werden verschlüsselte Management-Frames bezeichnet. Diese wurden eingeführt, da im vorherigen WPA2-Standard, Angreifer die Möglichkeit hatten manipulierte Deassoziierungspakete zu verschicken. Hierdurch konnten Netzwerk-Teilnehmer abgemeldet und mitteils kostengünstiger Hardware dauerhaft in ihrer Nutzung gestört werden. Auch wurden Abmeldung oft zum Aufzeichnen des WPA-Handshakes herbeigeführt, um den gemeinsamen Schlüssel offline berechnen zu können.

### 6.3 DPP - Device Provisioning Protocol

Unter "Device Privisioning Protocol (DPP)" wird ein vereinfachter Verbindungsmechanismus bezeichnet, welcher seinen Fokus auf Internet-of-Things-Geräte (kurz: IoT-Gerät) legt. Hierbei wird mitteils vorher abgelegter Informationen in einem QR-Code, ein IoT-Gerät in einem Netzwerk angemeldet. Das Anmeldeverfahren benötigt eine App vom Routerhersteller, sowie ein Smartphone. Dieses scannt zuerst den QR-Code des Netzwerkes und danach den IoT-Gerätes und leitet daraufhin den Anmeldevorgang ein.

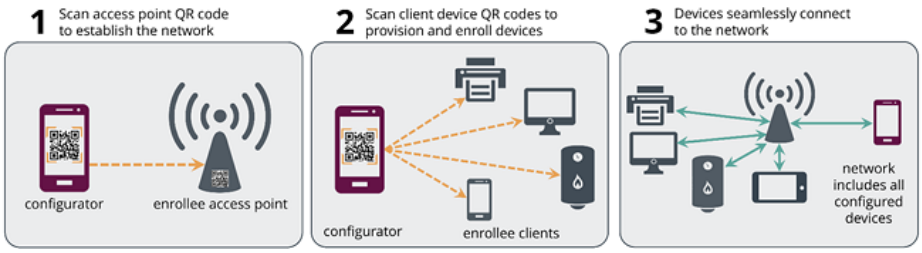


**Fig. 3.** Es wird die Anmeldung eines neuen Gerätes mittels des Device Provisioning Protocol veranschaulicht.

### 6.4 Schwachstellen

Am 10. April 2019 wurde ein wissenschaftliches Paper von Mathy Vanhoef und Eyal Ronen veröffentlicht [12]. In diesem wurden zahlreiche Design-Schwächen im SAE-Protokoll in WPA3 aufgedeckt. Insgesamt wurden fünf Schwachstellen entdeckt, welche als Gruppe unter dem Begriff "Dragonblood" bezeichnet werden. Es wurde entdeckt, dass durch Nutzung diversen Schwachstellen beim Schlüsselaustausch, unverschlüsselte Daten übertragen werden. Diese können dazu genutzt werden, um den gemeinsamen Schlüssel zu rekonstruieren. Weiter ist durch eine andere Schwachstelle ein Downgrade-Angriff möglich, wodurch bekannte Schwachstellen des WPA2-Handshakes genutzt werden können.

## References

[1] Paul Arana. "Benefits and vulnerabilities of Wi-Fi protected access 2 (WPA2)". In: *INFS* 612 (2006), p. 2.
[2] Paul Arana. "Benefits and vulnerabilities of Wi-Fi protected access 2 (WPA2)". In: *INFS* 612 (2006), p. 1.
[3] Kai-Oliver Detken and Evren Eren. "WLAN-Sicherheit–von WEP bis CCMP". In: *D* A* CH Security, Klagenfurt* (2006), p. 6.
[4] Kai-Oliver Detken and Evren Eren. "WLAN-Sicherheit–von WEP bis CCMP". In: *D* A* CH Security, Klagenfurt* (2006), p. 4.
[5] Matthias Ghering and Erik Poll. "Evil Twin vulnerabilities in Wi-Fi networks". In: (2016), p. 1.
[6] Vishal Kumkar et al. "Vulnerabilities of Wireless Security protocols (WEP and WPA2)". In: *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)* 1.2 (2012), p. 36.
[7] B Indira Reddy and V Srikanth. "Review on Wireless Security Protocols (WEP, WPA, WPA2 & WPA3)". In: (2019), p. 29.
[8] AMIRMOHAMMAD Sadeghian. "Analysis of WPS Security in Wireless Access Points". In: *6th International Conference on Security for Information Technology and Communications (SECITC 2013)*, p. 3.
[9] Philipp Stephan. *Wireless LAN 802.11*. 2003.
[10] Adam Stubblefield, John Ioannidis, Aviel D Rubin, et al. "Using the Fluhrer, Mantin, and Shamir Attack to Break WEP." In: *NDSS*. 2002, p. 1.
[11] Mathy Vanhoef and Frank Piessens. "Key reinstallation attacks: Forcing nonce reuse in WPA2". In: *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. 2017, p. 1.
[12] Mathy Vanhoef and Eyal Ronen. "Dragonblood: A Security Analysis of WPA3's SAE Handshake." In: *IACR Cryptology ePrint Archive* 2019 (2019), p. 383.
[13] Stanley Wong. "The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards". In: *SANS Institute* (2003), p. 2.
[14] Stanley Wong. "The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards". In: *SANS Institute* (2003), p. 4.