WPA2 war gestern – WPA3, Enhanced Open, und andere WLAN Erweiterungen

Max Riegel

2018-11-23

Ankündigung

- **WPA2 war gestern; WPA3, Enhanced Open, und andere WLAN Erweiterungen**

  Die Wi-Fi Alliance hat vor kurzem wesentliche Verbesserungen bei den WLAN Sicherheitsmethoden bekannt gegeben, die vor allem bei der nächsten Generation von WLAN zum Einsatz kommen soll. Der Vortrag stellt die neuen Funktionalitäten vor und gibt auch einen Überblick über die Verbesserungen, die in die nächste Generation von WLAN einfließen werden.

.

Inhaltsübersicht

- WLAN Standardisierung
- WLAN Sicherheit aktuell
- WPA3
- Enhanced Open
- Ein Blick in die Zukunft
- Generational Wi-Fi

WPA3, Enhanced Open, und andere WLAN Erweiterungen

WLAN STANDARDISIERUNG

IEEE 802.11 und Wi-Fi Alliance

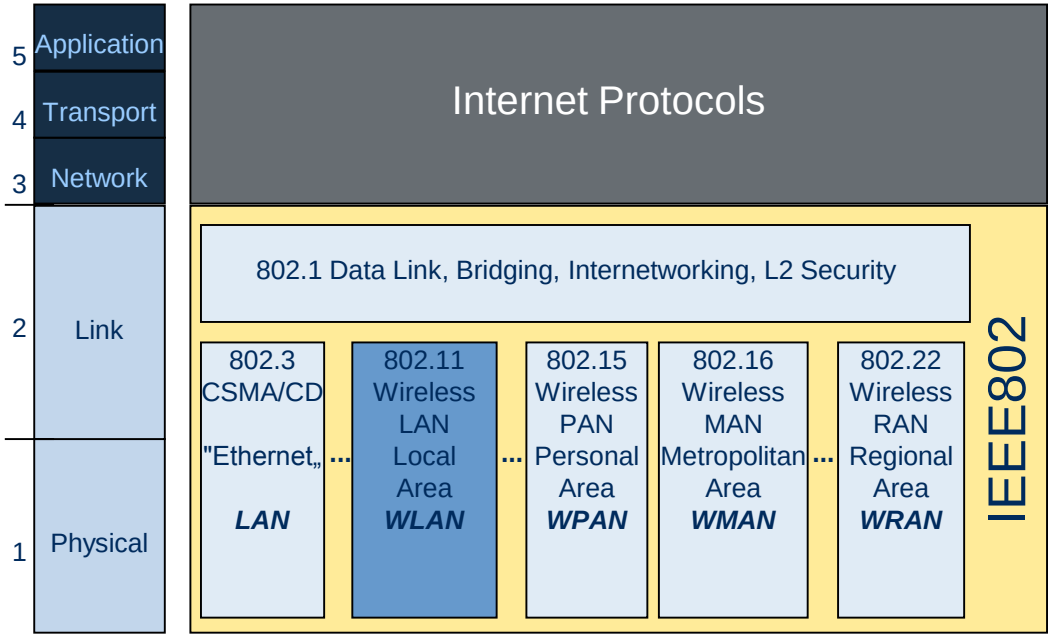
Die IEEE 802.11 ist eine Arbeitsgruppe des IEEE, die die technischen Spezifikationen erstellt.

Standards

Die Wi-Fi Alliance definiert Profile für den IEEE 802.11 Standard um Geräte zu zertifizieren.

Zusammenspiel
Konformität

Die IEEE 802 LAN/MAN Standardisierung



Die IEEE 802 spezifiert nur die DataLink und Physical Schicht für IP Protokolle.

- **Start des IEEE Computer Society Projekts 802 im Februar 1980.**
  - Später umbenannt in “LMSC”: LAN/MAN Standardization Committee
- **Beginn mit “Ethernet” mit 1 bis 20 Mbps**
- **IEEE 802.11 begann in 1990**
  - Ursprünglich gedacht um Registrierkassen zu vernetzen!
  - Schwierige rechtliche Fragen!
- **Weitere Gruppen, z.B. 802.15, 802.16 kamen später hinzu.**
- **Gemeinsamkeiten:**
  - Gleichartige LinkLayer Funktionalitäten
  - Gleichartige Paketstrukturen.

Die Zertifizierung der Wi-Fi Alliance

Wi-Fi CERTIFIED Geräte müssen in der Lage sein mit anderen Wi-Fi CERTIFIED Geräten gut zusammen-zuarbeiten, wenn Anwendungen in Alltagssituationen betrieben werden.

Interoperability

Strenge Testmethoden werden eingesetzt um nachzuweisen, dass Produkte ver-schiedener Hersteller zusammenarbeiten.

Backward Compatibility

Rückwärtskompatibilität sichert die Wertbeständigkeit von Geräten und erlaubt eine graduelle Erneuerung und Aufrüstung.

Innovation

Zeitnahe Einführung neuer Zertifizierungs-programme wenn neue Spezifikationen verfügbar werden. Hersteller sind in der Lage ihre Produkte bei Merkmalen zu differentieren, die nicht der Zertifizierung unterliegen.

WPA3, Enhanced Open, und andere WLAN Erweiterungen

WLAN SICHERHEIT AKTUELL

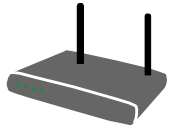
WLAN Sicherheitsverfahren

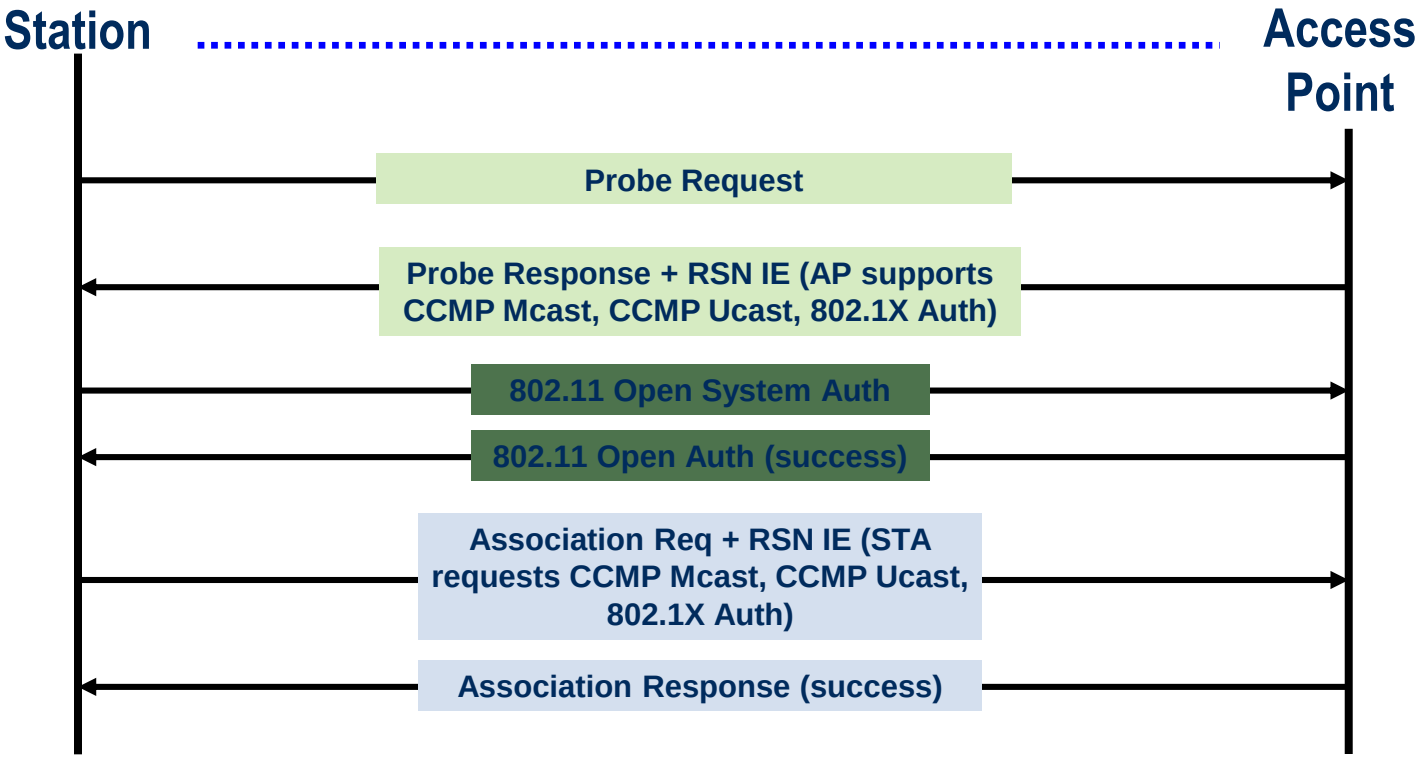
Sicherheitsmerkmal	Manual WEP	Dynamic WEP	TKIP (RSN)	CCMP (RSN)
Verschlüsselungs-Algorithmus	RC4	RC4	RC4	AES
Schlüssellänge	40bit oder 104bit (Verschlüsselung)	40bit oder 104bit (Verschlüsselung)	128bit (Verschlüsselung) 64bit (Integritätsschutz)	128bit (Verschlüsselung und Integritätsschutz)
Paketschlüssel	Erzeugt durch Verbindung von WEP Schlüssel und 24bit IV	Von EAP Authentisierung abgeleitet	Durch TKIP Verarbeitung erstellt	Nicht notwendig, da Arbeitsschlüssel ausreichend sicher
Integritätsschutz	Verschlüsselter CRC-32	Verschlüsselter CRC-32	Michael Message Integrity Check (MIC)	CCM
Header-Schutz	Nein	Nein	Quell- und Zieladdresse durch MIC geschützt	Src and Dest addresses protected by CCM
Wiederholungsschutz	Nein	Nein	Durch IV Sequenz sichergestellt	Durch IV Sequenz sichergestellt
Authentisierung	Open system oder Shared key	EAP Methode über IEEE 802.1X	PSK oder EAP Methode über IEEE 802.1X	PSK oder EAP Methode über IEEE 802.1X
Schlüsselverteilung	Manuell	IEEE 802.1X	Manuell / IEEE 802.1X	Manuell / IEEE 802.1X

Robust Security Network (RSN)

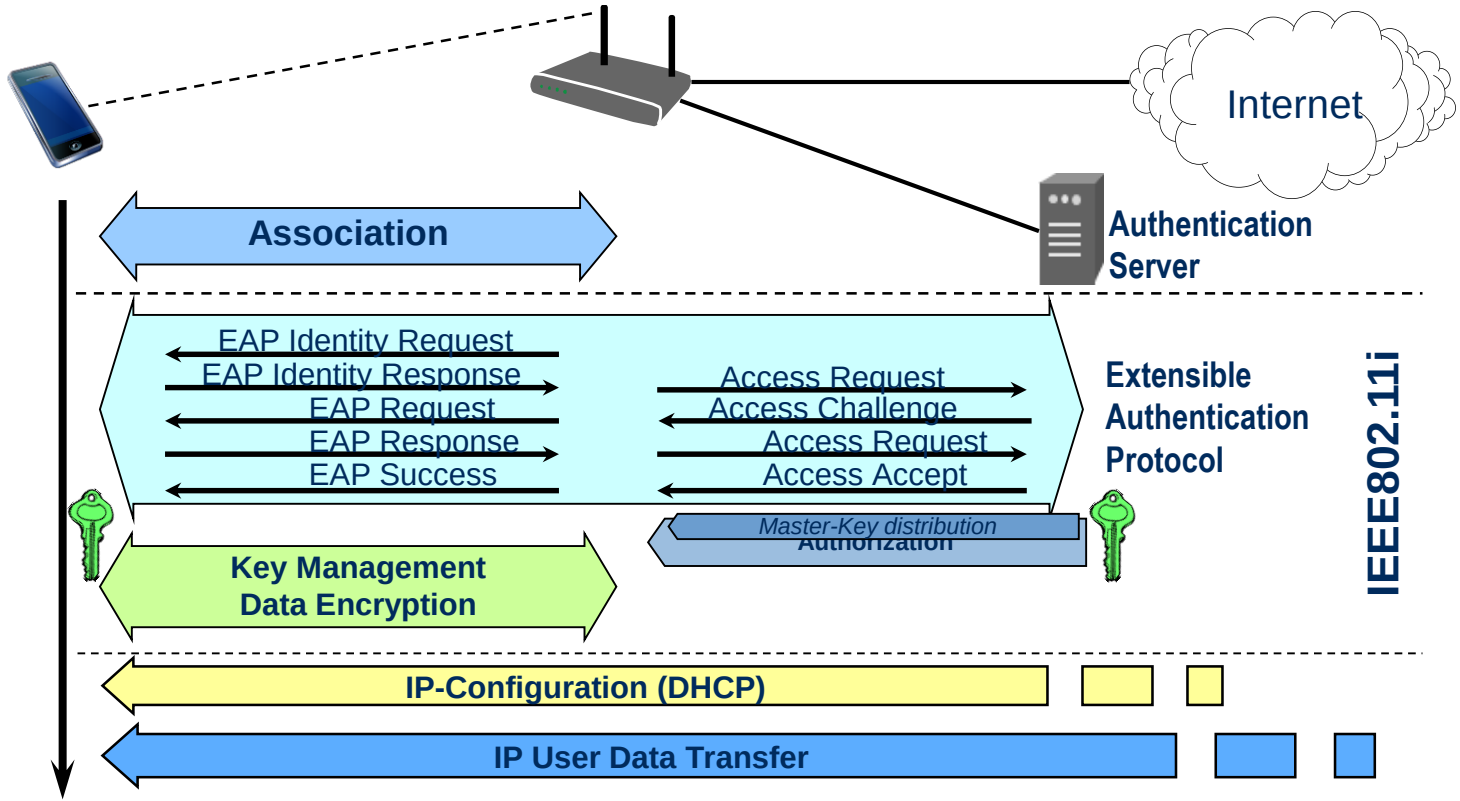
WPA2-Enterprise	WPA2-PSK
• Identifizierung der RSN-Fähigkeiten aus *Beacon-Frames* oder *Probe-Responses*	
• Open System authentication zur Erhaltung der Rückwärtskompatibilität	
• Aushandlung des Verschlüsselungsverfahren während der Assoziierung	
• *Abhänging von den Fähigkeiten von AP und Terminal*	
Enterprise	PSK
IEEE Std 802.1X-2004 Authentisierung Ableitung des Pairwise Master Keys	Ableitung des Pairwise Master Key aus dem eingestellten Passwort
• Erstellung der Arbeitsschlüssel durch das 4-Wege-Nachrichtenaustauschverfahren und Generierung der Gruppenschlüssel für Broadcasts	
• Schutz der Benutzerdatenübertragung durch die ausgehandelten Arbeits- und Gruppenschlüssel.	
• Wenn beide Seiten Protected Management Frame (PMF) unterstützen, werden die Arbeits- und Gruppenschlüssel auch zum Schutz von individuell addressierten Management Nachrichten eingesetzt.	

Verbindungs-Konfiguration





WPA2-Enterprise Authentisierung



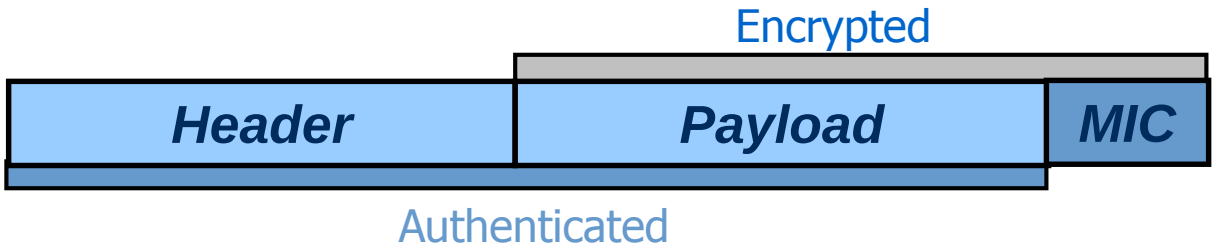
- **Verfahren basiert auf der Übernahme von IEEE 802.1X (EAP over LAN) in die IEEE 802.11i-2004 Spezifikation**

WPA2-PSK Authentisierung

- **PSK (Pre-Shared-Key) Generierung aus dem Passwort**
  - PKCS #5 v2.0 PBKDF2 (RFC2898; Public Key Cryptography Specification #5 v2.0, Password Based Key Derivation Function #2) wird verwendet um einen 256-bit PSK aus einem ASCII Passwort zu generieren.
- **Sinn des PSK-Mode:**
  - Heimanwender können Passwörter eingeben, aber kaum komplizierte Schlüssel.

CCMP Nutzdatenverschlüsselung

- **CCMP (Counter Mode mit Cipher Block Chaining Message Authentication Code Protocol)**
  - Verschlüsselt den Nutzdateninhalt
  - Schützt die Integrität der Header-Informationen gegen Verfälschung

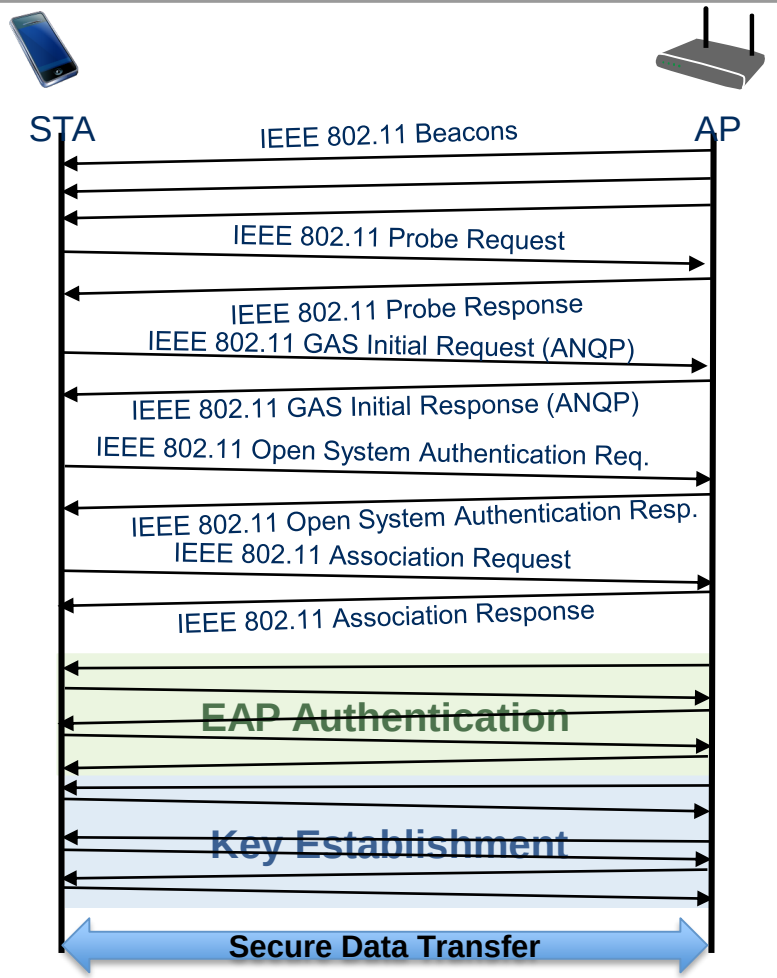


- **Spezielles Verfahren für IEEE 802.11**
  - CBC-MAC wird benutzt um einen Message Integrity Check (MIC) auf Header- und Nutzdateninhalt zu generieren
  - CTR mode wird benutzt um den Nutzdateninhalt und den MIC zu verschlüsseln
  - Benutzt den selben 128-bit Arbeitsschlüssel im AP und in STA
  - Basiert auf einem 128-bit block cipher – IEEE 802.11 verwendet dazu AES

Protected Management Frames (PMF)

- **Management Frames werden benutzt um Verbindungen auf- und abzubauen**
  - Z.B..: authentication, de-authentication, association, dissociation, beacon, probe
- **Management Frames müssen normalerweise unverschlüsselt übertragen werden**
  - … weil sie allgemein verstanden warden müssen
  - … weil noch keine Schlüssel ausgehandelt sind
- **IEEE 802.11w-2009 führte Protected Management Frames (PMF) ein für**
  - Disassociation,
  - De-authentication, and
  - Robust Action Frames (IEEE 802.11-2016 Table 9-47).
    - I.e: Spectrum management, QoS, DLS, Block Ack, Radio measurement, Fast BSS Transition, SA Query, WNM, Mesh, Multihop, Vendor specific protected

IEEE 802.11 Verbindungsaufbau



- **Suche**
  - Beacon
  - Probe Request/Response
- **Netzwerk Selektierung**
  - GAS (ANQP Request/Response)
- **Authentisierung**
  - Open System Authentication
- **Assoziierung**
  - Association Request/Response
- **Authentisierung/Authorisierung**
  - Entweder direkte Schlüsselerstellung bei PSK oder bei IEEE 802.1X EAPoL zur Authentisierung
    - Lässt im nicht-authntisierten Zustand nur EAPoL Nachrichten durch.
    - Das EAP Protokol transportiert die Authentisierungsnachrichten
  - Die abschließende Authorisierung konfiguruiert den Datenpfad und versorgt den AP mit dem Master-Key.
- **Schlüsseleinrichtung**
  - Vier-Weg-Austauschverfahren zur Erstellung des Arbeitsschlüssels.
  - Für Broadcasts warden Gruppen-Schlüssel erstellt.
- **Gesicherter Datentransport**
  - Wenn die Arbeitsschlüssel erstellt sind, wird der Datentransport für Benutzerdaten freigegeben.

WPA3, Enhanced Open, und andere WLAN Erweiterungen

WPA3

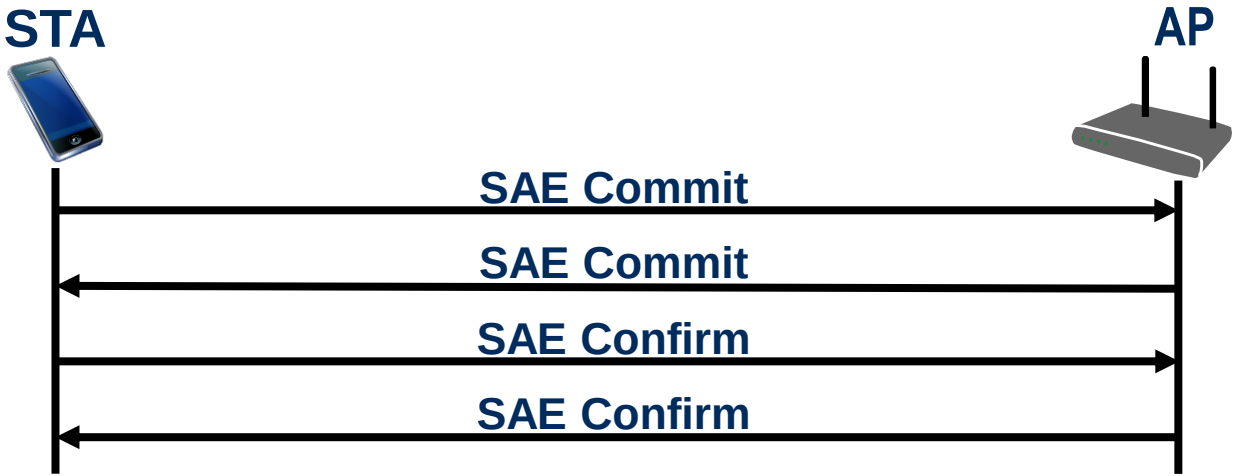
WLAN Sicherheitsprobleme

- **WPA2-PSK hat Schwächen**
  - PSK wird direkt vom Passwort abgeleitet
  - Empfindlich gegen *offline dictionary attack*
    - *Eine aufgezeichnete Verbindung kann in einem Rechenzentrum mittels Wörterbücher analysiert werden, und das gefundene Passwort dann zum Ausspionieren genutzt werden.*
  - Verschlüsselung empfindlich gegen ‚schwache' Passwörter
- **Keine zertifizierte höhere Sicherheit für ganz besonders empfindliche Anwendungen**
  - CCMP basiert auf 128bit Schlüssel
- **Nur optionaler Einsatz von Protected Management Frames**
  - Kein grundsätzlicher Schutz gegen Angriffe mit Deauthentication Frames

Simultaneous Authentication of Equals

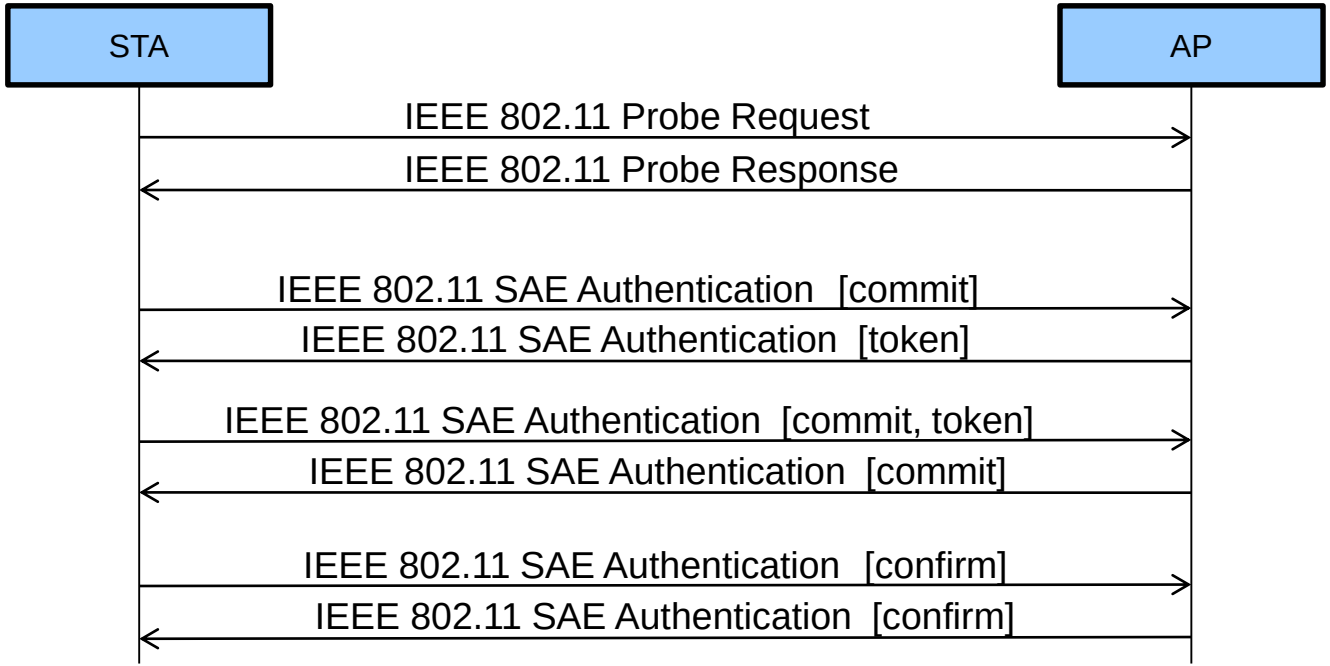
- **SAE löst WPA2-PSK ab.**
  - Schutz gegen Offline Dictionary Attacks
  - Keine nachträgliche Entschlüsselung von Daten bei Bekanntwerden des Schlüssels
    - Perfect forward secrecy
  - Hohe Sicherheit trotz Verwendung von einfachen Passwörtern
  - Handhabung so einfach wie WPA2-PSK
- **Ursprünglich für Absicherung von Mesh Nodes entwickelt und mit IEEE 802.11s-2011 standardisiert.**
  - Generelle Nutzung in IEEE 802.11-2016 spezifiziert.
- **Kann im AP zusammen mit WPA2-PSK nebeneinander verwendet werden.**
  - Ermöglicht weichen Übergang von WPA2-PSK auf WPA3-SAE
- **WPA3-SAE setzt PMF voraus.**

SAE Nachrichtenaustausch



- **Basiert auf *Dragonfly*, einer Passwort-authentisiertem Diffie-Hellman Schlüsselerstellung (RFC7664)**
- **Protokoll:**
  - Jede Seite kann mit SAE Commit beginnen
  - Nachdem beide Seiten SAE Commit geschickt haben, kann eine Seite mit SAE Confirm antworten
  - Das Protocol ist abgeschlossen, wenn beide Seiten SAE Confirm von der Gegenseite erhalten haben.

Blockierungsschutz für SAE



- **Ein AP kann auf ein SAE commit mit einem Token antworten und dadurch die Gegenseite bremsen.**
  - Durch den Token kann die Anzahl der offenen Verbindungsversuche limitiert werden.

WPA3-Enterprise

- **Optional erhöhte Sicherheit durch 192-bit Schlüssellänge**
  - CCMP (128-bit) wird durch 256-bit GCMP (Galois/Counter Mode Protocol)
  - Auch andere Kryptographische Komponenten werden verstärkt
    - 384-bit Hashed Message Authentication Mode mit Secure Hash Algorithm (HMAC-SHA384) für die Schlüsselerstellung und –verifikation
    - 384-bit Elliptic Curve Diffie-Hellman und Elliptic Curve Digital Signature Algorithm für Schlüsselbereitstellung und –authentisierung.
- **Eingesetzte Sicherheitsalgorithmen sind under dem Begriff *Suite-B* bekannt.**
- **Zusätzlich verpflichtende Unterstützung von Protected Management Frames**
- **Definition der Zusammenarbeit mit WPA2-Enterprise um einen weichen Übergang zu ermöglichen.**

WPA, WPA2 und WPA3

IEEE 802.11	WPA	WPA2	WPA3
IEEE 802.1X			
PSK			
SAE			
Datenverschlüsselung			
TKIP			
CCMP			
GCMP			
Weitere Funktionen			
Basic Service Set			
IBSS			
Pre-authentication			
Key hierarchy			
Key management			
Cipher & authentication Negotiation			
Protected Management Frames		opt.	

- **WPA (Wi-Fi Protected Access) als schnelle Lösung gegen WEP**
  - WPA konnte als Software-Update realisiert werden
- **WPA2 realisiert das Robust Security Network gemäß IEEE 802.11i**
  - Von WPA mit TKIP wird abgeraten
    - WPA-Einstellung beschränkt Geschwindigkeit auf 54 Mbps (11a, 11g)
    - 11n, 11ac verlangen WPA2 AES Verschlüsselung für volle Geschwindigkeit
- **WPA3 ersetzt PSK durch SAE und bietet für Enterprise bessere Verschlüsselung**
  - Protected Management Frames sind verpflichtend.

WPA3, Enhanced Open, und andere WLAN Erweiterungen

ENHANCED OPEN

Mehr Sicherheit im öffentlichen WLAN

- **Unverschlüsselte WLANs sind sehr verbreitet für offene WLAN Zugänge**
- **Unverschlüsselte WLANs bieten keinen Schutz und sollten eigentlich nur mit VPNs verwendet werden.**
- **Enhanced Open bietet Verschlüsselung für offene WLANs.**

Wi-Fi CERTIFIED™ Enhanced Open

- **Wendet Opportunistic Wireless Encryption (RFC 8110) auf WLAN an.**
  - Effektiv ein Diffie-Hellman Schlüsselaustausch ohne Authentisierung für WLAN („SAE ohne Passwort“)
- **Enhanced Open hat keine Authentisierung**
  - Empfindlich für Man-in-the-middle attack mittels Fake-AP
- **Aber nach abgeschlossenem Verbindungsaufbau ist die Verbindung zwischen STA und AP gegen Spionage und Fälschung gesichert.**
- **Benötigt eine eigene SSID**
  - Unverschlüsselte SSID kann nicht verwendet werden, eben so wenig wie eine WPA2-PSK oder WPA3-SAE SSID

WPA3, Enhanced Open, und andere WLAN Erweiterungen

EIN BLICK IN DIE ZUKUNFT

Geplante weitere Verbesserungen

- **Zertifizierung von Fast Transition**
  - Fast Transition ist eine Erweiterung, die Schlüssel vorsorglich an APs verteilt um nach einem Handover keinen neuen Schlüssel aushandeln zu müssen.
- **Zertifizierung von Client Privacy**
  - WLAN Clients können nicht nur durch ihre MAC Adresse sondern auch durch typische Vorbelegung von anderen Protokollelementen identifiziert werden. Die Zertifizierung soll sicherstellen, dass alle Protokollelemente möglichst gleichartig verwendet und vorbesetzt werden.
- **Validierung von Server Zertifikaten bei WPA2/3 Enterprise clients**
  - Die Sicherheit von EAP Methoden beruht auf der sorgfältigen Verifizierung der übermittelten Server Zertifikate.
- **SAE Passwort Identifizierung**
  - SAE erlaubt die parallel Benutzung mehrerer Passwörter an einem AP. Dadurch können Gruppen von Benutzern unterschieden werden, und den verschiedenen Gruppen auch unterschiedliche Profile zugewiesen werden.

WPA3, Enhanced Open, und andere WLAN Erweiterungen

GENERATIONAL WI-FI

Generationen anstelle Buchstabensuppe

- **Wi-Fi Radio Technologien wurden bisher anhand der mit Buchstaben identifizierten Standarderweiterung bezeichnet.**
  - 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac
- **Diese Bezeichnung hat zur Verwirrung im Markt geführt und eine schnelle Einführung neuer Standards verhindert.**
- **Die Wi-Fi Alliance möchte durch die Verwendung von Generationen anstelle der Buchstabenkombination der Standarderweiterung eine Mobilfunk ähnliche Lösung.**
  - Mobilfunk: 1G -> 2G -> 3G -> 4G ->5G
- **Die nächste Wi-Fi Technologie basierend auf 802.11ax wird als Wi-Fi 6 bezeichnet.**
  - Zertifizierte Produkte bezeichnet man als Wi-Fi CERTIFIED™ 6

Visualisierung von Wi-Fi Technologien

- **Bezeichnung und Visualisierung von Wi-Fi Generationen**

If the most advanced technology a device supports is …	Then it shall be identified as generation
802.11ax	Wi-Fi 6
802.11ac	Wi-Fi 5
802.11n	Wi-Fi 4

- **Der Benutzer soll anhand der WLAN-Icons auf dem Bildschirm sofort sehen, welche Technologie der AP unterstützt.**
  - Man erhofft sich dadurch einen erhöhten Wettbewerb zum schnelleren Umstieg auf neue Wi-Fi Technologien.

Vielen Dank für die Aufmerksamkeit

FRAGEN?, KOMMENTARE!