WLAN-Sicherheit 16.06.2018

https://www.elektronik-kompendium.de/sites/net/1403011.htm

Um ein WLAN sicher zu betreiben ist die Authentifizierung des Benutzers und die Verschlüsselung der Datenübertragung notwendig. Die deutsche Rechtsprechung sieht die Authentifizierung und Verschlüsselung eines WLANs zwingend vor. Wer ein WLAN unzureichend gesichert betreibt, gilt im Falle einer Rechtsverletzung über seinen Internet-Anschluss als Störer und wird demzufolge in Haftung genommen.

WPA2:

WPA2 (WiFi Protected Access 2) bzw. IEEE 802.11i ist ein Standard aus dem Jahr 2004 für die **Authentifizierung** und **Verschlüsselung** von WLANs, die auf den IEEE-Spezifikationen 802.11 basieren.

WPA-Variante		WPA	WPA2
Personal Mode	Authentifizierung	PSK	PSK
	Verschlüsselung	TKIP/MIC	AES-CCMP
Enterprise Mode	Authentifizierung	802.1x/EAP	802.1.x/EAP
	Verschlüsselung	TKIP/MIC	AES-CCMP

Verschlüsselung: AES (symmetrisches Verschlüsselungsfahren)

WPA2 Enterprise Mode

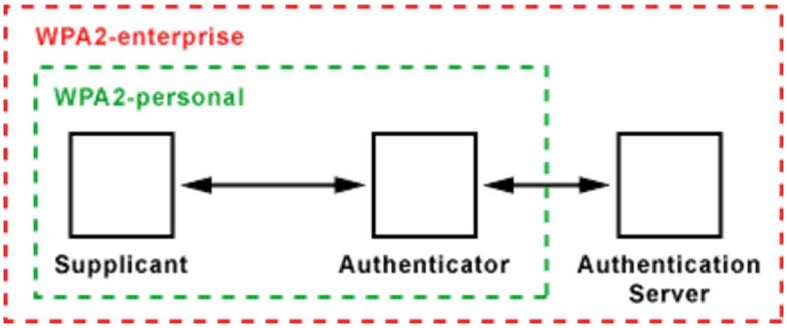
Der WPA2 Enterprise Mode ist mit IEEE 802.11i fast identisch. Der Unterschied ist die fehlende Funktion Fast Roaming, die für VoIP-, Audio- und Video-Anwendungen interessant ist. Mit dieser Funktion wird der Wechsel zwischen zwei Access Points (AP) schneller durchgeführt. Die Verbindung verläuft damit unterbrechungsfrei.

Wesentlicher Bestandteil ist die Authentifizierung per **RADIUS**.

WPA2 Personal Mode

Der WPA2 Personal Mode ist eine abgespeckte WPA2-Variante, die hauptsächlich in SOHO-Geräten für Privatanwender und kleine Unternehmen gedacht ist. Die Authentifizierung erfolgt mit ein Pre-Shared-Key (Passwort).

Funktionsweise von IEEE 802.11i und WPA/WPA2



Bei der WPA-Schlüsselverhandlung bekommen die Stationen Rollen zugewiesen. Der Access

Point ist der Authenticator (Beglaubigter) und der Client der Supplicant (Antragsteller/Bittsteller). Dabei ist genau festgelegt, welche Seite welches Paket zu welchem Zeitpunkt verschickt und wie darauf reagiert werden muss.
Bei WPA bzw. WPA2 erfolgt die Netzwerk-Authentifizierung mit einem Pre-Shared-Key (PSK) oder alternativ über einen zentralen 802.1x/Radius-Server. Dabei wird ein Passwort mit 8 bis 63 Zeichen Länge verwendet. Das Passwort ist Teil eines 128 Bit langen individuellen Schlüssels, der zwischen WLAN-Client und dem Access Point ausgehandelt wird. Der Schlüssel wird zusätzlich mit einem 48 Bit langen Initialization Vector (IV) berechnet. Dadurch wird die Berechnung des WPA-Schlüssels für den Angreifer enorm erschwert.
Die Wiederholung des aus IV und WPA-Schlüssel bestehenden echten Schlüssels erfolgt erst nach 16 Millionen Paketen (224). In stark genutzten WLANs wiederholt sich der Schlüssel also erst alle paar Stunden. Um die Wiederholung zu verhindern, sieht WPA eine automatische Neuaushandlung des Schlüssels in regelmäßigen Abständen vor. Damit wird der Wiederholung des echten Schlüssels vorgegriffen. Aus diesem Grund lohnt es sich für den Angreifer kaum den Datenverkehr zwischen Access Point und WLAN-Clients abzuhören.

https://de.wikipedia.org/wiki/Pre-shared_key

Pre-shared key

Mit Pre-shared key (PSK; englisch für „vorher vereinbarter Schlüssel“) bezeichnet man solche Verschlüsselungsverfahren, bei denen die Schlüssel vor der Kommunikation beiden Teilnehmern bekannt sein müssen, also **symmetrische** Verfahren. PSK-Verschlüsselung hat den Vorteil, dass sie zwischen zwei bekannten Teilnehmern wesentlich einfacher zu realisieren ist als asymmetrische Verschlüsselung. Der große Nachteil des Verfahrens besteht darin, dass beide Teilnehmer den Schlüssel vor der eigentlichen Kommunikation im Geheimen tauschen müssen. Daraus folgt, dass das PSK-Verfahren für viele Anwendungen im Internet (wie z. B. Online-Einkauf) ungeeignet ist, da der vorherige Schlüsseltausch in diesem Fall nicht möglich bzw. viel zu aufwendig ist. In einem solchen Fall verwendet man besser das Public-Key-Verfahren.
Der Begriff PSK wird oft mit Wireless LAN in Verbindung gebracht, da in Funknetzwerken häufig die Verschlüsselungsmethode WPA-PSK verwendet wird, hier wird häufig auch das Passwort für das WPA-PSK-Verfahren so oder als „WLAN-Passwort“ bezeichnet. Für kleine Netzwerke wie z. B. in Privathaushalten ist das eine gute Methode, da der Schlüssel problemlos von einer Person auf den verschiedenen Geräten wie Router und PC eingetragen werden kann.

https://www.ceilers-news.de/serendipity/901-WLAN-Sicherheit-5-WPA-Schluesselaustausch-und-DoS-Angriffe.html

WLAN-Sicherheit 5 - WPA-Schlüsselaustausch und DoS-Angriffe

Geschrieben von Carsten Eilers am Donnerstag, 31. August 2017 um 10:00

Da der ursprüngliche Standard-Verschlüsselungsalgorithmus für drahtlose Netze nach dem Standard IEEE 802.11 (WLAN), Wired Equivalent Privacy (WEP) einige Schwachstellen enthält und es etliche Tools für Angriffe darauf gibt, musste ein Ersatz her. Ein neuer Sicherheitsstandard, IEEE 802.11i, war bereits in Entwicklung, aber noch nicht einsetzbar. Daraufhin wurde von der Wi-Fi Alliance eine Zwischenlösung veröffentlicht, das in der vorherigen Folge vorgestellte Wi-Fi Protected Access (WPA). Für dessen vollständige Beschreibung fehlt noch der

Schlüsselaustausch

Nach erfolgreicher Authentifizierung wird der Schlüsselaustausch zur Bildung der notwendigen Schlüssel gestartet. Der erfolgt in folgenden Schritten:

1. Sowohl Access-Point als auch Client kennen bereits den so genannten 'Pairwise Master Key' (PMK) – entweder das individuelle temporäre Secret aus der EAP-Authentifizierung oder das aus dem PSK berechnete allgemeine Master-Secret.
   Beide erzeugen nun Zufallsdaten (Nonces).
   Der Access-Point sendet seinen Nonce-Wert an den Client.
2. Der Client berechnet aus dem PMK, seiner und der MAC-Adresse des Access-Points sowie den beiden Nonces den 'Pairwise Transient Key' (PTK), aus dem die benötigten Schlüssel für RC4-Verschlüsselung und MIC-Berechnung abgeleitet werden.
   Er sendet dann seinen Nonce und dessen MIC-Wert an den Access-Point.
3. Der Access-Point berechnet nun analog zum Client ebenfalls den 'Pairwise Transient Key' (PTK). Dieser wurde daher niemals übertragen.
   Damit ist der 'Pairwise Key Handshake' abgeschlossen, es folgt der 'Group Key Handshake'.
   Der Access-Point überträgt nun den für die Verschlüsselung von Broadcast- und Multicast-Paketen verwendeten 'Group Transient Key' (GTK). Die Übertragung erfolgt durch den PTK geschützt, außerdem wird der MIC-Wert des GTK übertragen.
4. Der Client antwortet mit dem mit dem PTK verschlüsselten empfangenen MIC.
5. Stimmt der mit dem übertragenen Wert überein, wurde der GTK nicht manipuliert und die verschlüsselte Kommunikation kann beginnen.

	Client		Access-Point
1.	• Kennt 'Pairwise Master Key' (PMK) • Erzeugt NonceC	NonceA <----------	• Kennt 'Pairwise Master Key' (PMK) • Erzeugt NonceA
2.	• Berechnet 'Pairwise Transient Key' (PTK)	NonceC, MIC(NonceC) ---------->	
3.			• Berechnet 'Pairwise Transient Key' (PTK) • Stellt 'Group Transient Key' (GTK) bereit

		• Verwendet PTK	
		PTK(GTK, MIC(GTK)) <----------	
4.	• Verwendet PTK und GTP	•	
		PTK(MIC(GTK)) ---------->	
5.			• Vergleicht gespeicherten und empfangenen MIC(GTK) Wenn identisch: Verschlüsselte Kommunikation beginnt

Durch WPA geschützte Kommunikation

Angriffe auf WPA

WPA schützt die Kommunikation deutlich besser als WEP. Aber das ist ja kein Wunder, denn WEP bietet bekanntlich überhaupt keinen Schutz mehr.

DoS-Angriffe über 'Michael'

Schon kurz nach der Veröffentlichung des neuen Standards wurde auf die Möglichkeit von DoS-Angriffen auf bzw. über den Message Integrity Check (MIC) 'Michael' hingewiesen: Beim Empfang von 2 Paketen mit falschem MIC-Wert innerhalb einer Sekunde werden alle Schlüssel für ungültig erklärt und die Verbindung für eine Minute gesperrt. Damit sollen Angriffe auf den MIC abgewehrt werden, die durch die relativ schwache verwendete Hash-Funktion entstehen.

Die Möglichkeit, das für DoS-Angriffe zu nutzen, wurde dabei bewusst in Kauf genommen. Denn alle Ansätze, die DoS-Möglichkeit zu verhindern, würden die Sicherheit des Protokolls reduzieren.

Die WLAN-Hardware ist einfach nicht leistungsstark genug um sicherere Kryptografie als 'Michael' zu bewältigen. Der Algorithmus wurde extra so entwickelt, dass die damals vorhandenen Geräte ihn bewältigen können. Dass darunter die Sicherheit leidet ist unvermeidbar: Der Schlüsselraum ist mit 2^{20} deutlich kleiner als z.B. die 2^{128} bei AES mit der minimalen Schlüssellänge von 128 Bit. Das ermöglicht natürlich Brute-Force-Angriffe, also musste ein Schutz her. Und wie eigentlich immer führt ein Schutz vor Brute-Force-Angriffen zu Möglichkeiten für DoS-Angriffe - man muss sich also entscheiden, was einem wichtiger ist: Vertraulichkeit oder Verfügbarkeit.

Mal abgesehen davon, dass Vertraulichkeit eigentlich immer vor zu ziehen ist, gibt es im zu Grunde liegenden 802.11-Protokoll schwerwiegendere DoS-Schwachstellen. Also wäre eine Schwächung von WPA zur Verhinderung dieses einen DoS-Angriffs völlig nutzlos - ein Angreifer, der einen DoS auslösen will, würde dann einfach eine der anderen DoS-Schwachstellen ausnutzen. Und in der Tat habe ich nie von DoS-Angriffen über WPA gehört. Oder von DoS-Angriffen auf WPA allgemein. Es scheint also keine gegeben zu haben, oder zumindest keine, die zu einem größeren Aufschrei oder Medienecho geführt hätten.

Außerdem sind DoS-Angriffe doch sowieso ziemlich lahm. Wirklich lohnenswert sind nur Angriffe auf die Verschlüsselung. Und die sind im Fall von WPA ebenfalls möglich. Und genau darum geht es in der nächsten Folge.

Carsten Eilers

WPA3

https://www.security-insider.de/was-ist-wpa3-a-742210/

Definition WPA3 (Wi-Fi Protected Access 3) Was ist WPA3?

10.09.2018Autor / Redakteur: Dipl.-Ing. (FH) Stefan Luber / Peter Schmitz

Der WLAN-Verschlüsselungsstandard WPA3 (Wi-Fi Protected Access 3) wurde im Juni 2018 als Ergänzung zum bestehenden Standard WPA2 verabschiedet. WPA3 bringt wesentliche Verbesserungen bei der Authentifizierung und Verschlüsselung mit. Zudem soll sich die Konfiguration von WLAN-Geräten vereinfachen und die Sicherheit an öffentlichen Hotspots erhöhen.

WPA3 (Wi-Fi Protected Access 3) wurde im Juni 2018 als Ergänzung zum WLAN-Verschlüsselungsstandard WPA2 verabschiedet.

(Bild: Pixabay / CC0)

Anfang 2018 kündigte die Wi-Fi Alliance den neuen Standard WPA3 (Wi-Fi Protected Access 3) an und verabschiedete ihn am 25. Juni 2018. WPA3 soll den vorhandenen Standard WPA2 nicht ablösen, sondern die Sicherheit weiter verbessern und neue Funktionen integrieren. Es ist davon auszugehen, dass WPA2 zukünftig noch weiterentwickelt und in Geräten implementiert wird. WPA3 und WPA2 werden über einen längeren Zeitraum parallel verfügbar sein. Erste nach WPA3 zertifizierte Endgeräte könnten bereits Ende 2018 erscheinen.

Wi-Fi Protected Access 3 bringt wesentliche Verbesserungen im Bereich der Authentifizierung und Verschlüsselung mit. Zudem soll sich die Konfiguration von WLAN-Geräten vereinfachen und die Sicherheit an öffentlichen Hotspots erhöhen. Aufgrund der verwendeten 192-bit-Encryption eignet sich Wi-

Fi Protected Access 3 für drahtlose Netzwerke mit höchsten Sicherheitsanforderungen, wie sie bei Behörden, Industriebetrieben, Militär oder Regierungen im Einsatz sind. Die in WPA2-geschützten WLANs und bestimmten WPA2-Implementierungen bestehende KRACK-Sicherheitslücke behebt WPA3 durch die Einführung eines verbesserten Handshake-Verfahrens.

Die wesentlichen Neuerungen und Verbesserungen von WPA3

Die wesentlichen Neuerungen von Wi-Fi Protected Access 3 lassen sich in vier Bereiche zusammenfassen. Diese vier Bereiche sind:

- 1. WPA3 bietet einen hohen Schutz des WLANs, selbst wenn einfache, nicht den Empfehlungen für sichere Kennwörter verwendete Passwörter eingesetzt werden.
- 2. Die WLAN-Konfiguration soll sich vereinfachen. Insbesondere gilt dies für Geräte, die keinen eigenen Bildschirm besitzen, wie sie beispielsweise im Internet oft Things (IoT) zu finden sind.
- 3. Die Sicherheit in öffentlichen WLANs und in Gast-WLANs verbessert sich durch eine individuelle Verschlüsselung der übertragenen Daten.
- 4. Aufgrund der 192-bit-Verschlüsselung ergibt sich ein höherer Sicherheitsstandard, der den Einsatz von WPA3-WLANs in besonders sicherheitsrelevanten Bereichen ermöglicht.

WPA3 enthält eine Implementierung des sogenannten Dragonfly-Protokolls mit Simultaneous Authentication of Equals (SAE). Ziel dieser Implementierung ist es, die Sicherheit beim Schlüsselaustausch mit dem Handshake-Verfahren zu verbessern. Die Sicherheit ist selbst dann gewährleistet, wenn schwache Kennwörter zum Einsatz kommen. Brute-Force- oder Wörterbuch-Attacken sind dank dem neuen Handshake-Verfahren so gut wie unmöglich. Es macht unter anderem die KRACK-Angriffsmethode unwirksam.

An öffentlichen Hotspots oder Gast-WLANs kommt die Opportunistic Wireless Encryption Methode (OWE) zum Einsatz. Sie basiert auf RFC 8110 und ermöglicht eine Verschlüsselung der übertragenen Daten ohne ein vorgegebenes Passwort. WLAN-Accesspoints und -Clients verwenden stattdessen einen nur einmal verwendbaren sogenannten Pairwise Master Key (PMK). Jede Verbindung zwischen einem Endgerät und dem Router oder Accesspoint nutzt zur Verschlüsselung der Daten einen individuellen, einzigartigen Schlüssel. Unbefugten ist es nicht mehr möglich, Daten in einem öffentlichen WLAN mitzulesen. Das Risiko für Man-in-the-Middle-Attacken ist ebenfalls minimiert.

Aufgrund der mit WPA3 eingeführten 192-bit-Verschlüsselung bestehen höhere Anforderungen an die Rechenkapazität der WLAN-Schnittstellen der Clients und der Accesspoints. Es ist daher davon auszugehen, dass Endgeräte nicht ohne weiteres per Softwareupgrade von WPA2 auf WPA3 umgestellt werden können. In vielen Fällen ist vermutlich neue Hardware erforderlich. Vor allem ältere Geräte werden kein Update auf WPA3 erhalten.

Dragonblood-Schwachstelle

Anfang April 2019 demonstrierten die beiden Forscher Mathy Vanhoef (NYUAD) und Eyal Ronen (Tel Aviv University & KU Leuven) in ihrem Paper „Dragonblood: A Security Analysis of WPA3's SAE Handshake“ mehrere Schwachstellen in WPA3. Zu diesen gehören einerseits Downgrade-Attacken, mit denen sich die höheren Sicherheitshürden von WPA3-Personal umgehen lassen. Des Weiteren ließen sich Schwachstellen des Dragonfly handshakes selbst ausnutzen.