# Sicherer funken

## WPA3 löst die löchrige WLAN-Verschlüsselung WPA2 ab

**Anfang Januar kündigte die Wi-Fi Alliance konkrete Pläne für den Nachfolger des in die Jahre gekommenen WLAN-Verschlüsselungsverfahrens WPA2 an. WPA3 soll viele Verbesserungen bringen, aber um eine simple gibt es Streit.**

**Von Jennifer Li**

Seit mehreren Jahren feilen verschiedene Firmen an verbesserten Verschlüsselungsverfahren fürs WLAN. Obschon die WPA3-Entwickler mehrfach bemerkten, dass Verschlüsselung wie eine Impfung sei, die man rechtzeitig vornehmen müsse und nicht erst, wenn das Kind schon krank ist, blockierten einige Mitarbeiter des Herstellerverbandes Wi-Fi Alliance (WFA) den Ansatz. Zu groß war ihre Angst, dass ein WPA2-Nachfolger Kunden verunsichern könnte, weil denen die bisherige Technik dann als angeknackst erscheint – völlig zu Recht, wie der KRACK-Angriff im Herbst 2017 bewiesen hat (siehe ct.de/yxar).

So kündigte die WFA erst zur CES im Januar konkret an, dass WPA3 noch in diesem Jahr eingeführt wird. Wie gewohnt wird es zwei Varianten geben: WPA3-Enterprise ist für Unternehmen gedacht und ermöglicht individuelle Authentifizierung. WPA3-Personal verwendet dasselbe Passwort für alle Nutzer eines WLANs, wie man es von WPA2-PSK kennt. Beide setzen auf denselben Unterbau.

Die als Suite-B von der NSA gesammelten, unter Experten als vertrauenswürdig geltenden Krypto-Empfehlungen sollen bei WPA3 für ein einheitliches Schutzniveau sorgen, vom Schlüsselaustausch über den Verschlüsselungsalgorithmus bis zum Hashing. Sie vermeiden beispielsweise, dass die sichere AES-Chiffre mit den unsicheren Hash-Algorithmen SHA1 oder MD5 kombiniert wird. Deshalb gibt es im WPA3-Prüfplan für das Wifi-Zertifikat der WFA erstmals auch Negativtests, damit ein Gerät verbotene Kombinationen weder anbietet noch akzeptiert. Für den Schlüsselaustausch mittels eines vorab festgelegten Passworts in der Personal-Variante setzt WPA3 auf SAE (Simultaneous Authentication of Equals). Das im RFC 7664 der IETF Dragonfly genannte Verfahren erschwert mittels „Zero-knowledge Proof“ das Offline-Knacken des Passworts so sehr, dass es selbst für exzellent ausgestattete Angreifer aussichtslos wird – herkömmliche Hardware angenommen.

Ferner stellt SAE sicher, dass ein Angreifer auch bei Kenntnis des Passworts keine Datenpakete nachträglich entschlüsseln kann (Perfect Forward Secrecy).

### WPA3 kommt

WPA3 kommt immer im Paket mit PMF: Protected Management Frames verhindern unter anderem Deauthentication-Angriffe, mit denen Angreifer versuchen, WLAN-Clients vom aktuellen Access Point zu lösen und auf einen Honeypot unter ihrer Kontrolle zu locken.

Fehlen wird OWE (Opportunistic Wireless Encryption), obwohl die WFA sie noch im Januar als einen wesentlichen Fortschritt von WPA3 herausstellte. Mit OWE hätte der unverschlüsselte Betrieb von WLANs ein Ende finden können. Doch nach Jahren unbeachteter Diskussionen von Sicherheitsexperten raufte sich eine Gruppe unbeteiligter Firmen zusammen und opponierte erfolgreich gegen OWE.

Anders als WPA3-Enterprise und -Personal braucht OWE kein Passwort oder Geheimnis. So würde eine WLAN-Basis ähnlich wie beim als „Open“ bezeichneten, unverschlüsselten Betrieb jedem Client Zugang gewähren. Trotzdem können Basis und Client individuelle Sitzungsschüssel aushandeln.

Damit wäre OWE sogar sicherer als WPA2-Personal, weil niemand das gemeinsame Geheimnis kennt, anhand dessen die Geräte ihre Sitzungsschlüssel aushandeln. Denn bei WPA2-Personal können Angreifer diese errechnen, wenn sie das Geheimnis kennen und den vierstufigen Anmeldeprozess belauschen können.

Die OWE-Gegner bemängeln, dass ein simultaner Betrieb von unverschlüsselten und OWE-Netzen im selben AP kompliziert zu implementieren sei. Auch müsse gegenüber SAE weiterer Code entwickelt werden. Es sei einfacher, OWE durch SAE mit einheitlichem Passwort zu ersetzen. Da der Streit um OWE noch läuft, wird es in der ersten Welle WPA3-fähiger Geräte wohl nicht implementiert sein und WLAN-Hotspots müssen noch einige Zeit unverschlüsselt weiterfunken.

### Noch dieses Jahr

Mitte Mai hat Qualcomm als erster Chiphersteller angekündigt, WPA3 in die nächste Treiberversion seiner aktuellen WLAN-Bausteine einzubauen. Man darf also damit rechnen, dass die neue Verschlüsselung noch in diesem Jahr per Firmware- oder Treiber-Update in erste Geräte einzieht. Zwar will AVM, in dessen aktuellen Fritzboxen Qualcomm-Chips funken, mit dem bald erscheinenden FritzOS 7 schon Protected Management Frames einführen. WPA3 wird aber erst später folgen.

Gegenwärtig beabsichtigt die WFA, WPA2 und WPA3 zwei Jahre lang parallel zu führen. Danach würde WPA2 entfallen und WPA3 für alle WFA-zertifizierten Geräte verpflichtend werden. So könnte WPA2 bei neuen Geräten schon 2020 fehlen.

Alte Clients werden dadurch aber nicht ausgesperrt: Alle WPA3-Geräte müssen auf WPA2 zurückfallen können (WPA3-SAE Transition mode). Denn bis alle alte, nur WPA2-fähige Hardware aus dem Markt verschwunden ist, wird es noch geraume Zeit dauern. Und bis dahin sollte man wie gewohnt auch an WPA3-fähigen Routern das voreingestellte WLAN-Passwort ändern. *(ea@ct.de)* c't

***WPA3-Ankündigung, Deauth-Angriff:*** ***ct.de/yxar***


**Auch bei WPA3 werden WLAN-Router eine Koppeltaste haben, mit der man Clients bequem per Tastendruck anmelden kann.**