Kurz erklärt: WLAN-Verschlüsselung mit WPA3

Gehärtet

Uwe Schulze

2018 verabschiedete die Wi-Fi Alliance den aktuellen Sicherheitsstandard WPA3. Jetzt erscheinen die ersten Geräte auf dem Markt, die ihn umsetzen.

Die Datenübertragung unterliegt einem ständigen Wettlauf zwischen Hackerangriffen und Schutzmaßnahmen. Der von der Wi-Fi Alliance (WFA) definierte Standard WPA2 (Wi-Fi Protected Access) für den Zugang zu drahtlosen lokalen Netzen kann hierfür so schlecht nicht sein, denn er ist bereits 15 Jahre alt und auf praktisch jedem WLAN-fähigen Gerät implementiert.

Das Vertrauen in WPA2 ist aber erschüttert, seit 2017 die KRACK-Sicherheitslücke Schlagzeilen machte. Dies nahm die WFA zum Anlass, einen Nachfolgestandard zu entwickeln. Auf den ersten Blick erscheint die neue Namensgebung wie reine Imagepflege, denn auch WPA2-Geräte können mit aktueller Software und starkem Passwort weiterhin sicher betrieben werden. Aber WPA3 bedeutet nicht nur eine Umbenennung, sondern eine neue Zertifizierung. Damit lassen sich endlich alte und potenziell unsichere Softwaremodule wirkungsvoll ausschließen. Vor diesem Hintergrund ist es ein Schritt zu mehr Sicherheit im WLAN und sollte schnell Eingang in alle neue Hardware finden.

WPA3 ist voll abwärtskompatibel, sodass die Interoperabilität auch während einer längeren Übergangszeit gewährleistet ist. Ob sich Geräte per Firmware nachrüsten lassen, hängt vom Hersteller ab. Wenn überhaupt, dürfte es WPA3 nur für die jeweils letzte Generation per Update geben, denn eine stärkere und individuelle Verschlüsselung für jede Clientverbindung erfordert mehr Rechenleistung und damit schnellere Hardware. Die Chiphersteller haben deshalb neue Funkmodule für WPA3 entwickelt.

WPA spezifiziert nicht die verwendeten Protokolle, sondern nur Zertifizierungskriterien. Die Beschreibung der eigentlichen Software für Schlüsselaustausch, Verschlüsselung und Hash-Berechnung steckt in der Suite B der amerikanischen NSA – einer Zusammenstellung besonders gehärteter und vertrauenswürdiger Protokolle.

WPA3 definiert aber nicht nur sicherere Techniken als der Vorgängerstandard, sondern schreibt im Zertifizierungsprozess auch gezielte Prüfungen auf Schwachstellen vor. Hierzu zählen Brute-Force-Angriffe zum Erraten des Passworts oder Man-in-the-Middle-Angriffe à la KRACK. Auch der Ausschluss von als unsicher eingestuften Protokollen und Hashes wird überprüft. Hierzu gehören TKIP (Temporal Key Integrity Protocol) und MD5.

Dienstliches von Privatem getrennt

WPA3 unterscheidet wie WPA2 zwischen Enterprise und Personal Mode. Der Personal Mode ist für öffentliche Hotspots gedacht, bei denen sich alle User mit demselben Passwort anmelden. WPA3 ersetzt die bisher verwendete Methode zum Aushandeln des Sitzungsschlüssels mittels Pre-shared Key (PSK) durch Simultaneous Authentication of Equals (SAE). So wird der Schlüssel nicht mehr im Funkkanal übertragen. Das erschwert Rückschlüsse auf den Schlüssel durch Mitschneiden des Handshake und erhöht die Sicherheit insbesondere für kurze oder schwache Kennwörter. Damit soll es nahezu unmöglich sein, ein WLAN mit Wörterbuchangriffen zu knacken. Außerdem stellt SAE mittels Perfect Forward Secrecy sicher, dass ein Angreifer auch bei Kenntnis des WLAN-Passwortes keine Datenpakete nachträglich entschlüsseln kann. SAE gilt als die entscheidende Neuerung in WPA3, ist aber gar nicht neu: Das Protokoll wurde im Rahmen des Mesh-Standards 802.11s entwickelt.

Der WPA3-fähige Mesh-Router MR2200ac von Synology beherrscht die passwortfreie Verschlüsselung mittels OWE, die es jedoch nicht in den Wi-Fi-Standard geschafft hat.

Der Enterprise Mode sieht WLAN-Nutzer mit individuellen Passwörtern vor, wie sie in Unternehmen üblich sind. Die Authentifizierung ändert sich hier nicht. Es kommt aber eine stärkere Verschlüsselung zum Einsatz, die einen 192-Bit-Schlüssel nutzt.

Bereits in WPA2 waren Protected Management Frames (PMF) als optionale Erweiterung vorgesehen. Sie behebt die Schwachstelle, dass die Managementinformationen zum Aufbau und Betrieb von Datenverbindungen unverschlüsselt bleiben. Zwar lassen sich damit keine Nutzdaten abgreifen, aber gefälschte Managementinformationen lancieren. Mit PMF wird nun auch der Management-Traffic verschlüsselt.

Eine von der Wi-Fi Alliance im Vorhinein als wesentlich angepriesene Erweiterung ist in der aktuellen WPA3-Spezifikation jedoch gar nicht enthalten: Opportunistic Wireless Encryption (OWE). Sie sieht vor, dass offene Hotspots, die möglichst einfach und ohne Eingabe eines Passworts nutzbar sind, Daten trotzdem verschlüsselt übertragen, indem Access Point und Endgerät individuelle Sitzungsschlüssel aushandeln.

Kritiker von OWE führen ins Feld, dass es kompliziert zu implementieren sei und nicht vor den eigentlichen Gefahren fehlender Authentifizierung schütze: Man-in-the-Middle-Angriffen oder Honeypot-Access-Points. Eine einfachere Lösung sei stattdessen SAE mit einheitlichem Passwort. Für OWE sieht die Wi-Fi Alliance eine eigene Zertifizierung vor: Wi-Fi Certified Enhanced Open.

Weiterhin lückenhaft

All solchen Anstrengungen um mehr Sicherheit und Komfort im drahtlosen Netz zum Trotz steht eines schon jetzt fest: Den Wettlauf mit den Angreifern kann auch WPA3 nicht beenden. Erst im April 2019 mussten mehrere Sicherheitslücken geschlossen werden. (un@ix.de)

Uwe Schulze

ist freier Autor in Berlin.