LANCOM Whitepaper

WPA3 & Enhanced Open

Mit WPA3 (Wi-Fi Protected Access) hat die Wi-Fi Alliance die nächste Generation ihrer Zertifizierung für WLAN-Verschlüsselung vorgestellt. Bei WPA handelt es sich nicht um ein Protokoll, sondern vielmehr um ein Zertifizierungsverfahren, bei dem gewisse Standards erfüllt werden müssen, um zum Beispiel mit „WPA2" zertifiziert zu werden.

Viele Jahre war WPA2 der Stand der Technik zur einfachen Absicherung von Drahtlosnetzwerken. Doch dann kam 2017 die KRACK-Sicherheitslücke und fügte WPA2 einen merklichen Imageschaden zu. Diese Alterserscheinungen von WPA2 machten deutlich, dass es nach über einem Jahrzehnt Zeit ist für eine Überarbeitung: WPA3. Aufbauend auf der weit verbreiteten Vorgängerversion WPA2 werden im Wesentlichen eine robustere Authentifizierung und eine erhöhte Verschlüsselungsstärke für sensitive Daten geliefert. WPA2-Geräte werden zwar nicht von der Benutzung ausgeschlossen, jedoch nutzen sie dann auch nicht die neuen sicheren Protokolle.

WPA3-Personal und Enterprise

Wie auch bei WPA und WPA2 erscheint WPA3 in einer „Personal"-Version für den privaten Gebrauch und als „Enterprise"-Version für Unternehmen. Der Unterschied zwischen den beiden Ausgaben liegt in den WLAN-Schlüsseln: Während bei WPA3-Personal die WLAN-Router, Access Points und Stationen/Clients nur einen gemeinsamen Pre-Shared Key verwenden, wird in der Enterprise-Variante vom Administrator jedem Nutzer ein individueller Schlüssel zugewiesen.

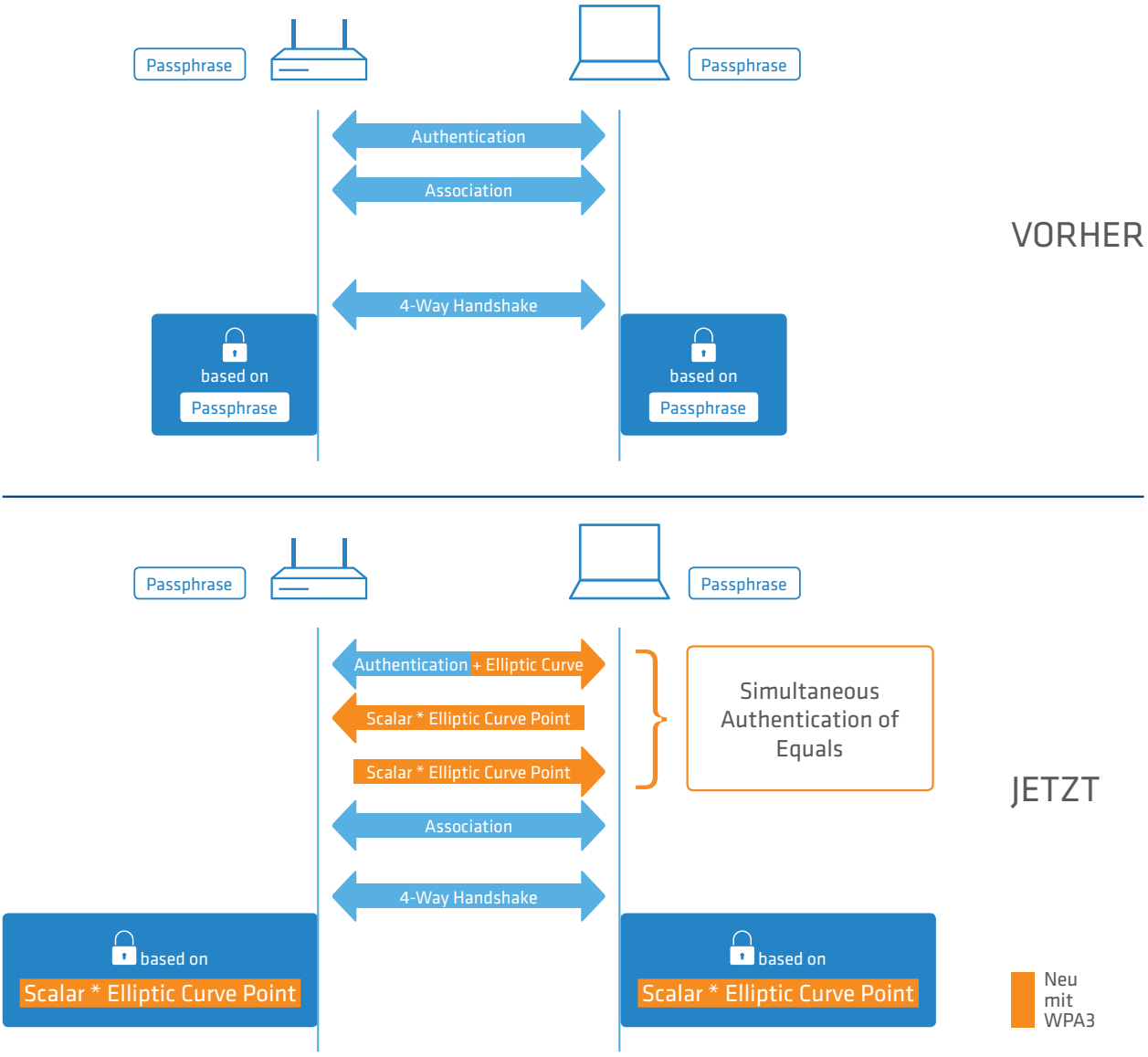
Zusätzlich läuft WPA3-Enterprise in der neuen optionalen Betriebsart mit einer 192-Bit-Chiffre. Diese Funktion ist zum Beispiel für Banken oder Regierungsbehörden interessant, wo in sicheren Netzen sensible Daten übertragen werden müssen.

Mit WPA3 werden nun auch konsequent unsichere Protokolle, beispielsweise Temporal Key Integrity Protocol (TKIP), ausgeschlossen. Bei der Zertifizierung prüft die Wi-Fi Alliance explizit, ob Geräte diese Vorrausetzung erfüllen. Damit möchte man auf die Schwäche von WPA2 reagieren, das potentiell anfällig ist für Brute Force-Attacken, bei denen das Passwort nachträglich erraten wird. Somit kann mitgeschnittener Datenverkehr bei WPA2 nachträglich entschlüsselt werden. Mit WPA3 ist dies nicht mehr möglich. Es wird ebenso überprüft, ob die Geräte gegen die KRACK-Attacken geschützt sind. Auch Sicherheitslücken, die Man-in-the-middle-Attacken wie KRACK ermöglichen, wodurch man ohne Passwortkenntnis die Daten entschlüsseln kann, werden mit WPA3 geschlossen.

Simultaneous Authentication of Equals

Eine Neuerung ist zudem der sogenannte „Dragonfly-Handshake“ oder auch „Simultaneous Authentication of Equals“. Dieses Verfahren wird bereits in Mesh-Netzwerken nach IEEE 802.11s benutzt und ist somit etabliert. Die eben genannten Brute Force-Attacken sollen enorm erschwert und auch das nachträgliche Entschlüsseln von Nutzdaten verhindert werden. Dafür wird in das bisherige Authentifizierungsverfahren zwischen Station und Access Point ein Zwischenschritt eingefügt. Bei der erstmaligen Authentifizierung einigen sich beide Geräte auf eine elliptische Kurve und schicken sich unterschiedliche Punkte dieser Kurve zu. Aus diesen Punkten wird dann ein neuer, gemeinsamer Schlüssel generiert, der über Hashes verifiziert wird. Ziel ist es, dass später bei den zugrundeliegenden Daten für den individuellen Übertagungsschlüssel das eigentliche Passwort nicht mehr vorkommt. An die Stelle des Passworts rückt nun der gemeinsame Schlüssel auf Basis der elliptischen Kurve.

Somit werden auch aufgezeichnete Datenübertragungen mit schwachen Passwörtern weniger angreifbar durch Brute Force-Attacken. Nichts desto trotz sollten natürlich weiterhin lange und komplexe Passwörter genutzt werden.



Easy-Connect und IoT

Unabhängig von WPA3 gibt es eine weitere Neuerung unter den WLAN-Authentifizierungsverfahren, den Easy-Connect-Modus, welcher eine eigenständige Zertifizierung ist. Dieser ist speziell erdacht für Clients, die lediglich eine rudimentäre oder gar keine Benutzeroberfläche haben. Vor dem Hintergrund des wachsenden Markts des Internet of Things (IoT) eine logische Neuerung. So werden Nutzer in Zukunft zum Beispiel mittels ihres Smartphones beliebige Geräte in das WLAN einbinden können. Wie zum Beispiel Waschmaschinen oder andere Haushaltsgeräte. Mithilfe einer App kann dann der jeweils QR-Code des Gerätes und des Access Points gescannt werden. Auf diese Weise werden zunächst beide Gerätedaten erfasst und danach automatisch gekoppelt.

Wi-Fi CERTIFIED Enhanced Open

Zudem hat die Wi-Fi Alliance das Zertifizierungsprogramm Wi-Fi Certified Enhanced Open eingeführt. Dies soll neue Vorteile für Nutzer in offenen WLAN-Netzwerken bringen. Enhanced Open verbessert den Datenschutz und gewährleistet gleichzeitig einfache Benutzbarkeit bei Szenarien, in denen keine Authentifizierung im WLAN-Netzwerk gefordert wird, wie zum Beispiel Cafes, Hotels, oder an öffentlichen Plätzen.

Das Protokoll „Opportunistic Wireless Encryption" (OWE) ermöglicht Wi-Fi Enhanced Open Verschlüsselungsmechanismen, die jedem Benutzer eine individuelle Verschlüsselung bietet, ohne dass eine Authentifizierung der Clients notwendig wird. Es schützt jedoch letztendlich nicht vor Man-In-The-Middle-Attacken wie bspw. vor unbeabsichtigtem Netzzugang über Honeypot-Access-Points, da bei Enhanced Open eben keine Authentifizierung durchgeführt wird.

Enhanced Open ist somit dennoch eine Verbesserung zur herkömmlichen Situation. Aus Gründen der Abwärtskompatibilität wurde zudem der Transitional Mode eingeführt. Hierbei können sowohl altes als auch neues Verfahren parallel betrieben werden.

Fazit

	802.1X	Passphrase	Authen-tifizierung	Datenver-schlüsselung
WPA3-Personal		x	x	x
WPA3-Enterprise	x		x	x
Easy-Connect			x	x
Enhanced Open				x

Die verschiedenen Methoden, die hier vorgestellt wurden, haben gemeinsam, dass sie die logische Evolution sind, um WLAN-Verschlüsselung wieder sicher zu machen. Sowohl das Bedürfnis von Unternehmen nach einer hochsicheren, individuellen Verschlüsselung im WLAN als auch das sinnvolle Verhältnis von Sicherheit und Alltagstauglichkeit im privaten Gebrauch sind gegeben.