LANCOM White Paper

WPA3 & Enhanced Open

With WPA3 (Wi-Fi Protected Access), the Wi-Fi Alliance unveiled their new certification program for the next generation of Wi-Fi encryption. WPA is not a protocol, but rather a certification process that requires certain standards to be met in order to qualify, for example as "WPA2" compliant.

For years, WPA2 was the state of the art for securing wireless networks. When the KRACK vulnerability was reported in 2017, the image loss for WPA2 was significant. With WPA2 showing its age after more than a decade, it became clear that it was time for an overhaul: WPA3. Based to a great extent on the widely used predecessor WPA2, WPA3 delivers what is essentially a more robust authentication and increased strength of encryption for sensitive data. Although WPA2 devices are not excluded from use, they do not operate with the new secure protocols.

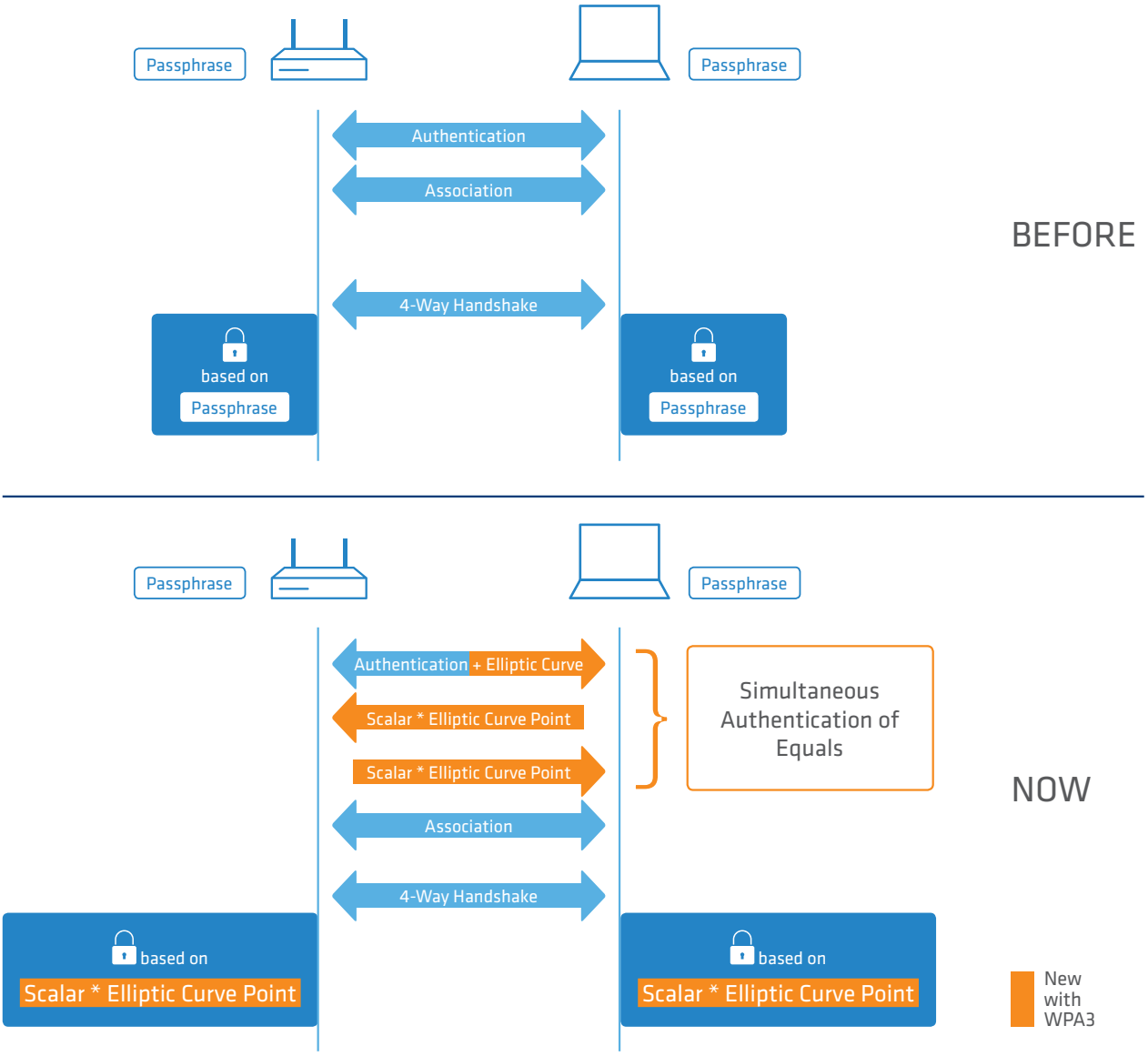
WPA3-Personal and Enterprise

As with WPA and WPA2, WPA3 comes as a Personal version for home use and as an Enterprise version for businesses and organizations. The difference between the two is the keys used for the Wi-Fi: With WPA3-Personal the Wi-Fi routers, access points and stations/clients all use a single pre-shared key, whereas the Enterprise variant allows administrators to assign an individualized key to each user.
WPA3-Enterprise also offers a the new optional operating mode with a 192-bit cipher. This feature is useful, among others, for banks or government agencies where sensitive data is transmitted over secure networks.
Furthermore, WPA3 eliminates insecure protocols such as the Temporal Key Integrity Protocol (TKIP). As a part of the certification procedure, the Wi-Fi Alliance explicitly verifies that devices meet this requirement. This is a response to the vulnerability with WPA2, which is potentially open to brute-force attacks if the password is discovered. Captured traffic that was secured with WPA2 can then be decrypted later. This is no longer possible with WPA3. The devices are also examined for protection against KRACK attacks. Security loopholes that allow man-in-the-middle attacks such as KRACK to decrypt data without knowledge of the password are also closed with WPA3.

Simultaneous Authentication of Equals

Another innovation is the "dragonfly handshake", otherwise known as the Simultaneous Authentication of Equals (SAE). This established method is used in mesh networks that are compliant to IEEE 802.11s. It makes brute-force attacks much more difficult, and it prevents offline dictionary attacks. An intermediate step was added to the authentication procedure between station and access point. When performing the initial authentication, the two devices agree on an elliptic curve and exchange different points on that curve. These points are used to generate a new shared key, which is verified using hashes. The objective is to prevent the actual password from later appearing in the underlying data for the individual key. The password is replaced by the shared key which is based on the elliptic curve.

Consequently, captured data traffic that is secured with weak passwords becomes less vulnerable to brute-force attacks. This of course is no reason to stop using long and complex passwords.



Easy Connect and IoT

Apart from WPA3, another innovation among the Wi-Fi authentication methods is the Easy Connect mode, which is a separate certification program. It was specifically designed for clients without a rich user interface, and even those without a user interface at all. This is a logical development in the light of the growing market of the Internet of Things (IoT). Users can integrate any device into the Wi-Fi with the help of their smartphone, including household appliances such as fridges or washing machines. An app is used to scan the QR codes of the device and the access point. Once identified, the devices are paired automatically.

Wi-Fi CERTIFIED Enhanced Open

Also new from the Wi-Fi Alliance is the certification program Wi-Fi Certified Enhanced Open. This benefits users of open Wi-Fi networks. Enhanced Open improves privacy while being easy to use in scenarios where authentication with the Wi-Fi network is not required, such as in cafés, hotels, or in public places.

The Opportunistic Wireless Encryption (OWE) protocol enables Wi-Fi Enhanced Open encryption mechanisms, whereby each user benefits from individualized encryption without the need for client authentication. Ultimately this does not protect against man-in-the-middle attacks, such as unintentional network access via honeypot access points, since Enhanced Open requires no authentication.
Still, Enhanced Open is an improvement to the situation we had so far. Furthermore, the transitional mode was introduced in the interests of backwards compatibility. This allows the old and new methods to operate in parallel.

Summary

	802.1X	Passphrase	Authen-tication	Data encryption
WPA3-Personal		x	x	x
WPA3-Enterprise	x		x	x
Easy Connect			x	x
Enhanced Open				x

The various methods described here represent a logical evolution that re-establishes the security of Wi-Fi encryption. They meet the needs of businesses and organizations for highly secure, individualized encryption in the Wi-Fi network, and they provide a useful balance between security and practicality in private networks.

LANCOM, LANCOM Systems and LCOS are registered trademarks. All other names or descriptions used may be trademarks or registered trademarks of their owners. Subject to change without notice. No liability for technical errors and/or omissions. 08/2018

LANCOM Systems GmbH I Adenauerstr. 20/B2 I 52146 Wuerselen I Germany I E-mail info@lancom.de

LANCOM Systems