Farah Alhamzawi

Mr.Green

Independent Study and Mentorship

26 January 2024

Analysis over WPA3

Hoelscher, Penny. “What Is WPA3? Is WPA3 Secure and Should I Use It?” Comparitech, 27 Aug. 2018, www.comparitech.com/blog/information-security/what-is-wpa3/#:~:text=In%20June%2018%2C%20Wi-Fi%20Alliance%C2%AE%20announced%20the%20introduction. Accessed 1 Feb. 2024.

The article "What is WPA3, is it secure and should I use it?" discusses WPA3, the Wi-Fi Protected Access protocol introduced in June 2018 as a successor to the previous WPA2. WPA aims to focus on the vulnerabilities present in WPA2, specifically the KRACKS, which stands for critical reinstallation attacks, which are severe replay attacks and a form of a man-in-the-middle attack. WPA3 comes in Personal and Enterprise editions, addressing the inherent flaw in WPA2, providing a solution to KRACK, and simplifying and securing the connection of IoT Wi-Fi devices. The KRACK flaw is detailed as a problem with the WPA2 certification standard itself, leading to the development of WPA3 as a solution.

By highlighting the significance of WPA3 certification for Wi-Fi devices by comparing it to a roadworthy car certificate, the article emphasizes the importance in claiming compliance

with Wi-Fi Alliance's security standards. While WPA3 became mandatory for all new Wi-Fi-certified devices in 2020, some older devices may need more support for WPA3 despite receiving software updates.

The article then digs into the analysis of WPA3's security, specifying that while it is a step in the right direction, more is needed to protect Wi-Fi networks entirely. Users are encouraged to implement a multi-faceted, layered security strategy to cover all aspects of their Wi-Fi network. The article also mentions the criticisms leveled at WPA3, suggesting that its improvements go a long way in plugging other Wi-Fi security holes.

The extent of the KRACK vulnerability is discussed, noting that, as of the article's writing, there have been no documented KRACK attacks in the wild since the introduction of WPA3. However, there are still unpatched devices that could be vulnerable. The article compares the security levels of different Wi-Fi encryption standards, including WEP, open networks, WPA, WPA2, and WPA3.

A detailed analogy explains the flaws in handshaking negotiations, where an access point and router authenticate a client's credentials, which lies at the heart of the WPA2 vulnerability. The primary vulnerability in WPA2, the four-way handshake, is discussed, and the article introduces the Simultaneous Authentication of Equals (SAE) handshake in WPA3 as a replacement for the Pre-Shared Key (PSK) in WPA2.

The article explains the differences and security features of the two versions of WPA3, namely WPA3-Personal and WPA3-Enterprise. It then outlines four new features introduced in WPA3 to enhance security, including the Simultaneous Authentication of Equals (SAE) protocol,

replacement of Wi-Fi Protected Setup (WPS), unauthenticated encryption using Wi-Fi Enhanced Open, and more extensive session key sizes in WPA3-Enterprise.

The security features of SAE are detailed, highlighting its resistance to brute force attacks, enabling forward secrecy, and limiting password guesses per session. The Wi-Fi CERTIFIED Easy Connect and Device Provisioning Protocol (DPP) are introduced as solutions for managing networks and IoT devices. Opportunistic Wireless Encryption (OWE) is discussed to provide safer hotspot surfing with unauthenticated encryption.

The article concludes with cautions and warnings from the researchers who discovered the KRACK flaw, emphasizing that WPA3, while an improvement, may be partially foolproof. The importance of staying up-to-date with patches and following security best practices, including strong passwords and multi-layered security, is stressed. The article provides Wi-Fi security tips for home networks and IoT devices and discusses potential vulnerabilities and attacks on unsecured networks. The need for a layered approach to Wi-Fi security and the importance of staying informed about potential risks are highlighted.

While I was reading this article, I found that I was able to gain more information about what WPA truly is and its importance, as well as a new point to talk about in the penetration testing guide.