Comparative Analysis of Wpa, Wpa2, And Wpa3

Seyidova Irada, Karatova Diana

Abstract

WPA (Wi-Fi Protected Access) to WPA2 and now WPA3 wireless network security protocols have substantially improved encryption algorithms, authentication procedures, and overall security.(1) Understanding the key differences between these protocols is crucial for securing wireless networks in today's digital environment.

Keywords: WPA, WPA2, WPA3, wireless network security, encryption protocols, authentication methods.

A top priority has been placed on preventing unwanted access to wireless networks due to the growing use of these networks for data transfer and communication.(2) Several security protocols have been created over time to address flaws in earlier protocols; the most popular ones are WPA, WPA2, and WPA3.(6) This thesis seeks to present a comparative analysis of various protocols, as indicated in Table 1, emphasizing the differences between them in terms of encryption algorithms, authentication techniques, and general security(3)

Table 1. Key differences between WPA, WPA2, and WPA3.

Protoco	Encryption Algorith	Authentication Method	Overall Security
WPA	Temporal Key Integri Protocol (TKIP)(6)	Pre-Shared Key (PSK	Less secure than WPA2 and vulnerable to attacks
WPA2	Advanced Encryption Standard (AES)	802.1X/EAP	More reliable than WPA and resistant to attacks(3)
WPA3	Opportunistic Wireles Encryption (OWE)	Simultaneous Authentication of Equals (SAE)	Most secure and provides protection against various attacks(2)

Algorithms for encryption. The Temporal Key Integrity Protocol (TKIP) encryption technique used by WPA has been revealed to have a number of security issues, including the ability to reuse keys and being vulnerable to attacks. (4) The Advanced Encryption Standard (AES), on the other hand, is a far more secure encryption method used by WPA2 and is regarded as being more secure due to its resistance to attacks. By implementing a new encryption method known as Opportunistic Wireless Encryption (OWE), WPA3 raises the bar for encryption and improves security.(8) OWE enables individual data encryption for each user, even in open networks.(1)

Methods of authentication. Pre-shared key (PSK) authentication, used by WPA, employs a single password to verify the identity of every device connected to the network.(7) Nevertheless, this is susceptible to password cracking or brute-force attacks. The 802.1X/EAP (Extensible Authentication Protocol) authentication mechanism, which enables each device on the network to authenticate separately, is a step up from this in WPA2. (8) Simultaneous Peer Authentication (SAE), a more robust authentication technique that defends against many attacks, including offline dictionary attacks (8), further improves the authentication process in WPA3 by building on this.

In overall security aspect. Although WPA and WPA2 offer a lot more security than earlier protocols, they still have flaws that knowledgeable attackers can take advantage of.(6) WPA3 intends to solve these flaws by bringing in a number of security improvements, like protected control frames that stop unwanted

modifications to network configurations and heightened protection for open networks.WPA3 is the most secure option among the three protocols (9) because it offers stronger defense against brute-force attacks, offline dictionary attacks, and other well-known attacks.

Conclusion

Wireless security protocols have made WPA stronger and more secure to WPA2 and now to WPA3, encryption algorithms, authentication techniques, and overall security have significantly improved.(1) WPA3, the most recent and sophisticated protocol, provides the best level of security and defense against different threats. (7) It's crucial to remember that the wireless network environment and unique security requirements determine the protocol to use. In the constantly evolving cybersecurity landscape of today, businesses and individuals alike should carefully assess their security requirements and think about upgrading to WPA3 to offer robust protection against future threats (5).

References

[1] Oloyede, S. Afolabi, and A. O. Adetunmbi. "A Comparative Analysis of WPA, WPA2 and WPA3 Security Mechanisms for Wireless Networks," in Journal of Communication and Computer Engineering, June 2021. DOI: 10.38159/jccej.2021.042

[2] Abdu, et al. "Comparative Analysis of Wireless Security Protocols: WPA, WPA2 and WPA3," in International Journal of Wireless Networks and Broadband Technologies, December 2020. DOI: 10.4018/IJWNBT.2020120102

[3] T. Gupta and A. Jain, “Security Analysis of WPA2 and WPA3 Wireless Networks,” International Journal of Computer Science and Information Security, vol. 17, no. 3, 2019.

[4] T. A. Bhatti and S. S. Choi, “Performance Analysis of WPA3 Security Protocol in IEEE 802.11ax Networks,” IEEE Access, vol. 8, 2020.

[5] Kuznetsov A. V. “Review of technologies for protecting Wi-Fi wireless networks”, Systems and Communications, No. 3 (33), 2012. Link: https://cyberleninka.ru/article/n/obzor-tehnologiy-zaschity - besprovodnyh-setey-wi-fi/viewer

[6] Chentsov A. A., "Wi-Fi. Security of wireless networks", St. Petersburg, 2010.

[7] What is Wi-Fi security? Https://www.cisco.com/c/en/us/products/wireless/what-is-wi-fi-security.html#~protocols

[8] Wi-Fi security modes and fortigate security extensions