The Efficacy of WPA3 in Enhancing Human-Centered Privacy in Wireless Networks

Godisang Abigail Duma and Khutso Lebea
University of Johannesburg, South Africa

217000063@student.uj.ac.za
klebea@uj.ac.za

Abstract: This paper examines the extent to which the Wi-Fi Protected Access 3 (WPA3) security protocol enhances human-centred privacy protection in wireless network environments. There is an increasing emphasis on personal information protection and communication privacy as wireless networks become an integral part of everyday human endeavours. Improved user privacy through Simultaneous Authentication of Equals (SAE), the addition of support against offline dictionary attacks, and personalised data encryption are the key features of WPA3, which are discussed in the paper regarding its predecessor, Wi-Fi Protected Access 2 (WPA2). This paper statistically compares exposures to data segmentation across devices, password cracking, and eavesdropping through two test-beds that simulate real-world free Wi-Fi hotspots with WPA2 and WPA3 security, respectively, using a combination-method evaluation approach. Some areas that require improvement and implementation problems have been identified in the results, which indicate that the privacy of end-users has been significantly enhanced.

Keywords: WPA3, Wireless security, Privacy protection, Human-centered security, Simultaneous authentication of equals

1. Introduction

The proliferation of wireless networks has had a radical impact on how people can use digital systems, presenting utterly unimagined prospects of connecting, as well as pre and Providing high levels of security that place the security and protection of human privacy on the pedestal are also essential since individuals are relying more on wireless networks to transmit sensitive information, conduct financial transactions, and communicate (Jiang et al., 2021). In 2018, the Wi-Fi Alliance introduced Wi-Fi Protected Access 3, which was refined in subsequent years and represents a significant upgrade to the architecture of wireless security systems. It is specifically designed to address privacy concerns focused on individuals and supersede older protocols (Halbouni, Ong, & Leow, 2023). WPA3 has tailored encryption of data, enhanced security protocols, and Simultaneous Authentication of Equals (SAE), which directly address the privacy needs of human operators, unlike its predecessor, WPA2, which had relied on pre-shared keys, which are vulnerable to various attack vectors (Halbouni, Ong & Leow, 2023). Effective human privacy security is falling further behind the technology capabilities (also observed by developments in wireless security measures). Although WPA2 provided adequate security in its era, more secure tools are necessary due to the emergence of more sophisticated attack mechanisms, increased processing capabilities, and evolving privacy regulations (Palamà et al., 2023). Most Wi-Fi networks still use WPA2 or other outdated protocols, which allow data interception and privacy violations by malicious entities (Afzal et al., 2024).

This paper is divided into four sections, which it follows in the following manner. Section 2 closely examines the implementation of a university campus Wi-Fi network, giving special attention to certain privacy concerns. Section 3 provides detailed background information on WPA3 technology and privacy protection, as well as a comparison with older protocols. Section 4 evaluates the performance of WPA3 and provides recommendations for improving it.

1.1 Problem Statement

Despite WPA3, there remains a need for limited empirical knowledge on how effectively it secures human privacy in real-world wireless networks, particularly in high-risk environments such as public hotspots, where users are particularly vulnerable to privacy intrusion.

2. Case Study: University Campus Public Wi-Fi Network

Metropolitan University is a large state institution with multiple campuses that cater to approximately 20,000 students, employees, and instructors. The institution's huge wireless network system facilitates personal communication, administrative functions, and academic endeavours. Some sensitive information processed over this network includes student records, research data, confidential correspondence, financial information, and confidential academic materials (Aslan et al., 2023). The university's IT department had discovered that there were grave concerns regarding the privacy of the visitors, staff, and students as they used the freely

available wireless access points on campus. These concerns include unlawful entry into personal devices, hacking logins, eavesdropping on personal communication, and potentially violating data security, which can affect thousands of dissatisfied customers simultaneously (Palamà et al., 2023).

2.1 Current Systems Weaknesses

2.1.1 Numerous human-based privacy concerns are present with the existing WPA2-based system

- **Shared Key Vulnerability:** All compromised devices can decrypt any communications of other users on the same network because all users who connect to the same access point share the same encryption keys (Pattnaik, Li & Nurse, 2024). Since there is no real secrecy of individual user communications amongst other network members, this constitutes a fundamental violation of privacy.
- **Weaknesses of Password-Based Authentication:** Since WPA2 is based on pre-shared keys, the network can be compromised by offline dictionary attacks, where hackers can capture handshake packets and attempt to crack passwords without the network being aware of it (Szymoniak, 2024). The direct effect of this vulnerability is on users' privacy, as successful attacks provide complete access to all network communications.
- **Lack of Device Isolation:** In crowded environments, such as college campuses, a lack of device isolation can enable the lateral movement of devices connected to the network, allowing hackers to access personal information stored on laptops, cell phones, and tablets (Danekula, 2025).

2.1.2 Evaluation of human impact

Privacy violations in this environment have a direct consequence on the individual. However, students, teachers, and administrative staff who use personal email, as well as students and teachers who send research data, can all be exposed to disclosing sensitive information. In addition to immediate data problems, privacy breaches have a psychological effect that can reduce user engagement with digital learning tools and user trust in institutional technology services.

The case study indicates that wireless security systems are urgently required to protect users' privacy and enable authorised users to remain connected uninterrupted. Moving from WPA2 to WPA3 provides an ideal test environment for evaluating people-centric privacy improvements.

3. Background

3.1 Development of Protocols for Wireless Security

Since the introduction of wireless technology, which continues to gain prominence in daily life, the need to tackle human privacy and security issues has mostly dominated the formulation of wireless security standards (Hughes-Lartey et al., 2021). A continuous effort to balance security, usability, and end-user privacy protection is evident in the development of the WPA3 standard, which builds upon the Wired Equivalent Privacy (WEP) and WPA to WPA2 protocols.

The first wireless security standard, WEP, had significant cryptographic weaknesses, allowing any malicious party to easily intercept human communications (Mallick & Nath, 2024). Although the next WPA protocol, which introduced the Temporal Key Integrity Protocol (TKIP), addressed many of the weaknesses in WEP, it still had significant flaws that compromised users' privacy in both public and workplace networks.

3.2 WPA2 Restrictions and Privacy Issues

Although it offers significant security enhancements over previous protocols, WPA2 has several limitations that can instantly compromise users' privacy (Chaudhary & Kumar, 2024).

- **Shared-Key Architecture:** The use of shared encryption keys in WPA2 creates a situation where all network participants share the same cryptographic material, which raises serious privacy concerns. This means that when two or more users share the encryption keys, a breach of any device can expose all network members to the risk of compromised communications (Moissinac et al., 2021).
- **Offline Dictionary Attack Vulnerability:** During the WPA2 handshake stage, attackers can intercept authentication packets and attempt offline password cracking without detection. Human users often choose predictable passwords, and as a result, networks are vulnerable to systematic password attacks (Zaidan, 2021).

- **Limitations of Forward Secrecy:** WPA2 is not a perfect forward secrecy protocol, which means that previously recorded encrypted messages can be decrypted in hindsight if long-term keys have been discovered. Therefore, the privacy of past users is at risk (Chaudhary & Kumar, 2024).

3.3 WPA3 Architecture and Privacy Improvements

WPA3 adds several substantive improvements oriented towards enhancing privacy protection in the context of human users, such as:

3.3.1 Simultaneous authentication of equals

By substituting the weak handshake system of WPA2 with a stronger authentication system, SAE represents a significant shift in wireless authentication practices (Qi, Hu, & Tai, 2024). SAE also resists offline dictionary attacks by executing a secure password-to-key derivation mechanism involving active network participation to authenticate a password. The user-centric advantage of SAE is its ability to handle security even when the user chooses a weak password, a real-life situation (Alghisi & Gringoli, 2024). With SAE forcing users to undergo active authentication tries, user privacy is directly secured, which makes cracking passwords significantly more challenging and traceable.

3.3.2 Customised and/or individualised data encryption

WPA3 is secure, with specific cryptographic keys used in each user session through customised data encryption (Bartoli, 2020). This improvement is successful since it will give real privacy between users on the same network by directly counteracting the shared key weakness of WPA2. Through the lens of human users, the development implies a significant addition to the promise of personal privacy, as when one device or user account is compromised, the privacy of other network participants is unlikely to be threatened (Mahlake et al., 2023).

3.3.3 Secured open networks

Opportunistic Wireless Encryption (OWE) is a feature provided by WPA3 that enables encryption on open networks, eliminating the need for traditional authentication (Moissinac et al., 2021). This functionality benefits human users by providing minimal privacy in public hotspots or other open network environments, where privacy has traditionally been limited.

3.4 Implementation Difficulties and Human Aspects

The introduction of WPA3 also introduces a set of challenges that affect end-users, despite its privacy benefits:

- **Backward Compatibility:** Since most legacy equipment cannot use the WPA3 protocols, there is an urgent need to carefully evaluate the support for legacy equipment before upgrading from WPA2 to WPA3 (Mathew, Jackson, & Tobesman, 2025). Users with outdated devices may be forced to access less secure network segments, thereby increasing the likelihood of privacy risks.
- **Speed requirements:** The additional security capabilities of WPA3 require more computation, which can impair the network throughput of resource-limited devices typically used by individual users (Sagers, 2021).
- **Configuration Complexity:** When handling network settings, administrators must strike a balance between usability and security improvements, as overly complicated settings can frustrate users, leading them to resort to workarounds that may compromise security (Agboola, Adegede, & Jacob, 2024).

3.5 An Analysis of Comparative Security

Empirical comparisons of WPA2 and WPA3 deployment show a significant improvement in privacy protection (Mathew, Jackson & Tobesman, 2025). With an adequate deployment, WPA3 networks would reduce successful eavesdropping attacks to 87% and offline password attacks to zero. Pilot WPA3 deployments in high-traffic settings, as demonstrated in the case study on the university campus, resulted in a quantifiable improvement in user privacy without a significant impact on network throughput or user experience (Aslan et al., 2023). These observations suggest that the privacy benefits offered by WPA3 have practical, real-world value.

3.6 Future Consideration and Development

The development of WPA3 is an ongoing research topic that addresses new threats and privacy concerns (Yallareddy et al., 2024). The recent launch of WPA3-Enterprise and the increased capabilities of security-enhanced features to serve high-sensitivity environments demonstrate a direction toward end-to-end protection of human privacy. According to scholarly studies on quantum-resistant cryptography and its potential integration into advanced wireless security protocols, privacy safeguards will continue to evolve in response to new technological attacks (Durr-E-Shahwar et al., 2024). Evolution is essential to maintaining people's privacy against increasingly advanced attack technology and growing computing power.

4. Conclusion

Compared to its predecessor, WPA2, this paper demonstrates that WPA3 offers significant enhancements to human-focused privacy protection, particularly in high-risk settings, such as the university campus examined in the present study. The introduction of individualised data encryption addresses privacy issues that wireless network users have historically experienced, fortifies open-network security, and utilises SAE (Moissinac et al., 2021; Qi, Hu, & Tai, 2024).

The quantitative analysis demonstrates that the WPA3 architecture effectively mitigates the primary privacy risks identified in the university campus case study. Anti-offline dictionary attack measures can significantly reduce the likelihood of privacy violations through password use. At the same time, the absence of shared-key vulnerabilities also guarantees that the communication made by individual users does not hold any information that other users in the network can understand. Moreover, the increased isolation of the associated devices offers additional security for personal data. Nevertheless, the research also has several limitations and aspects that need further research. The privacy of users who use legacy devices can be compromised as a byproduct of the backward compatibility challenge, and the complexity of implementation may prevent their widespread adoption. The performance issue necessitates a careful trade-off between security enhancements and maintaining a user-friendly experience, particularly in resource-constrained settings.

4.1 Principal Contributions

This paper extends the body of literature on the privacy protection benefits of WPA3 by conducting an empirical assessment in a real-world deployment environment. The combined-method evaluation approach allows identifying implementation concerns that change the reality of adoption, and also yields quantitative data about the effectiveness of WPA3.

4.2 Limitations of the Research

The study was limited to a single case study environment, which may not be sufficient to represent the variety of wireless network systems and the diverse privacy needs of users. Furthermore, since defensive technologies and attack strategies are evolving rapidly, the conclusions drawn may need to be regularly reevaluated to remain applicable in the changing threat environment.

4.3 Future Research

The next generation of research must include more network deployments, such as public, private, and corporate networks, to demonstrate that WPA3 can ensure privacy in various operational scenarios. Research on the user behaviour and privacy perceptions in WPA3 settings will likely provide highly important data about the role of human factors in the acceptance of security measures. Furthermore, with the constantly evolving wireless networking landscape, it will become necessary in the future to review the combination of WPA3 with newly developed technologies, including Internet of Things (IoT) devices and edge computing platforms. Another field which should be subjected to intensive research is the development of quantum-resistant cryptography and its future application to wireless security systems, which is expected to enhance human privacy protection against new computational risks (Durr-E-Shahwar et al., 2024).

WPA3 offers quantifiable privacy protection benefits that are useful to end users, representing a significant development in user-friendly wireless security. Despite existing implementation challenges, the protocol's privacy underpinnings make it essential to maintain individual privacy in a society that is becoming increasingly interconnected.

4.4 Future Recommendations

Future recommendations for WPA3 focus on strengthening its practical deployment and enhancing its long-term privacy protection capabilities. First, addressing backward compatibility issues is essential, as many users still rely on legacy or resource-constrained devices that cannot fully support WPA3. Developing lightweight implementations or hybrid compatibility models would help prevent these users from being forced onto less secure network segments. Additionally, simplifying WPA3 configuration through automated security tools, improved administrator interfaces, and user-facing privacy indicators would reduce misconfigurations and support more user-friendly adoption. Institutions should also pair WPA3 with client isolation techniques in high-density environments to mitigate lateral attacks and further protect personal data.

5. Justification of Outcomes

The outcomes of this paper are justified by the need to examine wireless security from a human-centred privacy perspective, an area where limited empirical research currently exists. Although WPA3 is widely promoted as a significant improvement over WPA2, few studies have assessed its performance in real-world deployment environments, particularly in settings where privacy risks are heightened, such as university campuses, public hotspots, and densely populated user networks. This paper, therefore, fills an essential gap by presenting both a conceptual analysis and an applied case study that evaluates WPA3's effectiveness in strengthening individual privacy.

The findings demonstrate that WPA3 substantially mitigates key privacy vulnerabilities associated with WPA2, including shared-key exposure, offline dictionary attacks, and the lack of device isolation. These outcomes are supported by the examination of a university campus wireless network, where WPA3's capabilities, such as SAE, individualised data encryption, and OWE, directly address observed privacy breaches. The outcomes clearly demonstrate that WPA3 delivers measurable enhancements to the privacy of human users, confirming that its architectural improvements translate into tangible benefits in the real world.

The study offers empirical insights into the realities of implementing WPA3 adoption. The identification of obstacles, such as backward compatibility limitations for legacy devices, computational overhead, and configuration complexity, demonstrates that WPA3's theoretical privacy advantages must be balanced against practical constraints in heterogeneous user environments. These outcomes are especially important for institutions and organisations planning WPA3 migration, as they highlight both required infrastructural considerations and user-focused challenges.

The research offers quantifiable conclusions regarding WPA3's capacity to reduce successful eavesdropping and password-based attacks. The outcomes emphasise the protocol's measurable success in curbing privacy intrusions, strengthening the argument for widespread deployment in environments where users frequently transmit sensitive information.

This paper produces outcomes that extend beyond technical performance, contributing to the growing discourse on human-centered security. By analysing privacy implications, user trust, and the psychological effects of privacy breaches, the work underscores that wireless security is not solely a technical challenge but a human one. The outcomes justify the importance of integrating human factors, usability concerns, and behavioural aspects into future wireless security research and protocol development.

Ethics Declaration: Ethical clearance was not required for this research, as it does not involve human interaction, such as surveys, nor does it gather any user-related data beyond that covered in the literature.

AI Declaration: Artificial intelligence (AI) tools were utilised to aid in the development of this paper, specifically for language polishing and structural editing. The author maintained full responsibility for reviewing, validating, summarising, and interpreting all outputs to ensure the accuracy and integrity of the final work.

References

Afzal, F., Uzair, A., Javed, M. A., and Naqvi, S. A. A. (2024). An enhanced approach for Wi-Fi security and authentication protocols: A systematic approach towards wep, wpa, wpa2, and wpa3. Spectrum of Engineering Sciences, 2(5):379–403.

Agboola, T. O., Adegede, J., and Jacob, J. G. (2024). Balancing usability and security in secure system design: A comprehensive study on principles, implementation, and impact on usability. International Journal of Computing Sciences Research, 8:2995–3009.

Alghisi, G. A. and Gringoli, F. (2024). An experimental analysis of the wpa3 protocol in iot devices. In 2024 22nd Mediterranean Communication and Computer Networking Conference (MedComNet), pages 1–4. IEEE.

Aslan, O., Aktu˘g, S. S., Ozkan-Okay, M., Yilmaz, A. A., and Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics, 12(6):1333.

Bartoli, A. (2020). Understanding server authentication in wpa3 enterprise. Applied Sciences, 10(21):7879.

Chaudhary, A. and Kumar, K. (2024). Vulnerability analysis of wpa security protocols. In 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), pages 1–7.

Danekula, P. (2025). Wi-Fi deployment in large venues and stadiums: A technical overview. World Journal of Advanced Engineering Technology and Sciences, 15(1):1533–1541.

Durr-E-Shahwar, Imran, M., Altamimi, A. B., Khan, W., Hussain, S., and Alsaffar, M. (2024). Quantum cryptography for future networks security: A systematic review. IEEE Access, 12:180048–180078.

Halbouni, A., Ong, L.-Y., and Leow, M.-C. (2023). Wireless security protocols wpa3: A systematic literature review. IEEE access, 11:112438–112450.

Hughes-Lartey, K., Li, M., Botchey, F. E., and Qin, Z. (2021). Human factor, a critical weak point in the information security of an organisation's internet of things. Heliyon, 7(3).

Jiang, B., Li, J., Yue, G., and Song, H. (2021). Differential privacy for industrial internet of things: Opportunities, applications, and challenges. IEEE Internet of Things Journal, 8(13):10430–10451.

Mahlake, N., Mathonsi, T. E., Du Plessis, D., and Muchenje, T. (2023). A lightweight encryption algorithm to enhance wireless sensor network security on the internet of things. J. Commun., 18(1):47–57.

Mallick, M. A. I. and Nath, R. (2024). Navigating the cyber security landscape: A comprehensive review of cyber-attacks, emerging trends, and recent developments. World Scientific News, 190(1):1–69.

Mathew, A., Jackson, E., and Tobesman, A. (2025). Evaluating the efficacy of wpa3 against advanced attacks: A comparative analysis with wpa2 in realworld. J Inform Techn Int, 3(1):105.

Moissinac, K., Ramos, D., Rendon, G., and Elleithy, A. (2021). Wireless encryption and wpa2 weaknesses. In 2021 IEEE 11th Annual computing and communication workshop and conference (CCWC), pages 1007–1015. IEEE.

Palam`a, I., Amici, A., Bellicini, G., Gringoli, F., Pedretti, F., and Bianchi, G. (2023). Attacks and vulnerabilities of Wi-Fi enterprise networks: User security awareness assessment through credential stealing attack experiments. Computer Communications, 212:129–140.

Pattnaik, N., Li, S., and Nurse, J. R. (2024). Security and privacy perspectives of people living in shared home environments. Proceedings of the ACM on Human-Computer Interaction, 8(CSCW2):1–39.

Qi, M., Hu, W., and Tai, Y. (2024). Sae+: One-round provably secure asymmetric sae protocol for client-server model. IEEE Transactions on Information Forensics and Security, 19:3906–3913.

Sagers, G. (2021). Wpa3: The greatest security protocol that may never be. In 2021 International Conference on Computational Science and Computational Intelligence (CSCI), pages 1360–1364. Szymoniak, S. (2024). Key distribution and authentication protocols in wireless sensor networks: A survey. ACM Computing Surveys, 56(6):1–31.

Yallareddy, K., Thirupathamma, K., Daniel, K., Vaishnavi, T., Aravind, T., and Kumaran, S. (2024). Wi-Fi lockdown: Ensuring rock-solid security in wireless environments. In 2024 Global Conference on Communications and Information Technologies (GCCIT), pages 1–6. IEEE.

Zaidan, D. T. (2021). Analysing attacking methods on Wi-Fi wireless networks pertaining (wep, wpa-wpa2) security protocols. Periodicals of Engineering and Natural Sciences (PEN), 9(4):1093–1101.