

Enhancing Security of Wireless Home Network from Deauthentication Attack

Siti Najihah Elia Che Rashid, Mohd Faris Mohd Fuzi*

College of Computing, Informatics and Mathematics,
Universiti Teknologi MARA, Perlis Branch, Arau Campus.

*Email: farisfuzi@uitm.edu.my

Keywords: deauthentication, wireless, secure, encryption.

1. Introduction

Wireless home networks are integral to modern living, connecting numerous devices for work, education, and entertainment. (Baluni et al., 2022) However, these networks are vulnerable to deauthentication attacks, which exploit Wi-Fi protocol weaknesses to disrupt connectivity and potentially gain unauthorised access. This research aims to enhance wireless home network security through two primary objectives: first, to develop a secure wireless network setting by implementing advanced security measures; second, to evaluate the network's security level against deauthentication attacks. The novelty of this research lies in its comprehensive approach, combining WPA3 protocol, AP isolation, and strong password policies to create a robust defence framework. By addressing this critical issue, the study seeks to significantly improve the reliability and security of home wireless networks.

2. Methodology

This research uses a two-scenario approach to assess wireless home network security against deauthentication attacks. In the first scenario, a router with default settings undergoes a deauthentication attack using Aircrack-ng, and the impact on network connectivity is recorded. (Baray & Kumar Ojha, 2021a). In the second scenario, the router is configured with WPA3 for robust encryption, AP isolation to prevent device-

to-device communication, and strong password policies. The same deauthentication attack is then executed to test the network's resilience under these enhanced security measures. Comparing the results from both scenarios allows for evaluation of the improved security provided by the advanced settings.

3. Results & Discussion

The results from the two scenarios provide a clear comparison of the effectiveness of advanced security settings against deauthentication attacks.

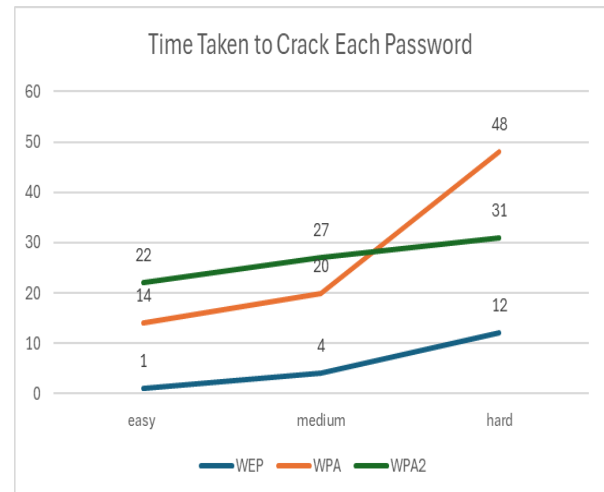


Figure 1. Result Scenario 1

From experiments evaluating the effectiveness of WPA3, AP isolation, and strong passwords in protecting a wireless home network from deauthentication attacks. Enabling WPA3 significantly improved security due to its advanced encryption and

authentication mechanisms, while AP isolation added an extra layer of protection by preventing direct device communication, though it alone was insufficient to stop attacks.

4. Conclusion

Implementing WPA3, AP isolation, and strong password policies significantly improves wireless home network security against deauthentication attacks. This research demonstrates that advanced security measures are essential for protecting network integrity and user privacy, providing a robust defence against evolving cyber threats.

References

Baluni, S., Dutt, S., Dabral, P., Maji, S., Kumar, A., & Chaudhary, A. (2022). Penetration testing on virtual machines. *2022 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, 1-6.

<https://doi.org/10.1109/ICRITO56286.2022.9964926>

Baray, E., & Kumar Ojha, N. (2021). WLAN security protocols and WPA3 security approach measurement through Aircrack-ng technique. *2021 5th International Conference on Computing Methodologies and Communication (ICCMC)*, 23-30. <https://doi.org/10.1109/ICCMC51019.2021.9418230>