

Course Title: Research Methodology in Computer Science
Course Code: AI800

Weighting: 20%

Lecturer: Dr. Mohammed Anbar

Hand-in Method: Online Submission via E-Learning.

**Assignment2 Report: Enhancing Wireless Network
Security: Bridging the Gap Between WPA2 and WPA3
Implementation.**

Student ID:221000924

Student Name: Ruba Ahmed Abusaifin

Enhancing Wireless Network Security: Bridging the Gap Between WPA2 and WPA3 Implementation.

Problem Statement:

Wireless network security is within the domain of developing encryption protocols and authentication systems effective for protecting data integrity and user privacy. The drawback of the transition from WPA2 to the more advanced WPA3 standard is the emergence of new vulnerabilities such as "Dragonblood" and downgrade attacks (Vanhoeft & Ronen, 2020). Although WPA3 was designed to eliminate the weaknesses of WPA2's 4-way handshake, its practical deployment in "Transition Mode" remains unreliable. This mode allows attackers to force connections into the weaker WPA2 standard, effectively bypassing modern security features. The widespread application of Wi-Fi in critical environments, such as corporate offices, public hotspots, and IoT ecosystems, highlights the magnitude of dealing with this issue (Rouissat et al., 2023). Identifying individuals and securing their data in different situations is essential for the performance and utility of these systems in real life.

Several existing solutions have been proposed to improve wireless security. For example, the Simultaneous Authentication of Equals (SAE) was introduced to replace the Pre-Shared Key (PSK) method,

providing resilience against offline dictionary attacks (Kohls & David, 2019). However, these solutions face limitations, particularly with low-power IoT devices that lack the computational resources to support full WPA3 encryption. Therefore, there is a need to develop a comprehensive framework that addresses these implementation gaps without compromising network performance.

Research Objectives:

To systematically address the security gaps identified in the transition from WPA2 to WPA3, this research aims to achieve the following specific, measurable, and expanded objectives:

1. **To analyze and identify** the specific technical vulnerabilities within the WPA3 "Transition Mode" that allow for protocol downgrade exploits. This involves conducting a rigorous examination of the handshake process to determine how an attacker can manipulate beacon frames to force a WPA3-capable client back to the vulnerable WPA2 standard.
2. **To evaluate and quantify** the security impact of side-channel attacks (specifically the Dragonblood vulnerability) on modern hardware. This objective focuses on measuring the success rate of password partitioning attacks and timing variations during the SAE hunting-and-pecking process across different device architectures.
3. **To propose and design** a lightweight security framework that enhances the resilience of resource-constrained IoT devices. This framework will aim to bridge the "security gap" for devices that cannot natively support WPA3, providing a secondary layer of protection that monitors and prevents unauthorized protocol changes in real-time.

4. To validate and test the proposed security solution through extensive network simulations and controlled testbeds. By using performance metrics such as Packet Delivery Ratio (PDR) and detection accuracy, the research will ensure that the proposed mitigation strategy effectively prevents exploits while maintaining optimal network efficiency and low latency.

Reference :

- **Kohls, K., & David, N. (2019).** Security Analysis of WPA3's SAE Handshake. International Conference on Network Security.
https://www.researchgate.net/publication/332151608_Security_Analysis_of_WPA3's_SAE_Handshake
- **Rouissat, M., Belkheir, M., & Mokaddem, A. (2023).** Parent supervision lightweight solution against version number attacks for IoT networks. Journal of Cybersecurity.
<https://doi.org/10.1109/JIOT.2022.3164741>
- **Vanhoef, M., & Piessens, F. (2017).** Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2. Proceedings of the 24th ACM Conference on Computer and Communications Security (CCS).
<https://www.krackattacks.com/resources/krack-paper.pdf>
- **Vanhoef, M., & Ronen, E. (2020).** Dragonblood: Analyzing the WPA3 SAE Handshake. IEEE Symposium on Security and Privacy.
<https://papers.mathyvanhoef.com/dragonblood.pdf>