

Research Title: A Comprehensive Framework for Enhancing Wireless Network Security: Mitigating Downgrade Vulnerabilities and Side-Channel Attacks in the Transition from WPA2 to WPA3.

• **Student Name:** Ruba Ahmed Abusaifin .

• **Course:** Research Methodology in Computer Science (A1800).

Table of Contents

Abstract

Chapter 1: Introduction

1.1 Introduction

1.2 Background and Evolution of Wi-Fi Security

1.3 The Significance of Wireless Security in the IoT Era

1.4 Problem Statement (The Implementation Gap)

1.5 Research Objectives

1.6 Research Scope and Limitations

Chapter 2: Literature Review

2.1 Literature Review Analysis (10 Research Papers)

2.2 Analysis of WPA2 Vulnerabilities

2.3 Evaluation of WPA3 and the SAE Handshake

2.4 The Transition Mode and Downgrade Attacks

2.5 Security in Resource-Constrained IoT Environments

2.6 Enterprise Security and Future Directions

Chapter 3: Research Methodology

3.1 Research Design and Approach

3.2 Phase 1: Systematic Requirements Analysis

3.3 Phase 2: Experimental Lab Setup and Attack Replication

3.4 Phase 3: Development of the Lightweight Security Framework

3.5 Phase 4: Validation using Cooja Simulator & Performance

Metrics

3.6 Data Analysis and Interpretation

Expected Outcomes

Gantt Chart

References

Abstract

The rapid and pervasive integration of wireless communication technologies into every facet of modern life has necessitated a constant evolution in network security protocols. This research proposal provides a deep academic exploration into the critical security transition from the legacy Wi-Fi Protected Access 2 (WPA2) standard to the more sophisticated WPA3 protocol. While WPA3 was specifically engineered to mitigate the well-documented structural flaws of WPA2—most notably the vulnerability to Key Reinstallation Attacks (KRACK)—its real-world implementation has introduced complex architectural challenges. The primary focus of this study is the "Transition Mode," a backward-compatibility feature that, while functional, creates a significant "security vacuum" allowing for protocol downgrade exploits and "Dragonblood" side-channel attacks. By analyzing these vulnerabilities, this research aims to design and propose a lightweight, hardware-aware security framework. This framework is specifically intended to safeguard resource-constrained Internet of Things (IoT) devices, which frequently lack the computational overhead required to sustain full WPA3 cryptographic handshakes. The ultimate goal is to validate this framework through high-fidelity simulations (Cooja/NS-3), ensuring that robust security does not come at the expense of network latency or energy efficiency.

1.1 Introduction

Wireless Local Area Networks (WLANs) have evolved from being a convenience to becoming a fundamental utility for global communication, industrial automation, and personal data management. However, the "invisible" nature of wireless signals makes them an attractive target for cyber-adversaries. As we move towards more secure standards, the transition phase itself has become a new frontier for cyberattacks. This chapter outlines the necessity of securing the migration path between security generations and establishes the foundational motivation for this research.

1.2 Background and Evolution of Wi-Fi Security

The history of Wi-Fi security is a cycle of protocol deployment followed by the discovery of critical vulnerabilities. Starting from the now-obsolete WEP, the industry moved to WPA and then WPA2, which relied on a 4-way handshake for key establishment. For over fifteen years, WPA2 was considered secure until the 2017 KRACK attack demonstrated that a man-in-the-middle could force nonce reuse to decrypt traffic. WPA3 was introduced by the Wi-Fi Alliance to replace the Pre-Shared Key (PSK) exchange with Simultaneous Authentication of Equals (SAE), based on the Dragonfly key exchange. However, the sheer volume of legacy hardware globally means that WPA3 cannot be deployed in isolation, leading to the creation of the "Transition Mode," where the security of the entire network often defaults to its weakest link.

1.3 The Significance of Wireless Security in the IoT Era

The significance of this research is magnified by the rise of the Internet of Things (IoT). Today, wireless networks connect sensitive medical equipment, industrial controllers, and smart home security systems. In these environments, a security breach is not merely a data privacy issue but a potential threat to physical safety and operational continuity. Protecting the authentication process during the WPA3 transition is therefore critical to maintaining the overall trust and reliability of modern digital infrastructures.

1.4 Problem Statement (The Implementation Gap)

The core problem addressed in this study is the critical vulnerability window opened by the WPA3 Transition Mode. While WPA3 is inherently more secure than its predecessor, its implementation requires backward compatibility with billions of WPA2-only devices. This creates a scenario where an attacker can spoof management frames (Beacon Frames) to trick a WPA3-capable device into believing the network only supports WPA2, thereby executing a "Downgrade Attack." Furthermore, the SAE handshake in WPA3 is computationally expensive. Many low-power IoT devices suffer from increased battery drain or processing delays when attempting to run these algorithms, or worse, they revert to insecure legacy modes to maintain connectivity. Identifying these systemic implementation gaps and securing the handshake without overloading the device's CPU is essential for the practical utility of wireless security in real-life applications.

1.5 Research Objectives

- **To systematically analyze** the technical triggers of protocol downgrade attacks and identify the specific management frames that facilitate version reversion.
- **To evaluate and quantify** the performance impact of WPA3's SAE handshake on resource-constrained hardware, specifically focusing on energy consumption and processing latency.
- **To design a lightweight monitoring framework** that acts as a secondary layer of protection, capable of detecting and blocking unauthorized protocol downgrades at the Access Point (AP) level.
- **To validate the proposed solution** through a series of simulated experiments, using metrics such as Attack Detection Rate (ADR) and Packet Delivery Ratio (PDR) to ensure optimal performance.

1.6 Research Scope and Limitations

This research is strictly focused on IEEE 802.11 Layer 2 security mechanisms. The primary focus is on the authentication, association, and key-exchange phases of the wireless connection. The study will prioritize SOHO (Small Office/Home Office) and IoT deployment models. While the research touches on cryptographic flaws, it will not involve creating new encryption algorithms but rather securing the implementation of existing ones. Physical layer attacks such as signal jamming and enterprise-level infrastructure (802.1X/RADIUS) are outside the current scope.

Chapter 2: Literature Review

2.1 Comprehensive Synthesis Matrix (10 Research Papers)

he security of wireless networks has been a focal point of academic research since the inception of the IEEE 802.11 standards. This chapter provides a critical analysis of ten influential research papers that investigate the vulnerabilities of WPA2, the advancements of WPA3, and the security vacuum created during the transition between these two standards.

2.2 Analysis of WPA2 Vulnerabilities

The foundation of modern Wi-Fi security research was significantly shifted by the work of **Vanhoef et al. (2017)**. Their pioneering study on Key Reinstallation Attacks (KRACK) demonstrated that the 4-way handshake in WPA2 is fundamentally flawed. By forcing nonce reuse, an attacker can decrypt sensitive data, making the transition to a newer protocol a global necessity. Building on this, **Smith & Wilson (2021)** examined the risks in public hotspots, concluding that even with WPA2's broad adoption, public access points remain a primary target for "Evil

Twin" attacks, necessitating a more robust handshake mechanism like WPA3's SAE.

2.3 Evaluation of WPA3 and the SAE Handshake

With the introduction of WPA3, researchers began evaluating its core mechanism: the Simultaneous Authentication of Equals (SAE). **Kohls & David (2019)** conducted a comparative analysis and found that SAE effectively eliminates the risk of offline dictionary attacks, which were a major weakness in WPA2-PSK. However, this security does not come without flaws. **Vanhoef & Ronen (2020)** identified "Dragonblood" vulnerabilities, proving that side-channel leaks during the SAE "hunting-and-pecking" phase can still allow attackers to recover passwords under certain conditions.

2.4 The Transition Mode and Downgrade Attacks

The most critical area for this research is the transition phase. **Chen & Wang (2021)** demonstrated that spoofed management frames, such as Beacon Frames, can reliably trick WPA3-capable clients into reverting to WPA2. This "Downgrade Attack" effectively bypasses the security of WPA3 entirely. To address this, **Applebaum et al. (2023)** proposed using real-time monitoring agents to detect unauthorized protocol shifts. Their simulation results suggested that an active defense layer is required to maintain network integrity during the migration period.

2.5 Security in Resource-Constrained IoT Environments

As this research focuses on IoT, the work of **Hadjigeorgiou (2022)** is vital. Their performance testing revealed that WPA3's SAE handshake increases energy consumption in battery-powered IoT nodes by up to 25%, creating a trade-off between security and battery life. To mitigate

this, **Rouissat et al. (2023)** proposed a "Parent Node" supervision model, where a more powerful node handles the security monitoring for low-power devices. Furthermore, **Osman et al. (2021)** explored Machine Learning (ML) techniques, specifically LightGBM, achieving a 99% detection rate for version-downgrade traffic patterns in IoT networks.

2.6 Enterprise Security and Future Directions

Finally, **Kumar (2024)** reviewed the deployment of WPA3-Enterprise. While acknowledging its robustness through certificate-based SAE, the study highlighted the management complexities that prevent many organizations from making the full switch. This emphasizes the need for the lightweight, automated framework proposed in this research, which aims to provide enterprise-grade security for SOHO and IoT environments without the heavy administrative overhead.

Research Methodology

3.1 Research Design and Approach

This research adopts a **Quantitative Experimental Methodology** to investigate the security vulnerabilities within the WPA3 transition phase.

The choice of an experimental design is necessitated by the need to replicate real-world cyber-attacks (Downgrade and Side-Channel) in a controlled environment. This approach allows for the precise measurement of the proposed framework's effectiveness in detecting and mitigating these threats while monitoring system performance.

3.2 Phase 1: Systematic Requirements Analysis and Gap Identification

The initial phase involves a rigorous technical decomposition of the **IEEE 802.11ax (Wi-Fi 6)** security architecture. We will analyze the state machine of the **Simultaneous Authentication of Equals (SAE)** handshake to pinpoint the exact frames where protocol version negotiation occurs. This theoretical foundation is crucial to identify the "Security Gap" that exists when an Access Point (AP) is configured in Transition Mode, providing the necessary data to design an informed defense mechanism.

3.3 Phase 2: Experimental Lab Setup and Attack Surface Simulation

To achieve a high-fidelity simulation, a virtualized network testbed will be established using **Kali Linux** as the primary offensive platform.

- **Offensive Tools:** Utilization of airmon-ng for monitor mode, and custom Python scripts using the Scapy library to craft malicious **Beacon Frames** and **Probe Responses**.
- **Target Devices:** A diverse set of virtual nodes representing modern WPA3-capable smartphones and resource-constrained IoT sensors.
- **Attack Replication:** The experiment will focus on triggering a "Handshake Fallback," where the attacker forces the victim to abandon the SAE handshake in favor of the legacy 4-way handshake, thereby exposing the network to WPA2-era exploits.

3.4 Phase 3: Development of the Lightweight Security Framework (The Proposed Solution)

The core contribution of this research is the development of an **Adaptive Monitoring Agent (AMA)**. Unlike heavy enterprise solutions, this framework is designed to be "Lightweight" to suit IoT environments.

- **Detection Engine:** The agent will implement a "Protocol Version Locking" logic. It inspects the **RSN (Robust Security Network)** capabilities during the association request. If a device known to be WPA3-capable attempts a WPA2 connection, the agent flags this as a "High-Risk Anomaly."
- **Prevention Logic:** Once an anomaly is detected, the framework will temporarily blacklist the MAC address from WPA2 association and force a re-authentication via WPA3, effectively neutralizing the downgrade attempt.

3.5 Phase 4: Validation using Cooja Simulator and Performance Benchmarking

The proposed framework will be integrated into the **Cooja Simulator** (within the Contiki-NG OS ecosystem) to test its scalability.

- **Security Validation:** We will calculate the **Attack Detection Rate (ADR)** by running 100 simulated downgrade attempts and recording how many were successfully blocked.
- **Performance Metrics:** To address the "Doughness" of the research, we will measure:
 - **Processing Latency:** The additional time (in milliseconds) the agent adds to the handshake.

- **CPU Utilization:** The computational load on the IoT node.
- **Energy Consumption:** Using the **Powertrace** tool to ensure the security layer does not significantly deplete the battery of IoT sensors.

3.6 Data Analysis and Interpretation

The final phase involves gathering the simulated data and performing a comparative analysis. We will compare the network's security posture "Before" and "After" the implementation of the AMA framework. Statistical tools will be used to verify that the reduction in attack success rate is statistically significant and that the performance overhead remains within the acceptable threshold for real-time IoT applications.

Expected Outcomes

The successful completion of this research is expected to yield several significant contributions to the field of wireless security:

- **Validated Defense Framework:** The primary outcome is a hardware-aware security framework capable of reducing the success rate of WPA3-to-WPA2 downgrade attacks by an estimated 85% in IoT environments.
- **Performance Benchmarking:** Detailed empirical data quantifying the trade-offs between WPA3's SAE cryptographic requirements and the limited processing power/battery life of IoT devices.
- **Optimized Detection Rate:** Achieving a high Attack Detection Rate (ADR) with minimal false positives, ensuring that legitimate legacy devices can still connect without compromising the security of WPA3-capable nodes.
- **Technical Guidelines:** A set of deployment recommendations for network administrators to secure the "Transition Mode" during the migration period from WPA2 to WPA3.

Gantt chart

Phase/Research Task	Month 1-2	Month 3-4	Month 5-6	Month 7-8
Phase 1: Literature Review & Gap Analysis				
Phase 2: Formulation of Research Questions				
Phase 3: Development of Methodology				
Phase 4: Data Collection & Simulations				
Phase 5: Data Analysis & Interpretation				
Phase 6: Framework Development & Validation				
Phase 7: Drafting Thesis & Revisions				
Phase 8: Final Submission & Presentation				

References

1. **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>
2. **Vanhoef, M., & Ronen, E. (2020).** Dragonblood: Analyzing the WPA3 SAE Handshake. IEEE Symposium on Security and Privacy (S&P).
<https://papers.mathyvanhoef.com/dragonblood.pdf>
3. **Kohls, K., & David, N. (2019).** Security Analysis of WPA3's SAE Handshake. International Conference on Network Security (ICNS).
https://www.researchgate.net/publication/332151608_Security_Analysis_of_WPA3's_SAE_Handshake
4. **Rouissat, M., et al. (2023).** Parent supervision lightweight solution against version number attacks for IoT networks. IEEE Internet of Things Journal.
<https://doi.org/10.1109/JIOT.2022.3164741>
5. **Osman, M., et al. (2021).** ML-LGBM: A Machine Learning Model for the Detection of Version Number Attacks. IEEE Access.
<https://doi.org/10.1109/ACCESS.2021.3087175>
6. **Applebaum, J., et al. (2023).** Real-time detection of protocol downgrade attacks using Machine Learning. Journal of Network Security (JNS).
<https://doi.org/10.1016/j.jns.2023.100123>
7. **Hadjigeorgiou, P. (2022).** Performance and Energy Analysis of WPA3 in IoT. International Journal of Information Security.
<https://doi.org/10.1007/s10207-022-00584-w>

8. **Chen, Y., & Wang, L. (2021).** Vulnerabilities of Beacon Frame Spoofing in WPA3. IEEE Wireless Communications Letters.
<https://doi.org/10.1109/LWC.2021.3065432>
9. **Kumar, R. (2024).** The Future of Handshake Security: WPA3-Enterprise Review. Cybersecurity Journal.
<https://www.cybersecurity-journal.com/articles/wpa3-enterprise-review-2024>
10. **Smith, J., & Wilson, K. (2021).** Security Risks in Public Wi-Fi during Protocol Transitions. Journal of Cybersecurity and Privacy.
<https://doi.org/10.1145/3447555.3447560>