Borneo International Journal eISSN 2636-9826; Vol.8 (2); 2025; 81-89
Published by *Majmuah Enterprise*
www.majmuah.com

A Case Study of Wi-Fi Penetration Testing: WPA2WPA3 Cracking

MUHD AMIRUL NAJHAN SHAMSUDIN, MOHAMAD FADLI ZOLKIPLI
School of Computing, Awang Had Salleh Graduate School, College of Arts and Science, Universiti Utara Malaysia (UUM), 06010 Sintok, Kedah, MALAYSIA
Email : amirul_najhan@ahsgs.uum.edu.my, m.fadli.zolkipli@uum.edu.my

Received: June 27, 2025
Accepted: June 30, 2025
Online Published: July 02, 2025

Abstract

The pervasive nature of Wi-Fi networks in both individual and organizational spheres has brought forth unparalleled convenience alongside significant cybersecurity challenges. This paper presents a systematic literature review (SLR) evaluating the contemporary landscape of Wi-Fi penetration testing, with a particular focus on cracking methodologies targeting Wi-Fi Protected Access 2 (WPA2) and Wi-Fi Protected Access 3 (WPA3) protocols. Employing an SLR approach, we synthesized findings from a comprehensive array of academic sources to identify common vulnerabilities, analyze prevalent attack vectors, and assess the efficacy of tools such as Aircrack-ng, Wireshark, and Airgeddon. Our investigation reveals that despite WPA3's advancements, including Simultaneous Authentication of Equals (SAE) and Protected Management Frames (PMF), certain vulnerabilities persist, notably through downgrade attacks, side-channel exploits, and sophisticated social engineering tactics leveraging captive portals. The findings underscore the critical need for continuous security assessments, robust mitigation strategies, and enhanced user awareness to fortify Wi-Fi network defenses against evolving threats. Future research directions are discussed, advocating for the integration of machine learning and deep reinforcement learning to automate and refine penetration testing processes, thereby improving detection accuracy and reducing response times.

Keywords: Penetration Testing; Wi-fi; Cybersecurity; WPA2; WPA3;

1. Introduction

In our modern era, marked by an increasing reliance on digital connectivity, the internet has become deeply woven into the fabric of daily life for individuals, governments, and non-governmental organizations alike [Alhamed & Rahman, 2023]. While this digital transformation offers immense opportunities, it concurrently introduces considerable security concerns. The proliferation of cybercrime, encompassing activities such as service disruption, the theft of sensitive and confidential data, and other malicious acts, poses a grave threat to organizations worldwide [Alhamed & Rahman, 2023]. Consequently, ensuring robust network protection and adherence to stringent security requirements have become paramount. Among the myriads of network infrastructures, Wireless Local Area Networks (WLANs), commonly known as Wi-Fi networks, stand out as one of the most widely adopted forms of connectivity [Alhamed & Rahman, 2023; Halbouni et al., 2023]. Their inherent convenience over wired technologies has led to widespread integration across various sectors, from education and healthcare to commercial operations and personal social interactions [Alhamed & Rahman, 2023]. However, this convenience comes with an elevated risk profile, making Wi-Fi networks a prime target for attackers [Alhamed & Rahman, 2023]. The potential damage from such attacks can range from partial to complete destruction of network infrastructure, leading to operational halts and significant financial losses [Alhamed & Rahman, 2023].

To counteract these threats, network penetration testing has emerged as a crucial security assessment technique [Alhamed & Rahman, 2023; Singh et al., 2023]. This proactive measure is designed to pinpoint risk areas and exploitable vulnerabilities within a network's operation, design, or implementation, providing essential controls for attack prevention and detection [Alhamed & Rahman, 2023]. By simulating real-world cyberattacks in a controlled and ethical manner, penetration testers, often referred to as ethical hackers, can identify weaknesses before malicious actors exploit them [Alhamed & Rahman, 2023]. This paper aims to delve into the intricate world of Wi-Fi penetration testing, specifically focusing on the methodologies and tools employed for cracking WPA2 and WPA3 security protocols. Through a systematic literature review, we seek to provide a comprehensive understanding of existing vulnerabilities, the techniques used to exploit them, and the strategies for remediation. Our objective is to contribute to the broader awareness of Wi-Fi security and to highlight avenues for future research in this continuously evolving field.

2. Background

To comprehend the nuances of Wi-Fi security and its testing, it is essential to first establish a foundational understanding of penetration testing itself and the evolution of wireless security protocols.

2.1. Penetration Testing Defined

The Penetration testing is fundamentally a proactive security measure aimed at identifying vulnerabilities in digital assets by actively searching for and exploiting them from an attacker's perspective [Alhamed & Rahman, 2023]. Its primary purpose is to help organizations achieve core cybersecurity objectives: integrity, availability, and confidentiality, a necessity in today's digital landscape, especially with regulations like the European General Data Protection Regulation (GDPR) [Alhamed & Rahman, 2023; Singh et al., 2023]. Essentially, it is an authorized, simulated cyberattack conducted by trained security experts, often referred to as ethical hackers, to reveal security weaknesses in an IT infrastructure before real attacks occur [Alhamed & Rahman, 2023]. These tests are vital for detecting existing vulnerabilities, understanding their potential impact, and devising strategies for their elimination, thereby serving as a critical risk assessment and network security verification process [Alhamed & Rahman, 2023]. Penetration tests typically follow structured methodologies, often comprising phases such as planning and preparation, assessment (which includes detection and attacking), and reporting [Alhamed & Rahman, 2023]. Common approaches include:

- Black Box Testing: Testers simulate an attack with no prior knowledge of the infrastructure, mimicking a real-world external attacker [Alhamed & Rahman, 2023].
- White Box Testing: Testers have full knowledge of the target system's infrastructure, allowing for in-depth analysis [Alhamed & Rahman, 2023].
- Gray Box Testing: Testers possess partial information, blending elements of both black and white box approaches [Alhamed & Rahman, 2023].

2.2 Evolution of Wi-Fi Security Protocols

Academic Wireless networking, based on the IEEE 802.11 standard, relies on encryption protocols to protect communications due to the open nature of wireless signals [Ye et al., 2024]. Over time, these protocols have evolved in response to discovered vulnerabilities:

- Wired Equivalent Privacy (WEP): Introduced as the first security protocol for wireless LANs, WEP aimed to provide security comparable to wired networks [Halbouni et al., 2023]. It utilized the Rivest Cipher 4 (RC4) encryption algorithm [Halbouni et al., 2023]. However, significant flaws were quickly identified, leading to its deprecation in 2004 [Halbouni et al., 2023; Ye et al., 2024]. Its main vulnerabilities stemmed from weaknesses in RC4 and the ease with which its encryption key could be compromised through attacks that computed Temporal Keys based on shared Initialization Vectors [Halbouni et al., 2023].
- Wi-Fi Protected Access (WPA): Launched in 2003 as an interim solution following WEP's weaknesses, WPA also employed RC4 but introduced improvements like Temporal Key Integrity Protocol (TKIP) for per-packet key mixing and message integrity checks [Halbouni et al., 2023; Ye et al., 2024]. Despite these enhancements, WPA was still susceptible to major flaws, particularly to brute-force attacks if weak passwords were used [Halbouni et al., 2023].
- Wi-Fi Protected Access 2 (WPA2): Released in 2004 and based on the IEEE 802.11i standard, WPA2 marked a significant enhancement in wireless security [Halbouni et al., 2023]. It replaced RC4/TKIP with the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP), which leverages the Advanced Encryption Standard (AES) block cipher for data encryption [Halbouni et al., 2023]. A crucial element of WPA2's security is the 4-way handshake, used to derive the Pairwise Transient Key (PTK) and Group Temporal Key (GTK) for authentication and encryption [Chen & Punya, 2021; Halbouni et al., 2023]. Despite its robustness, WPA2 has been extensively targeted and found vulnerable to attacks, most notably the Key Reinstallation Attack (KRACK), which allowed attackers to read previously encrypted information [Alhamed & Rahman, 2023; Mathew et al., 2025; Shen et al., 2024].
- Wi-Fi Protected Access 3 (WPA3): Announced in June 2018 and made mandatory for Wi-Fi Certified implementations by July 2020, WPA3 was developed to address the shortcomings of WPA2 and provide higher levels of security and usability [Halbouni et al., 2023]. A primary motivation for WPA3's development was to enhance the WPA2-PSK handshake [Halbouni et al., 2023]. Key features of WPA3 include:

- Simultaneous Authentication of Equals (SAE): This protocol replaces the WPA2 4-way handshake, offering a more robust method for secure connections without transmitting passwords directly. SAE uses a Password Authenticated Key Exchange (PAKE) to hash passphrases with keys from both the Access Point (AP) and the client, making it resistant to offline dictionary attacks [Chadee, 2024; Mathew et al., 2025]. It also provides forward secrecy, ensuring encrypted communication even if the passphrase is later compromised [Chadee, 2024].
- Protected Management Frames (PMF): PMF is designed to protect management traffic in WPA3 networks, defending against de-authentication and disassociation attacks that malicious parties use to disrupt service or redirect users [Mathew et al., 2025]. If PMF is not implemented, WPA3 can still be vulnerable [Chadee, 2024].
- Opportunistic Wireless Encryption (OWE): A new component in WPA3 that brings encryption to previously unprotected open networks, significantly reducing the occurrence of data interception in public Wi-Fi environments [Mathew et al., 2025].
- Modes of Operation: WPA3 offers "Personal" (WPA3-SAE) for home use and "Enterprise" (using 192-bit encryption and EAP-pwd) for highly sensitive data environments [Halbouni et al., 2023]. A "Transition Mode" (WPA2-PSK/WPA3-SAE Mixed Mode) exists to allow WPA3-only devices to connect to WPA2 networks, aiding backward compatibility [Chadee, 2024; Halbouni et al., 2023]. However, this transition mode can also be leveraged for downgrade attacks [Chadee, 2024].

Despite its advancements, WPA3 is not without its challenges, including compatibility concerns, performance impact on resource-limited devices, and susceptibility to emerging attack vectors [Mathew et al., 2025]. These aspects highlight the continuous cat-and-mouse game between security development and adversarial exploitation.

3. Literature Review

This section presents a comprehensive review of existing literature pertaining to Wi-Fi penetration testing, with a particular emphasis on vulnerabilities and cracking methods targeting WPA2 and WPA3 protocols.

3.1. Vulnerabilities in WLAN Environments

The sources underscore that despite advancements in Wi-Fi security protocols, vulnerabilities persist across various layers of network operation.

- WPA2 Vulnerabilities: The most notable vulnerability in WPA2 is the Key Reinstallation Attack (KRACK) [Alhamed & Rahman, 2023; Mathew et al., 2025; Shen et al., 2024]. This attack exploits weaknesses in the 4-way handshake, allowing attackers to force nonce reuse and decrypt information previously thought to be securely encrypted, potentially leading to the theft of sensitive data like credit card numbers, passwords, and chat messages [Alhamed & Rahman, 2023]. The KRACK attack was a primary driver for the development of WPA3 [Halbouni et al., 2023].
- WPA3 Vulnerabilities: While WPA3 significantly improves security, it is not entirely immune to attacks. Sources indicate ongoing concerns, including downgrade attacks, where attackers can force WPA3 devices to revert to weaker WPA2 protocols, and side-channel attacks, which can leak information about password conversion methods [Mathew et al., 2025; Chadee, 2024; Halbouni et al., 2023; Shen et al., 2024]. The "Dragonblood" vulnerabilities, discovered in the SAE handshake, highlight these weaknesses, potentially leading to downgrade attacks, Denial-of-Service (DoS) attacks, and side-channel password leakage [Chadee, 2024; Shen et al., 2024; Zhou et al., 2024]. Furthermore, if Protected Management Frames (PMF) are not fully implemented or are disabled, WPA3 networks remain susceptible to de-authentication and disassociation attacks [Chadee, 2024; Mathew et al., 2025].

3.2. Attack Methods and Techniques

Attackers employ a diverse range of techniques to compromise Wi-Fi networks, often combining multiple methods for greater effectiveness:

- Handshake Capture: A fundamental step in cracking WPA and WPA2 is capturing the 4-way handshake [Chen & Punya, 2021; Singh et al., 2023]. This handshake contains crucial information that, when combined with other methods, can lead to password cracking [Chadee, 2024]. For WPA3, while the SAE handshake is more robust, variations of handshake capture, sometimes preceded by downgrade attacks, are still explored [Chadee, 2024].
- Dictionary and Brute-Force Attacks: These are common methods used to guess passwords or passphrases [Chen & Punya, 2021; Singh et al., 2023; Asaad, 2017]. While WPA3's SAE is specifically designed to resist

offline dictionary attacks by making passphrase hashing more complex, online brute-force methods can still be attempted [Chadee, 2024; Mathew et al., 2025].

- De-authentication Attacks: These attacks are used to disconnect legitimate clients from an access point, forcing them to re-authenticate and thereby enabling the capture of the 4-way handshake [Chadee, 2024; Singh et al., 2023]. PMF in WPA3 aims to mitigate these by encrypting management frames [Mathew et al., 2025].
- Evil Twin / Rogue Access Point Attacks: Attackers set up fake Wi-Fi access points that mimic legitimate ones to trick users into connecting and revealing their credentials [Wang et al., 2022; Chadee, 2024; Mathew et al., 2025]. These attacks are particularly effective when combined with social engineering tactics, such as deploying captive portals that prompt users for Wi-Fi passwords [Chadee, 2024]. User susceptibility to these attacks is a significant concern, even in professional environments [Wang et al., 2022].
- MAC Spoofing: This technique involves changing a device's Media Access Control (MAC) address to impersonate another device or to anonymize the attacker's presence on the network [Singh et al., 2023; Chadee, 2024; Jin & Papadimitratos, 2024]. While MAC address randomization is designed for privacy, it can also be manipulated or exploited [Jin & Papadimitratos, 2024].
- Beamforming Feedback Forgery: A newly identified physical layer attack, BeamCraft, manipulates Wi-Fi traffic by forging clear-text beamforming feedback information (BFI). This allows an attacker to misdirect an AP's beamforming, potentially gaining higher throughput or disrupting services for other users in a covert manner [Xu et al., 2024]. This highlights a critical vulnerability in modern Wi-Fi systems that rely on beamforming for high throughput and reliability [Xu et al., 2024].

3.3. Penetration Testing Tools

Ethical hackers and security professionals rely on a variety of specialized tools, often integrated within operating systems like Kali Linux, to conduct Wi-Fi penetration tests:

- Aircrack-ng: This is a cornerstone of Wi-Fi security assessment. It is a comprehensive suite of tools used for detecting networks, sniffing packets, and cracking WEP, WPA, and WPA2-PSK keys [Alhamed & Rahman, 2023; Singh et al., 2023; Asaad, 2017]. Its capabilities extend to analyzing 802.11 wireless LANs and performing de-authentication attacks to capture handshakes [Alhamed & Rahman, 2023; Chen & Punya, 2021; Hu et al., 2021; Xu et al., 2024].
- Wireshark: An indispensable network protocol analyzer, Wireshark is used for in-depth inspection of captured network traffic [Alhamed & Rahman, 2023; Singh et al., 2023; Chadee, 2024; Hu et al., 2021; Alyami et al., 2020]. It helps in determining overhead and understanding communication patterns [Chen & Punya, 2021].
- Hashcat (or OCLHashcat): Known for its speed, Hashcat is a powerful tool for performing offline brute-force and dictionary attacks, particularly effective against Wi-Fi network hashes [Asaad, 2017].
- Airgeddon: This is a versatile wireless auditing script that automates many Wi-Fi attack scenarios. It can create rogue access points with captive portals, launch de-authentication attacks, and facilitate the capture of WPA handshakes [Chadee, 2024].
- Nmap: A widely used network scanner, Nmap helps in discovering hosts, identifying open ports, and detecting running services on a network, providing crucial reconnaissance information for penetration testers [Alhamed & Rahman, 2023; Singh et al., 2023; Ye et al., 2024].
- Kali Linux: Often described as the world's most powerful penetration testing platform, Kali Linux is an operating system that comes pre-loaded with a vast array of security tools, including many mentioned above, making it a preferred choice for ethical hackers [Alhamed & Rahman, 2023; Asaad, 2017; Singh et al., 2023].
- Raspberry Pi: These low-cost, portable mini-computers are frequently used in penetration testing for simulating WPA3 environments, deploying rogue networks, and performing on-field activities due to their size and affordability [Chadee, 2024; Huang & Lin, 2018].

The literature highlights that while automated tools are efficient for initial scans, manual penetration testing remains crucial for uncovering business logic vulnerabilities and rare cases that automated scanners might miss [Alhamed & Rahman, 2023]. This blend of automated and manual techniques ensures a comprehensive security assessment.

4. Methodology

To systematically evaluate the tools and methods used in Wi-Fi security testing, particularly for WPA2/WPA3 cracking, this study employed a Systematic Literature Review (SLR) methodology. This approach allows for a comprehensive, transparent, and reproducible synthesis of existing research, ensuring that all relevant and high-quality evidence is identified, analyzed, and summarized. The framework for this SLR was primarily guided by the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines, a widely recognized standard in academic research for conducting robust literature reviews [Alhamed & Rahman, 2023].

Our systematic review process comprised the following key phases:

4.1. Planning Phase

This initial phase involved defining the research questions and developing a detailed review protocol.

i. Research Questions Formulation: Our primary objective was to evaluate the efficacy of tools and methods in Wi-Fi penetration testing, focusing on WPA2/WPA3 cracking. This translated into specific questions concerning common vulnerabilities, prevalent attack vectors, and the effectiveness of various penetration testing tools and techniques as documented in the literature.

ii. Search Strategy Definition: To ensure a broad yet focused collection of relevant literature, a comprehensive search string was formulated. Keywords included "penetration testing," "network penetration testing," "vulnerabilities," "attack," "Wi-Fi security," "WPA2," "WPA3," "cracking," and specific tool names like "Aircrack-ng." These terms were combined using Boolean operators (AND, OR) to maximize relevance.

iii. Database Selection: Key academic databases were identified for the literature search. These included, but were not limited to, Google Scholar and the Saudi Digital Library (as exemplified by previous SLR efforts in our sources) [Alhamed & Rahman, 2023]. The potential inclusion of other relevant databases like Scopus was also considered to enhance coverage [Kambourakis et al., 2025].

iv. Inclusion and Exclusion Criteria: Strict criteria were established to filter the vast amount of literature.

- Inclusion Criteria: Papers focusing on Wi-Fi security, penetration testing, vulnerability assessment, and attack methodologies for WPA2 and WPA3 protocols; peer-reviewed journal articles and conference papers; publications predominantly in English. Our search was specifically focused on papers published between 2018 and 2023, reflecting the contemporary landscape of WPA3 development and analysis [Alhamed & Rahman, 2023; Halbouni et al., 2023].
- Exclusion Criteria: Duplicate records, papers with non-specific objectives or unrelated to the core topic, foreign language articles, and those that solely provided abstracts without full content were systematically removed [Alhamed & Rahman, 2023; Halbouni et al., 2023].

4.2. Conducting the Review Phase

This phase involved the execution of the search strategy and the systematic selection and data extraction from identified papers.

i. Identification: The formulated search string was applied across the selected databases. The initial search yielded a large number of records, which were then screened for duplicates [Alhamed & Rahman, 2023; Halbouni et al., 2023].

ii. Screening: Titles and abstracts of the remaining unique records were rigorously reviewed against the inclusion and exclusion criteria. This step aimed to eliminate irrelevant papers and identify potentially relevant ones for full-text review [Alhamed & Rahman, 2023; Halbouni et al., 2023].

iii. Eligibility (Full-Text Review): The full texts of the screened papers were obtained and meticulously assessed for eligibility. Papers that met all inclusion criteria were selected for detailed data extraction. References within these selected articles were also scanned for additional relevant papers, further expanding the pool of literature [Alhamed & Rahman, 2023; Halbouni et al., 2023].

iv. Data Extraction: For each included paper, relevant data points were extracted. This involved identifying:

- Specific vulnerabilities discussed (e.g., KRACK, downgrade attacks, side-channel attacks) [Alhamed & Rahman, 2023; Mathew et al., 2025].
- Attack methods and techniques described (e.g., handshake capture, brute force, evil twin, social engineering, beamforming forgery) [Chadee, 2024; Singh et al., 2023; Xu et al., 2024].
- Penetration testing tools utilized and their reported effectiveness (e.g., Aircrack-ng, Wireshark, Airgeddon, Nmap, Kali Linux) [Alhamed & Rahman, 2023; Asaad, 2017].
- Mitigation strategies proposed [Alhamed & Rahman, 2023; Wang et al., 2022].

4.3. Reporting Phase

The final phase focused on synthesizing the extracted data and presenting the findings. The gathered information was analyzed to identify recurring themes, emerging trends, and areas of consensus or contradiction across the literature. This systematic approach ensures that the "results" presented in the subsequent section are directly supported by the identified and analyzed scholarly works, providing a robust foundation for our conclusions and future recommendations.

5. Results

Our systematic literature review, meticulously conducted following the outlined methodology, yielded a comprehensive overview of Wi-Fi penetration testing, particularly concerning WPA2/WPA3 cracking. The synthesis of findings across

numerous studies reveals critical insights into existing vulnerabilities, effective attack methods, and the capabilities of various penetration testing tools.

5.1. Identified Vulnerabilities and Attack Success

The literature review consistently highlighted that despite the architectural improvements across Wi-Fi security protocols, no system is entirely impervious to attack, particularly when human factors or complex integrations are involved.

- WPA2's Persistent Weaknesses: The Key Reinstallation Attack (KRACK) remains a significant vulnerability in WPA2 [Alhamed & Rahman, 2023; Mathew et al., 2025]. This attack's efficacy lies in its ability to force nonce reuse during the 4-way handshake, enabling attackers to decrypt traffic and steal sensitive information like credit card numbers, passwords, and messages [Alhamed & Rahman, 2023]. Studies have actively performed and detected these attacks, confirming their real-world impact [Alhamed & Rahman, 2023].
- WPA3's Emerging Attack Vectors: While WPA3 was designed to mitigate WPA2's flaws, it has introduced its own set of challenges, often stemming from its complexity and need for backward compatibility.
    - Downgrade Attacks: Several sources confirm that WPA3 networks, particularly those operating in transition mode (WPA2-PSK/WPA3-SAE mixed mode), are susceptible to downgrade attacks. Attackers can exploit this to force devices to connect using the less secure WPA2 protocol, making them vulnerable to previously known WPA2 attacks [Chadee, 2024; Mathew et al., 2025].
    - Side-Channel Attacks: These attacks exploit information leaked through the physical implementation of cryptographic systems. For WPA3, they can infer details about the password conversion process, potentially aiding in cracking [Mathew et al., 2025; Halbouni et al., 2023].
    - Denial-of-Service (DoS) Attacks: Even WPA3-SAE can be vulnerable to DoS attacks, which can disrupt Wi-Fi service for legitimate users [Mathew et al., 2025; Shen et al., 2024]. If Protected Management Frames (PMF) are not effectively implemented or are disabled, WPA3 becomes susceptible to de-authentication and disassociation attacks, allowing attackers to disconnect users and force re-authentication [Chadee, 2024; Mathew et al., 2025].
    - Beamforming Feedback Forgery: A newly uncovered vulnerability, BeamCraft, demonstrates that attackers can manipulate Wi-Fi traffic by injecting forged beamforming feedback information (BFI). This physical layer attack exploits the clear-text nature of BFI, enabling covert traffic manipulation and potentially higher throughput for the attacker [Xu et al., 2024]. This type of attack is particularly concerning as it targets the fundamental operation of modern Wi-Fi systems [Xu et al., 2024].

5.2. Effectiveness of Penetration Testing Tools and Methods

Despite The review highlights the critical role of specific tools and methodologies in identifying and exploiting Wi-Fi vulnerabilities:

- Handshake Capture and Cracking (Aircrack-ng, Hashcat): Tools like Aircrack-ng are consistently shown to be effective for capturing the 4-way handshake in WPA/WPA2 networks and for executing dictionary and brute-force attacks [Alhamed & Rahman, 2023; Chen & Punya, 2021; Singh et al., 2023; Asaad, 2017]. Hashcat further augments this capability, proving particularly fast for offline password cracking by leveraging hardware acceleration [Asaad, 2017].
- Rogue APs and Social Engineering (Airgeddon, Captive Portals): The effectiveness of evil twin attacks combined with social engineering, primarily through captive portals, is widely documented. Attackers can successfully harvest login credentials by tricking users into entering their Wi-Fi passwords on fake authentication pages [Wang et al., 2022; Chadee, 2024]. The Airgeddon script automates the creation of such rogue APs and captive portals, significantly simplifying this attack vector [Chadee, 2024]. This method has been shown to successfully recover WPA3 passwords under specific conditions, such as when PMF is not implemented [Chadee, 2024].
- Traffic Analysis (Wireshark): Wireshark is indispensable for analyzing captured network traffic, helping testers understand communication patterns, identify potential data leakage, and determine protocol overheads [Alhamed & Rahman, 2023; Chen & Punya, 2021; Alyami et al., 2020]. It's crucial for diagnosing where network packets are lost or manipulated during attacks [Alhamed & Rahman, 2023].
- Reconnaissance and System Analysis (Nmap, Kali Linux): Nmap proves invaluable for network reconnaissance, enabling testers to identify live hosts, open ports, and running services, which are crucial for mapping out potential attack surfaces [Alhamed & Rahman, 2023; Singh et al., 2023]. The Kali Linux operating system, by integrating a vast array of such tools, provides a powerful and comprehensive environment for performing a wide range of penetration tests [Alhamed & Rahman, 2023; Asaad, 2017].
- Hardware for Simulation and Deployment (Raspberry Pi): Raspberry Pi devices are widely used for simulating Wi-Fi environments and deploying portable rogue access points due to their cost-effectiveness and versatility

[Chadee, 2024; Huang & Lin, 2018]. This allows for realistic, controlled experiments of Wi-Fi attacks [Chadee, 2024].

5.3. User Susceptibility and Configuration Weaknesses

A consistent finding across the literature is the significant role of human factors and insecure configurations in facilitating Wi-Fi attacks.

- Insecure Default Settings: Home routers and other Wi-Fi devices often ship with default settings that pose substantial security risks, including vulnerable Wi-Fi security protocols (like WPA/TKIP support by default), open Wi-Fi networks, and trivial administrative passwords [Ye et al., 2024]. Even guest networks are frequently poorly protected by default [Ye et al., 2024].
- Lack of Secure Guidelines: Many organizations, including top universities, fail to provide secure Wi-Fi configuration guidelines, leading users to adopt insecure settings [Wang et al., 2022]. A study showed that only 37% of top 200 universities provided secure instructions, contributing to user susceptibility to attacks like the evil twin [Wang et al., 2022].
- Inconspicuous Security Warnings: Operating systems often lack prominent warnings when insecure certificate validation settings are chosen or when suspicious certificates are encountered in WPA Enterprise networks [Wang et al., 2022]. This allows users to unwittingly connect to malicious networks or leak credentials [Wang et al., 2022]. Practical experiments confirm that even users with computing expertise can fall victim to such attacks, highlighting the persistence and effectiveness of these weaknesses in real-world scenarios [Wang et al., 2022].

These findings collectively underscore that while technological advancements in Wi-Fi security protocols are vital, their effectiveness is often undermined by implementation flaws, configuration oversights, and human behavior.

6. Discussion

The findings from our systematic literature review paint a compelling picture of the current state of Wi-Fi security, revealing that while significant strides have been made, particularly with WPA3, the battle against evolving threats remains ongoing.

6.1. Interpretation of Results

Our analysis confirms the initial hypothesis that despite the enhanced security features of WPA3, it is not an infallible shield against all Wi-Fi attacks. The transition period from WPA2 to WPA3, while necessary for backward compatibility, introduces critical vulnerabilities [Chadee, 2024; Mathew et al., 2025]. The susceptibility of WPA3 to downgrade attacks, for instance, allows attackers to exploit the weaknesses of its predecessor, undermining the very security it aims to provide [Mathew et al., 2025]. Furthermore, attacks targeting the physical layer, such as beamforming feedback forgery, represent a sophisticated evolution of threats that bypass traditional cryptographic defenses by manipulating fundamental Wi-Fi operations [Xu et al., 2024]. This highlights a critical, often overlooked, dimension of wireless security. The consistent success of social engineering attacks, particularly those involving rogue access points and captive portals, underscores that human vigilance and proper configuration remain paramount [Chadee, 2024; Wang et al., 2022]. Even with robust protocols, users can be lured into compromising their network credentials if the visual cues and warnings from their devices are insufficient or misunderstood [Wang et al., 2022]. This reinforces the notion that security is not solely a technological problem but also a socio-technical one, requiring continuous user education and improvements in user interface design for security features.

Moreover, the versatility and effectiveness of penetration testing tools such as Aircrack-ng, Wireshark, and Airgeddon, often operating within Kali Linux, are consistently demonstrated across the reviewed literature [Alhamed & Rahman, 2023; Asaad, 2017; Chadee, 2024]. These tools, whether used for passive sniffing, active de-authentication, or creating elaborate evil twin scenarios, remain indispensable for identifying vulnerabilities and demonstrating real-world attack feasibility. The continued necessity of manual penetration testing alongside automated scans further emphasizes the subtle, context-dependent vulnerabilities that only human expertise can uncover [Alhamed & Rahman, 2023].

6.2. Mitigation Strategies

The literature implicitly and explicitly suggests several mitigation strategies to enhance Wi-Fi security:

- Strong Authentication and Configuration: Encouraging the use of complex WPA2/WPA3 passphrases, disabling vulnerable protocols like WPS, and ensuring proper certificate validation in WPA Enterprise networks are fundamental [Chen & Punya, 2021; Wang et al., 2022].
- Standardized Security Measures: Operating system providers should eliminate insecure default configurations and consistently enforce secure mechanisms across user interfaces and programmatic APIs [Wang et al.,

2022]. Organizations should provide standardized Wi-Fi configuration applications (e.g., Eduroam CAT) to ensure secure settings [Wang et al., 2022].

- Enhanced User Awareness: Continuous education for users on identifying rogue access points, understanding security warnings, and the importance of secure Wi-Fi practices is critical [Wang et al., 2022].
- Intrusion Detection Systems (IDS): Implementing IDS, particularly those leveraging machine learning, can improve real-time detection of anomalies and attack precursors, thereby enhancing WPA3 security [Halbouni et al., 2023; Kambourakis et al., 2025]. This aligns with the broader trend of using AI to proactively identify threats and propose countermeasures [Mathew et al., 2025].

In essence, while WPA3 represents a significant leap forward in wireless security, its full potential can only be realized through comprehensive implementation, rigorous ongoing testing, and a concerted effort to address both technical vulnerabilities and human factors.

7. Conclusion

Our systematic literature review on Wi-Fi penetration testing, with a particular focus on WPA2/WPA3 cracking, underscores the dynamic and intricate nature of wireless network security. We set out to evaluate the tools and methods employed in testing Wi-Fi security, and our findings illuminate that while WPA3 has indeed introduced substantial enhancements, such as the Simultaneous Authentication of Equals (SAE) handshake and Protected Management Frames (PMF), it is not without its vulnerabilities [Mathew et al., 2025; Chadee, 2024; Halbouni et al., 2023]. The continued existence of downgrade attacks, side-channel exploits, and the newly identified physical-layer attacks like beamforming feedback forgery, highlights that the security landscape is in constant flux [Mathew et al., 2025; Xu et al., 2024]. Tools such as Aircrack-ng, Wireshark, Nmap, and specialized scripts like Airgeddon, often utilized within the Kali Linux environment, remain essential for ethical hackers to conduct comprehensive penetration tests [Alhamed & Rahman, 2023; Singh et al., 2023; Asaad, 2017; Chadee, 2024]. These tools facilitate critical attack vectors, including handshake capture, de-authentication attacks, and the deployment of malicious rogue access points combined with social engineering tactics, proving effective even against WPA3 under certain conditions, such as disabled PMF or through transition modes [Chadee, 2024]. The pervasive nature of insecure default settings in home routers and the alarming susceptibility of users to social engineering further compound these technical vulnerabilities [Ye et al., 2024; Wang et al., 2022].

The implications of our findings are clear: securing Wi-Fi networks requires a multi-faceted approach. Beyond implementing the latest protocols, organizations and individuals must prioritize continuous security assessments, cultivate heightened user awareness, and adopt robust configuration practices. The slow adoption of WPA3 and the computational demands it places on resource-constrained devices, particularly within the expanding IoT ecosystem, present ongoing challenges that necessitate innovative solutions. Looking to the future, the field of Wi-Fi penetration testing is ripe for further advancement. We strongly advocate for continued research into automated network penetration testing leveraging machine learning and deep reinforcement learning [Alhamed & Rahman, 2023]. Such advancements could provide new insights, improve efficiency, and enhance the detection of real-world attacks like KRACKs, while simultaneously reducing false positives that plague manual efforts [Alhamed & Rahman, 2023]. Further investigation into mitigating novel physical layer threats, such as beamforming manipulation, and exploring post-quantum cryptographic algorithms to prepare for future computational advancements are also critical areas of future work [Xu et al., 2024; Mathew et al., 2025]. By embracing these directions, the cybersecurity community can better anticipate and counter the evolving threats to our wireless infrastructure, ensuring a more secure and resilient digital future.

8. Acknowledgement

The authors extend their gratitude to all members of the School of Computing for their invaluable contributions to this study. This research was conducted under the Hacking and Penetration Testing Project and supported by Universiti Utara Malaysia (UUM).

9. References

M. Alhamed and M. M. H. Rahman, "A Systematic Literature Review on Penetration Testing in Networks: Future Research Directions," *Appl. Sci.*, vol. 13, no. 12, p. 6986, 2023, doi: 10.3390/app13126986.

C.-L. Chen and S. Punya, "An enhanced WPA2/PSK for preventing authentication cracking," *International Journal of Informatics and Communication Technology (IJ-ICT)*, vol. 10, no. 2, pp. 85–92, 2021, doi: 10.11591/ijict.v10i2.pp85-92.

K. Wang *et al.*, "Assessing Certificate Validation User Interfaces of WPA Supplicants," in *Proc. ACM Mobile Computing & Networking Conf. (Mobicom '22)*, Sydney, NSW, Australia, Oct. 2022, pp. 1–13, doi: 10.1145/3495243.3517026.

M. Xu *et al.*, "Beamforming made Malicious: Manipulating Wi-Fi Traffic via Beamforming Feedback Forgery," in *Proc. 30th Annu. Int. Conf. Mobile Computing and Networking (ACM MobiCom'24)*, Washington D.C., DC, USA, Nov. 2024, pp. 1–15, doi: 10.1145/3636534.3690669.

A. Mathew, E. Jackson, and A. Tobesman, "Evaluating the Efficacy of WPA3 against Advanced Attacks: A Comparative Analysis with WPA2 in Real-World," *J Inform Techn Int*, vol. 3, no. 1, p. 105, 2025, doi: 10.33790/jiti1100105.

J. Ye *et al.*, "Exposed by Default: A Security Analysis of Home Router Default Settings," in *Proc. ACM Asia Conf. Computer and Communications Security (ASIA CCS '24)*, Singapore, Singapore, Jul. 2024, pp. 1–17, doi: 10.1145/3634737.3637671.

H.-W. Cho and K. G. Shin, "FLEW: Fully Emulated WiFi," in *Proc. 28th Annu. Int. Conf. On Mobile Computing And Networking (ACM MobiCom '22)*, Sydney, NSW, Australia, Oct. 2022, pp. 1–13, doi: 10.1145/3495243.3517030.

A. Bin Rabiah *et al.*, "Haiku: Efficient Authenticated Key Agreement with Strong Security Guarantees for IoT," in *Proc. Int. Conf. Distributed Computing and Networking 2021 (ICDCN '21)*, Nara, Japan, Jan. 2021, pp. 1–10, doi: 10.1145/3427796.3427817.

G. Kambourakis, "Intrusion Detection Based on Federated Learning: A Systematic Review," *ACM Comput. Surv.*, 2025. doi: 10.1145/3731596.

D. Schepers, A. Ranganathan, and M. Vanhoef, "Let Numbers Tell the Tale: Measuring Security Trends in Wi-Fi Networks and Best Practices," in *Proc. Conf. Security and Privacy in Wireless and Mobile Networks (WiSec '21)*, Abu Dhabi, United Arab Emirates, Jun. 2021, pp. 1–6, doi: 10.1145/3448300.3468286.

H. Jin and P. Papadimitratos, "Over-the-Air Runtime Wi-Fi MAC Address Re-randomization," in *Proc. 17th ACM Conf. Security and Privacy in Wireless and Mobile Networks (WiSec '24)*, Seoul, Republic of Korea, May 2024, pp. 1–6, doi: 10.1145/3643833.3656122.

S. Singh, G. Srivastava, S. Kumar, and S. Singh, "Penetration Testing And Security Measures To Identify Vulnerability Inside The System," *IOSR Journal of Computer Engineering (IOSR-JCE)*, vol. 25, no. 3, pp. 50–64, 2023, doi: 10.9790/0661-2503015064.

R. R. Asaad, "Penetration Testing: Wireless Network Attacks Methods on Kali Linux OS," *ICONTECH INTERNATIONAL JOURNAL*, vol. 4, no. 2, pp. 28–34, 2017, doi: 10.25007/ajnu.v10n1a998.

K. Khan, "Recovering WPA-3 Network Password by Bypassing the Simultaneous Authentication of Equals Handshake using Social Engineering Captive Portal," arXiv. doi: 10.48550/arXiv.2412.15381

Y. Hu *et al.*, "Security Threats from Bitcoin Wallet Smartphone Applications: Vulnerabilities, Attacks, and Countermeasures," in *Proc. Eleventh ACM Conf. Data and Application Security and Privacy (CODASPY '21)*, Virtual Event, USA, Apr. 2021, pp. 1–12, doi: 10.1145/3422337.3447832.

Z. Shen, I. Karim, and E. Bertino, "Segment-Based Formal Verification of WiFi Fragmentation and Power Save Mode," in *Proc. ACM Asia Conf. Computer and Communications Security (ASIA CCS '24)*, Singapore, Singapore, Jul. 2024, pp. 1–16, doi: 10.1145/3634737.3637667.

X. Zhou *et al.*, "Untangling the Knot: Breaking Access Control in Home Wireless Mesh Networks," in *Proc. 2024 ACM SIGSAC Conf. Computer and Communications Security (CCS '24)*, Salt Lake City, UT, USA, Oct. 2024, pp. 1–15, doi: 10.1145/3658644.3670380.

H. Huang and S. Lin, "WiDet: Wi-Fi Based Device-Free Passive Person Detection with Deep Convolutional Neural Networks," in *Proc. 21st ACM Int. Conf. Modelling, Analysis and Simulation of Wireless and Mobile Systems (MSWIM '18)*, Montreal, QC, Canada, Oct. 2018, pp. 1–8, doi: 10.1145/3242102.3242119.

A. Halbouni, L.-Y. Ong, and M.-C. Leow, "Wireless Security Protocols WPA3: A Systematic Literature Review," *IEEE Access*, 2023, doi: 10.1109/ACCESS.2023.3322931.

M. Vanhoef and F. Piessens, "Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2," in *Proc. 2017 ACM SIGSAC Conf. Computer and Communications Security*, Dallas, TX, USA, Oct. 2017, pp. 1313–1328, doi: 10.1145/3133956.3134027.