International Journal of Circuit, Computing and Networking

E-ISSN: 2707-5931
P-ISSN: 2707-5923
Impact Factor (RJIF): 5.64
Journal's Website
IJCCN 2026; 7(2): 33-36
Received: 13-01-2026
Accepted: 15-02-2026

Flávio Cezar Amate
Associate Professor, Department of Informatics, Federal Institute of Education, Science and Technology of São Paulo, Bragança Paulista, São Paulo, Brazil

Cauã Barcellos Moreto
Student, Department of Informatics, Federal Institute of Education, Science and Technology of São Paulo, Bragança Paulista, São Paulo, Brazil

Michele Maria de Oliveira
Student, Department of Informatics, Federal Institute of Education, Science and Technology of São Paulo, Bragança Paulista, São Paulo, Brazil

Corresponding Author:
Flávio Cezar Amate
Associate Professor, Department of Informatics, Federal Institute of Education, Science and Technology of São Paulo, Bragança Paulista, São Paulo, Brazil

Experimental analysis of security vulnerabilities in IEEE 802.11 wireless networks and mitigation strategies

Flávio Cezar Amate, Cauã Barcellos Moreto, Michele Maria de Oliveira

DOI: https://doi.org/10.33545/27075923.2026.v7.i2a.142

Abstract
This paper presents an experimental evaluation of security vulnerabilities in IEEE 802.11 wireless networks, focusing on authentication and encryption mechanisms in WEP, WPA, and WPA2 protocols. The study was conducted in a controlled laboratory environment using widely adopted penetration testing tools, including Aircrack-ng, Wireshark, Kismet, Wifite, and Reaver. The results demonstrate the complete insecurity of WEP, with encryption keys recovered in less than four minutes (mean time 3 min 44 s), and reveal critical vulnerabilities in WPA2 networks when WPS is enabled, allowing password recovery with a mean execution time of 5 h 12 min. Furthermore, the findings show that WPA2 security is highly dependent on password strength, with weak credentials being easily compromised through dictionary attacks. Based on the experimental analysis, this work proposes practical mitigation strategies aimed at improving wireless network security through proper configuration, protocol selection, and user awareness.

Keywords: Wi-Fi security, IEEE 802.11, WPA2, penetration testing, network vulnerabilities, wireless security

1. Introduction
IEEE 802.11 wireless networks play a fundamental role in modern communication systems, enabling a wide range of applications, from enterprise services to Internet of Things (IoT) environments. Despite their widespread adoption, their broadcast nature exposes them to various security threats.
The evolution of Wi-Fi security protocols (from WEP to WPA, WPA2, and WPA3) aims to mitigate vulnerabilities; however, legacy protocols remain in use, and even modern protocols present exploitable weaknesses under certain conditions [1, 2].
This work performs an experimental evaluation of vulnerabilities in wireless networks, focusing on real attack scenarios. Unlike purely theoretical analyses, this study applies penetration testing techniques to validate the effectiveness of attacks and assess practical security risks. The main contribution of this research is twofold. First, it presents an experimental validation of vulnerabilities in IEEE 802.11 protocols by reproducing realistic attack scenarios in a controlled environment. Second, it proposes practical mitigation strategies derived from the observed attack behavior, providing actionable insights for improving the security of wireless networks.

2. Related work
Wireless network security has been extensively studied due to the inherent vulnerabilities of IEEE 802.11 communications, which rely on an open transmission medium. Over the years, several security protocols have been developed, including WEP, WPA, WPA2, and WPA3, aiming to ensure confidentiality, integrity, and authentication.
Early studies demonstrated that WEP suffers from critical design flaws, particularly related to the RC4 encryption algorithm and weak key management mechanisms. These vulnerabilities allow attackers to recover encryption keys within minutes using statistical and brute-force techniques [1]. As a result, WEP has been widely considered obsolete and unsuitable for modern deployments.
Subsequent protocols such as WPA and WPA2 introduced significant improvements, including the use of TKIP and AES encryption. However, research has shown that these protocols are still vulnerable under certain conditions. In particular, WPA2 networks remain

susceptible to dictionary attacks when weak passwords are used, highlighting that security is strongly dependent on credential complexity rather than protocol robustness alone [2]. Additionally, comparative studies indicate that alternative authentication approaches, such as RADIUS-based systems, can provide improved security when compared to WPA2-PSK configurations [6].

Another major class of vulnerabilities involves management frame exploitation, especially deauthentication attacks. These attacks can disrupt communication between devices and access points, enabling attackers to capture authentication handshakes and perform offline password cracking. Experimental studies in IoT environments confirm that deauthentication attacks remain effective and can significantly impact network availability and performance [3]. These findings reinforce the persistence of this attack vector even in modern wireless environments.

Penetration testing has been widely adopted as a practical approach to evaluate wireless network security. Several works have demonstrated the effectiveness of tools such as Aircrack-ng, Wifite, and Reaver in identifying vulnerabilities and exploiting weaknesses in real-world scenarios [4, 7]. These tools enable automated execution of attacks such as handshake capture, brute-force attempts, and WPS exploitation, providing valuable insights into network security posture.

Experimental studies based on Kali Linux penetration testing environments have also demonstrated the practical exploitation of vulnerabilities in IEEE 802.11 security protocols. Previous research showed that attacks such as ARP replay, fake authentication, and dictionary-based password cracking can successfully compromise WEP, WPA, and WPA2 networks under specific conditions, reinforcing the importance of secure configuration practices and robust credential management [8].

In addition to traditional wireless attacks, recent studies have explored packet injection and manipulated traffic attacks in software-defined networking environments. These studies demonstrated that maliciously crafted packets can disrupt network services, consume network resources, and affect communication stability, highlighting the broader relevance of packet manipulation techniques in modern network security research [9].

More recent studies have focused on the latest Wi-Fi security protocol, WPA3. Although WPA3 introduces stronger authentication mechanisms and improved protection against brute-force attacks, research indicates that it is not entirely immune to threats. Attacks such as Evil Twin, deauthentication, and social engineering remain effective, particularly in transitional mode configurations [5]. Furthermore, experimental analyses demonstrate that even modern security enhancements can be bypassed under specific conditions, especially when user behavior or misconfiguration is exploited [5].

Despite the extensive body of research, many studies either focus on theoretical analysis or isolated attack scenarios. There is still a need for comprehensive experimental evaluations that integrate multiple attack techniques in controlled environments and provide actionable mitigation strategies.

In this context, the present work contributes by conducting an experimental analysis of multiple attack vectors on IEEE 802.11 networks and proposing practical security recommendations based on observed results.

3. Materials and Methods

This research adopted an experimental methodology conducted in a controlled laboratory environment.

3.1 Experimental setup

The attack environment was configured using a penetration testing infrastructure based on Kali Linux, which is widely adopted in wireless security assessments [2, 7]. The experimental setup included USB Wi-Fi adapters with monitor mode support (chip Atheros compatible with packet injection) and two wireless routers configured with different security protocols, enabling the evaluation of multiple attack scenarios. Scenario 1 employed WEP, Scenario 2 used WPA2-PSK with WPS enabled, and Scenario 3 used WPA2-PSK with WPS disabled.

Prior to the experiments, the infrastructure was validated to ensure proper support for packet injection and traffic monitoring capabilities, which are essential for executing wireless penetration testing techniques.

The experimental setup is illustrated in Fig. 1, which presents the main components of the test environment, including the attacker system, wireless access point, and client device.

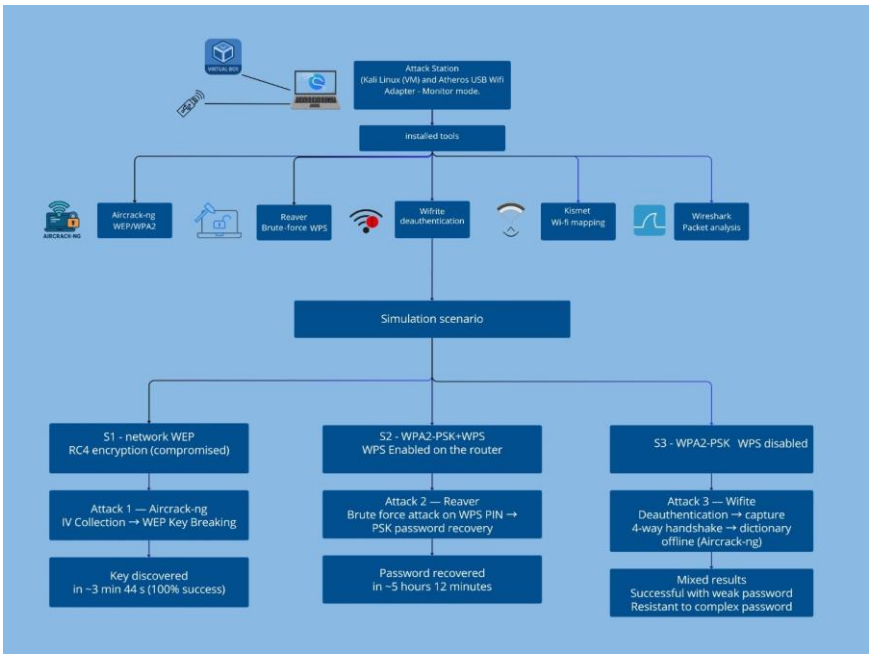


Fig 1: Experimental workflow and attack scenarios used in the wireless network penetration testing environment

3.2 Penetration testing tools and environment

The experiments were conducted using a set of widely adopted wireless penetration testing and network analysis tools. Wireshark was used for packet capture and traffic analysis, enabling detailed inspection of network communications. Kismet was employed for wireless network discovery and monitoring, allowing the identification of access points and connected devices.

For attack execution, Aircrack-ng was used to perform password cracking and key recovery processes, while Wifite provided an automated framework for executing multiple wireless attacks. Additionally, Reaver was utilized to conduct brute-force attacks against WPS-enabled networks, enabling the assessment of vulnerabilities related to WPS configurations.

3.3 Attack scenarios

The experimental evaluation considered multiple attack scenarios targeting different security mechanisms of IEEE 802.11 networks. Initially, WEP cracking was performed to assess the vulnerability of legacy encryption protocols. Subsequently, a brute-force attack against WPS-enabled networks was conducted to evaluate weaknesses related to WPS configurations.

To analyze WPA and WPA2 security, handshake capture techniques were applied, followed by dictionary-based attacks to test password robustness under different conditions. In addition, deauthentication attacks were executed to disrupt communication between clients and access points, enabling the capture of authentication handshakes and facilitating further offline attacks.

To ensure consistency and reproducibility, scripts were developed to automate attack execution processes, including handshake capture and password cracking workflows.

4. Results and Discussion

The experimental results, summarized in Table 1, reveal significant differences in the security levels of IEEE 802.11 protocols under various attack scenarios.

The results confirm that WEP is fundamentally insecure, as its encryption key was successfully recovered in less than four minutes, with a mean execution time of 3 min 44 s. This finding is consistent with previous studies [1], which demonstrate that WEP vulnerabilities can be exploited through statistical attacks, rendering the protocol obsolete.

In the case of WPA2 networks with WPS enabled, the experiments showed that the network password could be recovered in approximately five hours using brute-force techniques, with a mean execution time of 5 h 12 min. This highlights a critical vulnerability associated with WPS, which significantly weakens the overall security of WPA2 networks.

Table 1: Summary of experimental results for IEEE 802.11 attack scenarios

Protocol	Attack type	Result	Mean time	Security implication
WEP	Key Cracking	Successful	3 min 44 s	Completely insecure
WPA2 (WPS enabled)	Brute-force (WPS)	Successful	5 h 12 min	Critical vulnerability
WPA2	Dictionary Attack	Conditional	Variable	Depends on password strength
WPA/WPA2	Deauthentication	Successful	Immediate	Enables further attacks

For WPA2 networks without WPS, the results indicate that security is strongly dependent on password complexity. Networks configured with weak passwords were successfully compromised through dictionary attacks, whereas strong passwords provided effective resistance. For example, complex credentials such as "R#d&s$@gUr@2026!" demonstrated significantly greater resistance to password cracking attempts, indicating that the security of WPA2-PSK relies heavily on the robustness of the configured password. This observation aligns with findings reported in [2], reinforcing the importance of robust credential management.

Additionally, deauthentication attacks proved to be highly effective, allowing attackers to disrupt communication between clients and access points and enabling the capture of authentication handshakes. These results are consistent with previous studies [3], which highlight the persistence of deauthentication-based attacks even in modern wireless environments.

Overall, the findings demonstrate that wireless network security is not solely determined by the protocol used, but also by configuration practices and the presence of auxiliary features such as WPS.

4. Mitigation strategies

Based on the experimental findings, several mitigation strategies are recommended to enhance the security of IEEE 802.11 wireless networks. First, legacy mechanisms such as WEP and WPS should be permanently disabled due to their critical vulnerabilities, as demonstrated by the rapid key recovery and brute-force attacks observed in this study.

The adoption of WPA3 is strongly recommended whenever supported, as it provides improved protection against brute-force and dictionary-based attacks compared to previous protocols. In addition, password policies should enforce strong credentials, preferably with a minimum length of 12 characters and sufficient complexity, in order to mitigate dictionary attacks.

To address vulnerabilities related to management frame exploitation, the implementation of Protected Management Frames (PMF) is recommended, as it can reduce the effectiveness of deauthentication attacks. Furthermore, continuous network monitoring should be employed to detect anomalous behaviors, such as repeated deauthentication attempts or unauthorized access.

Finally, user awareness and training are essential components of wireless network security, as social engineering techniques and poor configuration practices can significantly weaken even robust security mechanisms.

5. Conclusion

This study presented an experimental evaluation of security vulnerabilities in IEEE 802.11 wireless networks, demonstrating that network security is strongly influenced by configuration practices rather than protocol design alone.

The results confirmed the complete obsolescence of WEP and highlighted that WPA2 networks, although more robust, remain vulnerable under specific conditions, particularly when WPS is enabled or weak passwords are used. Additionally, deauthentication attacks were shown to be

effective in enabling further exploitation, reinforcing their relevance in modern wireless threat scenarios.

The main contribution of this work lies in the practical validation of multiple attack vectors within a controlled environment, providing empirical evidence of real-world vulnerabilities and their exploitation mechanisms. Furthermore, the proposed mitigation strategies offer actionable recommendations to improve wireless network security through the adoption of stronger protocols, secure configurations, and continuous monitoring.

Overall, the findings emphasize that effective wireless security depends not only on protocol evolution but also on proper implementation and user awareness.

6. Acknowledgments

The authors acknowledge the support of the Federal Institute of Education, Science and Technology of São Paulo (IFSP) in the development of this research.

References

1. Adbeib KA. Comprehensive study on Wi-Fi security protocols by analyzing WEP, WPA, and WPA2. African Journal of Advanced Pure and Applied Sciences. 2023;2(4):385-402.
2. Joshi D, Dwivedi VV, Pattani KM. Penetration testing on wireless network 802.11i. International Journal of Advance Research in Engineering, Science & Technology. 2017;4(4):21-27.
3. Kristiyanto Y, Ernastuti E. Analysis of deauthentication attack on IEEE 802.11 connectivity based on IoT technology using external penetration test. CommIT (Communication and Information Technology) Journal. 2020;14(1):45-51.
4. Koutras D, Dimitrellos P, Kotzanikolaou P, Douligeris C. Automated WiFi incident detection attack tool on 802.11 networks. In: Proceedings of the IEEE Symposium on Computers and Communications (ISCC); 2023. p. 464-469.
5. Ghanim AA, Thanoun MY. Evaluating the effectiveness of WPA3 protocol against advanced hacking attacks. International Journal of Wireless and Microwave Technologies. 2025;15(4):1-18.
6. Wahyudi E, Luthfi ET, Efendi MM. Wireless penetration testing method to analyze WPA2-PSK system security and captive portal. Jurnal Explore STMIK Mataram. 2019;9(1):1-7.
7. Singh H, Singh J. Penetration testing in wireless networks. International Journal of Advanced Research in Computer Science. 2017;8(5):2213-2216.
8. Kissi MK, Asante M. Penetration testing of IEEE 802.11 encryption protocols using Kali Linux hacking tools. International Journal of Computer Applications. 2020;176(32):26-33.
9. Deng S, Gao X, Lu Z, Gao X. Packet injection attack and its defense in software-defined networks. IEEE Transactions on Information Forensics and Security. 2018;13(3):695-707.