World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(RESEARCH ARTICLE)

Check for updates

Securing Campus Wi-Fi Against MITM Attacks: Penetration testing, student awareness and a multilayer defense model

Faisal Syafar [1,*], Halimah Husain [2] and Ganggang Canggi Arnanto [1]

[1] *Department of Electronics and Information Technology, Faculty of Engineering, Universitas Negeri Makassar, Makassar, Indonesia.*
[2] *Department of Chemistry, Faculty of Mathematical and sciences, Universitas Negeri Makassar, Makassar, Indonesia.*

World Journal of Advanced Engineering Technology and Sciences, 2025, 17(02), 488-495

Publication history: Received 15 October 2025; revised on 25 November 2025; accepted on 28 November 2025

Article DOI: https://doi.org/10.30574/wjaets.2025.17.2.1527

Abstract

Campus Wi-Fi networks remain vulnerable to man-in-the-middle (MITM) attacks due to outdated protocols, weak configurations, and low user awareness. This study evaluated the Wi-Fi security posture at the Faculty of Engineering, Universitas Negeri Makassar (UNM) using penetration testing, controlled MITM simulations, and a cybersecurity awareness survey (N = 120). Results showed that 70% of access points (APs) used insecure or misconfigured settings, enabling high MITM success in ARP spoofing, DNS spoofing, and SSL stripping. Student awareness was low, with only 28% understanding MITM and 18% routinely using VPNs. A multilayer security architecture integrating WPA3, VPN tunneling, VLAN segmentation, and Snort-based IDS reduced MITM success by 78% and achieved 92% detection accuracy. These findings highlight the importance of integrated defenses and continuous user education.

Keywords: Man-in-the-middle; Securing Campus wi-fi; Penetration testing; Multilayer defense

1. Introduction

Wi-Fi has become the backbone of digital transformation in higher education, serving as the primary communication medium for learning management systems, cloud services, digital libraries, campus administrative systems, and research collaboration platforms. As universities adopt hybrid and fully online instructional models, the dependency on uninterrupted, secure Wi-Fi access has grown exponentially. However, this increased reliance also magnifies the attack surface, especially in environments where network configurations evolve incrementally, legacy devices remain active, and cybersecurity literacy among users varies widely.

One of the most persistent threats to wireless environments is the man-in-the-middle (MITM) attack, a technique in which an adversary intercepts, manipulates, or relays communication between a victim and the intended destination. Prior works show that attackers can exploit weaknesses at multiple layers—including the Wi-Fi link layer, ARP/DNS resolution layer, and application layer—making MITM a multifaceted threat capable of bypassing even relatively modern security configurations [1–3]. For instance, the discovery of FragAttacks demonstrated that even well-configured WPA3 networks could be vulnerable to frame injection and aggregation flaws when exploited by an adversary with proximity to the target [3].

The introduction of WPA3 was expected to significantly strengthen Wi-Fi security through its Simultaneous Authentication of Equals (SAE) handshake, resistance to offline dictionary attacks, and mandatory Protected Management Frames (PMF). Yet, empirical studies have revealed that WPA3 deployment in real-world campus environments is far from uniform. Many institutions continue to operate mixed WPA2/WPA3 modes, which introduce downgrade vectors allowing attackers to force clients into weaker handshakes or exploit transitional vulnerabilities [4–

* Corresponding author: Faisal Syafar

9]. Additionally, PSK-based networks (WPA2-PSK or WPA3-PSK) remain susceptible when weak passphrases or outdated encryption schemes are employed.

Beyond protocol weaknesses, user behavior remains a critical vulnerability factor. Several studies emphasize that students often lack foundational cybersecurity awareness, rarely verify the authenticity of Wi-Fi networks, overlook certificate warnings, reuse passwords, and seldom employ privacy-enhancing tools such as VPNs [13–16]. Behavioral tendencies—such as connecting to any SSID resembling the official campus network—create significant opportunities for rogue AP placement and credential phishing, further amplifying MITM feasibility.

University campus environments are particularly challenging due to the coexistence of multiple Wi-Fi networks: staff networks, student networks, laboratory networks, guest networks, and device-specific networks. Many of these operate on separate APs with diverse configurations accumulated over years. Heterogeneous infrastructure can inadvertently create inconsistent security postures, even within a single faculty or building.

Given these challenges, cybersecurity frameworks increasingly advocate defense-in-depth, integrating multiple layers of protection such as WPA3, VPN tunneling, intrusion detection, micro-segmentation, and continuous monitoring [11,12,17–20]. However, empirical studies evaluating such multilayer implementations in developing countries—especially within real university environments—remain limited.

This research fills that gap by providing a detailed evaluation of the Faculty of Engineering, UNM, through three approaches:

- **Penetration testing** of representative APs to measure technical vulnerabilities.
- **Controlled MITM experiments** to quantify practical attack feasibility.
- **A cybersecurity awareness survey** to assess behavioral vulnerability factors.

A multilayer security architecture integrating WPA3 enforcement, VPN tunneling, VLAN segmentation, and Snort-based IDS/IPS was then developed and evaluated experimentally.

2. Methods

2.1. Study Setting and Wi-Fi Infrastructure Profile

The Faculty of Engineering at UNM operates multiple Wi-Fi networks serving over five thousand daily users. The infrastructure includes enterprise-grade access points installed in laboratories and lecture buildings, as well as lower-tier devices in public areas and administrative rooms. Prior to this study, the network had undergone partial upgrades toward WPA3 compliance, but many legacy devices remained operational.

To ensure a representative assessment, ten APs were selected based on:

- **User density** (e.g., lecture halls with >200 students)
- **Security sensitivity** (e.g., labs handling research data)
- **Coverage area** (public vs. restricted zones)
- **Model diversity** (different vendors and generations)

This approach aligns with sampling strategies used in prior Wi-Fi security assessments [4–9].

2.2. Penetration Testing Procedures

Penetration testing was performed systematically during off-peak hours to avoid service disruption. The evaluation covered:

- **Protocol identification:** Detecting whether APs operated in WPA2-PSK, WPA3-Personal, WPA2/WPA3 transition, or legacy modes (WEP/Open).
- **Configuration auditing:** Checking PMF status, client isolation, beacon information, and passive scanning of management frames.

- **Credential robustness:** Capturing WPA2/WPA3 handshakes and performing offline dictionary attacks where permitted.
- **Downgrade attack feasibility:** Attempting to force clients away from WPA3-SAE into weaker handshakes.
- **Rogue AP susceptibility:** Establishing look-alike SSIDs to test whether clients automatically reconnect.

Tools included **Airodump-ng**, **Aircrack-ng**, **Bettercap**, and custom scripts for PMF validation. All penetration testing followed responsible disclosure guidelines and institutional approval.

2.3. MITM Attack Simulations

Five APs were selected for controlled experiments to reflect varying security levels. Three MITM techniques were executed:

2.3.1. ARP Spoofing

ARP poisoning tools redirected traffic flows between clients and gateways, consistent with methods proposed in ARP spoofing literature [21–23].

2.3.2. DNS Spoofing

Attacks manipulated DNS responses to redirect users to attacker-controlled pages.

2.3.3. SSL Stripping / HTTPS Downgrade

- Tools attempted to downgrade HTTPS connections to HTTP to collect plaintext credentials where possible.
- Each attack type was repeated 20 times per AP to ensure reliability.

Success Metrics

A run was considered successful when:

- Traffic interception occurred,
- Credential leakage was observed, or
- Victim device displayed no security warning.

2.4. Cybersecurity Awareness Survey

A structured online questionnaire adapted from prior studies [13–16] captured:

- Knowledge of MITM and basic concepts
- Routine cybersecurity practices
- Wi-Fi behavior (SSID verification, use of public networks)
- VPN usage frequency
- Exposure to formal training

Responses from 120 students were collected, anonymized, and scored into awareness categories.

2.5. Multilayer Security Architecture Design

The proposed architecture integrated:

2.5.1. WPA3 Enforcement

- Activating SAE
- Enabling PMF
- Disabling transitional mixed modes
- Enforcing minimum PSK complexity

2.5.2. VPN Tunneling for Sensitive Systems

Traffic to the learning management system, administrative portals, and research servers passed through an institutional VPN gateway.

2.5.3. VLAN Segmentation

Distinct VLANs separated student, staff, IoT, and administrative devices, following segmentation guidelines [17–20].

2.5.4. Snort-based IDS/IPS

Snort 3 was deployed inline with:

- Community rules
- MITM-related signatures
- Custom rules for ARP anomalies and DNS irregularities

2.6. Evaluation Metrics

The architecture was evaluated using:

- MITM success rate before vs. after deployment
- Detection rates (true/false positives)
- Latency and throughput impact
- Cross-VLAN containment

3. Results

3.1. Baseline Security Audit

3.1.1. Wi-Fi Security Posture

Table 1 Baseline Security Configuration of Representative APs

Access Point	Encryption	Client Isolation	MITM Risk	Notes
FTLab2	WPA3	Enabled	Low	Secure configuration
FTAdmin	WPA2-PSK	Disabled	High	Weak PSK
FTLab1	WPA2-PSK	Disabled	High	No IDS monitoring
FTKantin	WPA2-PSK	None	High	Public, high exposure
FTOpenSpace	WEP	None	Very High	Legacy protocol still active

70% of APs had significant weaknesses, including weak passphrases, disabled PMF, or legacy security.

The audit revealed inconsistent security configurations:

- **WPA3 fully enabled:** 2 APs
- **WPA2-PSK only:** 3 APs
- **WPA2/WPA3 transition:** 4 APs
- **WEP/Open:** 1 AP

Additional findings included:

- PMF disabled on 70% of APs
- Client isolation inactive on 60%
- Two PSKs cracked in under **5 minutes** using dictionary tools

- WPS still active on one AP

These configurations significantly increased exposure to rogue AP and spoofing attacks.

3.2. MITM Attack Effectiveness

Table 2 MITM Attack Success Rates

MITM Technique	Success Rate	Description
ARP Spoofing	60–75%	No ARP validation mechanisms
DNS Spoofing	70–85%	Weak DNS integrity
SSL Stripping	20–30%	Limited by HSTS/HTTPS adoption

Overall baseline MITM success: **80%**.

Across 300 total attack attempts:

- **ARP spoofing:** consistently high success due to absence of ARP inspection
- **DNS spoofing:** highly effective on APs without encrypted DNS
- **SSL stripping:** moderately effective where HSTS was not enforced

Notably, user devices frequently ignored certificate warnings, contributing to higher-than-expected success rates.

3.3. Student Awareness Survey Results

Table 3 Summary of Student Awareness (N = 120)

Indicator	%	Interpretation
Understand MITM attacks	28%	Low conceptual literacy
Regular VPN use	18%	High plaintext exposure
Connect to SSIDs without checks	72%	Poor verification habits
Received security training	33%	Significant educational gap

Detailed analysis of the 120 respondents showed:

- **45%** believed WPA2 alone is “secure enough”
- **52%** had never heard of PMF or SAE
- **31%** reused the same password for personal and campus systems
- **72%** connected automatically to look-alike SSIDs
- **Only 12%** checked certificate details when accessing portals

These behaviors directly increased susceptibility to rogue AP and MITM scenarios.

3.4. Post-Implementation Security Improvements

Table 4 Pre–Post Security Comparison

Metric	Baseline	After Deployment	Improvement
MITM success rate	80%	18%	↓ 78%
Snort detection accuracy	–	92%	High
False positives	–	7%	Moderate
Cross-VLAN movement	Allowed	Blocked	Eliminated
Performance overhead (RTT)	–	+6–9 ms	Minimal

After deploying the multilayer architecture:

- MITM success dropped from **80% → 18%**
- WPA3-SAE prevented offline dictionary attacks
- Snort detected 92% of spoofing attempts
- VLAN segmentation blocked lateral movement even when local spoofing succeeded
- Latency overhead remained minimal (+6–9 ms)

This validated the effectiveness of multilayer controls in realistic campus settings.

4. Discussion

Findings confirm that technical weaknesses—such as WPA2-PSK, disabled PMF, and weak passphrases—create favorable conditions for MITM exploitation, consistent with prior analyses of Wi-Fi vulnerabilities [1–5,7–9]. The dominance of ARP and DNS spoofing aligns with other studies demonstrating that these local-layer protocols remain insufficiently protected in campus environments [21–24].

WPA3 significantly reduced attack feasibility, but its effectiveness depended on correct deployment and the removal of transitional WPA2/WPA3 modes, as noted in related research [6–9]. VLAN segmentation proved highly effective at mitigating lateral movement, supporting recommendations in network architecture literature [17–20]. Snort's 92% detection accuracy aligns with results reported in wireless IDS studies [25–27].

Human factors emerged as equally critical: low understanding of MITM and poor VPN adoption replicate patterns documented in international higher-education studies [13–16].

4.1. MITM Feasibility in Modern Campus Environments

Despite the presence of WPA3 in parts of the network, most vulnerabilities stemmed from:

- Transitional WPA2/WPA3 configurations
- Weak PSKs
- Disabled PMF
- Legacy devices requiring backward compatibility

This mirrors global findings that practical Wi-Fi insecurity often arises from configuration issues rather than protocol limitations [1–9].

4.2. Effectiveness of WPA3 When Properly Configured

WPA3-SAE significantly reduced handshake capture possibilities, though its protection weakened substantially when transitional modes were active. This confirms prior research that transitional modes create downgrade vectors exploitable by attackers [6–9].

4.3. Importance of Segmentation and IDS

VLAN segmentation proved crucial for preventing lateral movement, echoing network security research emphasizing micro-segmentation as an essential defense strategy [17–20]. Snort further improved detection visibility, validating the usefulness of signature-based IDS in campus environments [25–27].

4.4. Human Factors: The Weakest Link

Low awareness and inadequate practices magnified technical vulnerabilities. Students rarely used VPNs, seldom verified SSIDs, and ignored certificate warnings—behaviors aligned with prior studies in higher education [13–16]. This underscores the need for mandatory cybersecurity training programs.

4.5. Implications for University IT Governance

Universities in developing regions must consider:

- Accelerating WPA3 migration
- Eliminating transitional modes
- Enforcing VPN use for sensitive systems
- Deploying segmentation from design
- Institutionalizing cybersecurity awareness programs

5. Conclusion

The study demonstrates that campus Wi-Fi networks remain exposed to MITM threats when outdated configurations and low user awareness intersect. A multilayer security architecture—consisting of WPA3, VPN, segmentation, and IDS—reduced MITM success by 78% while maintaining acceptable performance. Universities should incorporate integrated defenses and structured cybersecurity education to strengthen overall resilience.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Thankappan M, Rifà-Pous H, Garrigues C. Multi-channel man-in-the-middle attacks against protected Wi-Fi networks: A state-of-the-art review. Expert Syst Appl. 2022.

[2] Amoordon A, et al. Characterizing Wi-Fi Man-in-the-Middle Attacks. In: URSI GASS 2020; Rome, Italy. 2020.

[3] Vanhoef M. FragAttacks: Forging frames in protected Wi-Fi networks. USENIX Security / Black Hat USA white paper. 2021.

[4] Halbouni A, Ong L-Y, Leow M-C. Wireless security protocols WPA3: A systematic literature review. IEEE Access. 2023.

[5] Reddy BI, Srikanth V. Review on wireless security protocols (WEP, WPA, WPA2 & WPA3). Int J Sci Res Comput Sci Eng Inf Technol. 2019;5(4):28-35.

[6] Wi-Fi Alliance. WPA3 Security Considerations [Internet]. Austin (TX): Wi-Fi Alliance; 2019 [cited 2025 Nov 26]. Available from: https://wpa3.mathyvanhoef.com/WPA3_Security_Considerations_20190410.pdf

[7] Guaki GS. WPA3: An analysis of its flaws and limitations – A literature review. 2023.

[8] Ghanim AA, Thanoun MY. Evaluating the effectiveness of WPA3 protocol against advanced hacking attacks. Int J Wireless Microwave Technol. 2025;15(4):1-18.

[9] Cisco Systems. WPA3 Deployment Guide – Cisco Catalyst 9800 Wireless Controller [Internet]. 2024 [cited 2025 Nov 26]. Available from: https://www.cisco.com/

[10] Security and privacy of public Wi-Fi. Int J Res Publ Rev. 2022;3(11):1-8.

[11] Spectra. From access points to end points: Complete campus Wi-Fi security [Internet]. 2024 [cited 2025 Nov 26]. Available from: https://www.spectra.co/

[12] Immunity Networks. Best practices for planning, assessing, maintaining, and running a campus-wide WiFi network [Internet]. 2024 [cited 2025 Nov 26]. Available from: https://blog.immunitynetworks.com/

[13] Raju R, Abd Rahman NH, Ahmad A. Cyber security awareness in using digital platforms among students in a higher learning institution. Asian J Univ Educ. 2022;18(3):757-766.

[14] Bottyán L. Cybersecurity awareness among university students. J Appl Tech Educ Sci (JATES). 2023;13(3):1-11.

[15] Cybersecurity awareness level: The case of Saudi Arabia university students. Int J Adv Comput Sci Appl. 2021;12(3).

[16] Moallem A. Cybersecurity Awareness Among Students and Faculty. Boca Raton: CRC Press; 2019.

[17] Check Point Software. VLAN – Segmentation and Security [Internet]. 2023 [cited 2025 Nov 26]. Available from: https://www.checkpoint.com/

[18] Cisco Press. Segmentation – Security through network fundamentals [Internet]. 2019 [cited 2025 Nov 26]. Available from: https://www.ciscopress.com/

[19] Prince M. Network segmentation for better security and speed [Internet]. LCNTech; 2024 [cited 2025 Nov 26]. Available from: https://www.lcntech.com/

[20] Implementing wireless segmentation – How to implement wireless network segmentation and why it is important. GeeksforGeeks [Internet]. Updated 2025 Nov 8 [cited 2025 Nov 26]. Available from: https://www.geeksforgeeks.org/

[21] ARP spoof detection and mitigation. Int J Eng Res Technol. 2023;12(11).

[22] Detection and mitigation of ARP spoofing attack. In: Advances in Computer and Communication Technologies. Springer; 2023. p. 1-12.

[23] Detecting and preventing ARP spoofing attacks using real-time data analysis and machine learning. Int J Innov Res Comput Sci Technol. 2024;12(1).

[24] Rajamurugan A, et al. Detection and localization of multiple spoofing attacks in wireless networks: A Python-based real-time security monitoring approach for local area networks. Int J Sci Dev Res. 2025;10(5):e81-e88.

[25] Snort Project. Snort – Network Intrusion Detection & Prevention System [Internet]. 2025 [cited 2025 Nov 26]. Available from: https://www.snort.org/

[26] Widodo T, et al. Implementation of intrusion detection system (IDS) and Snort community rules to detect types of network attacks. Int J Comput Appl. 2021;183(42):31-36.

[27] Naldi LD, Siswanto A. Design and implement of intrusion prevention system based on Snort and IP tables. J Comput Res Innov. 2025;10(1).