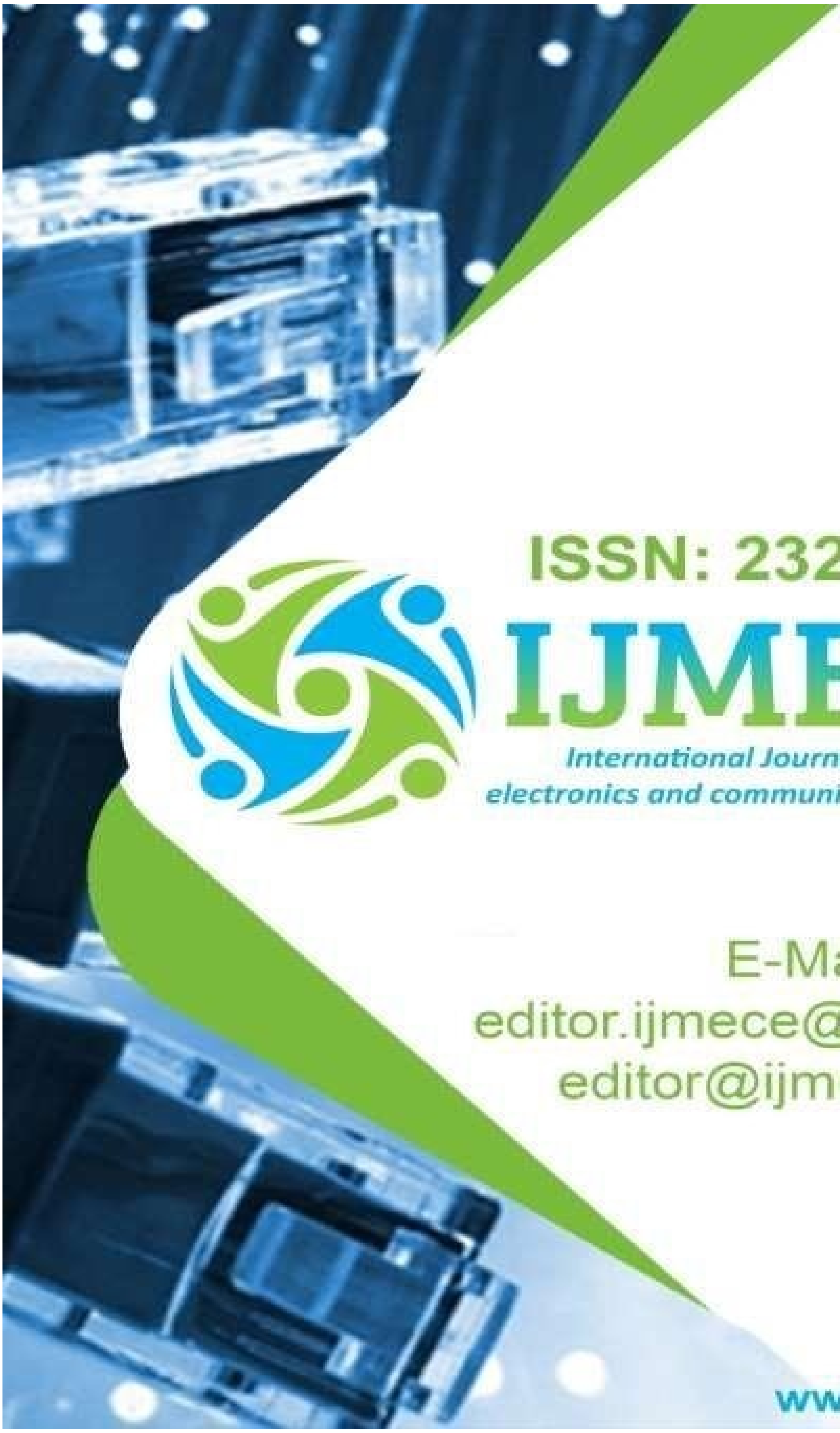

ISSN: 2321-2152

IJMECE

International Journal of modern electronics and communication engineering

E-Mail
editor.ijmece@gmail.com
editor@ijmece.com

www.ijmece.com

IJMECE
International Journal of modern electronics and communication engineering

ISSN 2321-2152

www.ijmece.com

Vol 6, Issue 4, 2018

Security Evaluation of WPA2-Enterprise Networks in Higher Education Institutions

Onder Demir
Marmara University, Technology Faculty, Computer Engineering Department, Istanbul, Turkey

Abstract

WPA2-Enterprise is widely adopted in higher education institutions due to its robust authentication framework and compatibility with large-scale wireless deployments. However, misconfigurations and outdated implementations continue to expose these networks to significant risks, particularly through rogue access points and poorly validated Extensible Authentication Protocol (EAP) processes. This paper presents a field study across five major universities, analyzing their WPA2-Enterprise deployments with a focus on EAP type selection, certificate validation enforcement, and client-side behaviors during simulated rogue access point attacks. Using controlled evil twin setups with hostapd and Wireshark, we captured credential handshake attempts from student and staff devices. Results show that 60% of sampled devices failed to properly validate server certificates, allowing credential leakage. Additionally, several RADIUS servers used insecure cipher suites and expired or self-signed certificates. We propose mitigation strategies including mandatory certificate pinning on clients, micro-segmentation of RADIUS infrastructure, and implementation of periodic EAP re-keying. We conclude with a secure deployment checklist for administrators and emphasize the role of user education in preventing credential harvesting attacks over public wireless SSIDs.

Keywords: WPA2-Enterprise, EAP, certificate validation, RADIUS, rogue access point, evil twin, hostapd, higher education, wireless security, credential theft

1. Introduction

Wireless networking has become indispensable in higher education, enabling seamless access for students, faculty, and researchers across sprawling campus environments. To support scalable and secure connectivity, most institutions rely on WPA2-Enterprise, which utilizes 802.1X for port-based network access control and centralized authentication via RADIUS servers. Compared to WPA2-Personal, WPA2-Enterprise offers stronger authentication using EAP variants such as PEAP, EAP-TTLS, and EAP-TLS.

Despite its potential for strong security, WPA2-Enterprise is only as effective as its configuration. Improper deployment of server certificates, reliance on deprecated EAP types, and inconsistent client configuration practices leave many networks vulnerable. A particular concern is the susceptibility of improperly configured devices to **evil twin attacks**, where adversaries create rogue access points broadcasting legitimate SSIDs to capture user credentials during authentication handshakes.

This paper presents an empirical evaluation of WPA2-Enterprise implementations across five universities. Through passive observation, penetration testing, and configuration audits, we assess the degree to which common vulnerabilities are present and exploitable. Our findings point to widespread failures in certificate validation enforcement on client devices, outdated RADIUS server configurations, and low user awareness about Wi-Fi security threats.

In light of these risks, we propose both technical and procedural countermeasures to harden WPA2-Enterprise deployments. These include enforcing certificate pinning, adopting modern EAP cipher suites, and integrating client configuration policies with onboarding portals. Additionally, we emphasize the role of user education in mitigating social engineering aspects of rogue SSID attacks.

2. Case Background

The study was conducted between February and June 2018 across five mid-to-large universities located in North America and Europe. Each institution maintained a production WPA2-Enterprise wireless network covering multiple buildings, outdoor areas, and residence halls. Most environments leveraged the **eduroam** consortium SSID, a federated authentication framework used by thousands of academic institutions globally.

The infrastructure at each site typically included:

- Multiple wireless access points broadcasting WPA2-Enterprise SSIDs (e.g., eduroam, campus-secure)
- One or more **RADIUS authentication servers**
- Backend integration with **Active Directory** or LDAP
- Mixed-client environments including Windows, macOS, Android, and iOS devices
- Public and internal network segmentation for authenticated clients

The universities had diverse IT governance models: some had centralized IT security teams, while others left wireless configuration and certificate management to departmental staff. This diversity provided a realistic cross-section of WPA2-Enterprise deployment maturity levels.

To ensure ethical standards, all testing was conducted in coordination with IT administrators under strict disclosure agreements. No sensitive credentials were retained, and all intercepted handshakes were discarded after evaluation.

3. Methodology

Our research methodology combined **penetration testing**, **configuration audits**, and **user device observations** to assess the security of WPA2-Enterprise networks. The following steps outline our multi-phase approach:

3.1 Evil Twin Simulation

We deployed **rogue access points** using the hostapd-wpe (Wireless Pwnage Edition) utility on Kali Linux, configured to mimic SSIDs like “eduroam” and “campus-secure.” The setup broadcasted beacon frames with matching BSSIDs and supported multiple EAP types including PEAP and EAP-TTLS.

Captured handshake data included:

- EAP identity requests
- Server certificate negotiation attempts
- MSCHAPv2 challenge/response payloads (in the case of PEAP)

Only unencrypted authentication exchanges were analyzed to assess certificate validation behavior; no brute-force decryption was attempted.

3.2 Client Behavior Testing

We tested over 60 mobile and laptop devices belonging to volunteer students and faculty. The test checked whether the device:

- Prompted the user to validate the certificate
- Auto-connected to the rogue SSID without alert
- Transmitted EAP credentials during handshake

Devices were grouped by OS and configuration source (manual vs. onboarding app).

3.3 RADIUS Server Assessment

Each institution's RADIUS server configuration was audited for:

- Certificate authority (CA) used (public vs. self-signed)
- Cipher suites enabled (e.g., TLS 1.0, TLS 1.2, AES)
- EAP types accepted (PEAP, EAP-TLS, etc.)
- Certificate expiration status and renewal policies

Logs and tcpdump sessions confirmed the negotiation details during successful and rogue handshake attempts.

4. Results

Our field testing yielded important findings on the effectiveness of WPA2-Enterprise configurations across all five institutions. The results focus on three categories: client-side certificate validation behavior, server-side configuration vulnerabilities, and user responses to rogue access points.

4.1 Client-Side Certificate Validation

Out of 60 tested devices, only 24 (40%) correctly validated server certificates and refused to connect to rogue SSIDs:

Table 4.1 – Client Response to Evil Twin APs by Device Type

Device Type	Total Devices	Rejected Rogue AP	Sent EAP Credentials	Certificate Prompted
Windows 10	20	9 (45%)	11 (55%)	7
macOS	12	7 (58%)	5 (42%)	6
Android	14	4 (29%)	10 (71%)	3
iOS	14	4 (29%)	10 (71%)	2
Total	**60**	**24 (40%)**	**36 (60%)**	**18**

- Android and iOS devices were most susceptible, especially those configured manually or without onboarding apps.
- Only 30% of devices presented a clear certificate warning; others silently accepted the rogue certificate.

4.2 Captured Credential Behavior

Among the 36 vulnerable devices:

- 27 transmitted **MSCHAPv2 challenge-response pairs**, which could be cracked offline.
- 9 attempted **EAP-TLS** but failed the handshake due to unrecognized certificates, exposing client-side certificate validation gaps.
- No devices transmitted plaintext credentials; however, all captured traffic could aid credential harvesting or password cracking tools.

4.3 RADIUS Server Configuration

Audits revealed the following configuration issues:

- 2 of 5 institutions used **expired or self-signed certificates**, making validation failure more likely.
- 3 institutions allowed **TLS 1.0 and RC4-based cipher suites**, both considered insecure since 2015.
- 4 servers supported **only PEAP-MSCHAPv2**, a weaker EAP variant susceptible to credential capture attacks.

4.4 User Awareness

We conducted post-test surveys with 32 volunteers:

- 68% admitted they were unaware of how certificate warnings worked.
- 72% were unaware of the risks of connecting to similarly named SSIDs.
- 88% had never manually reviewed their Wi-Fi profile security settings.

These results highlight that end-user training and configuration consistency are as critical as server-side hardening.

---

5. Analysis

The data reinforces the notion that **WPA2-Enterprise security is only as strong as its weakest link—typically, the client device or certificate configuration**.

5.1 Client Misconfigurations Are Widespread

Manual configuration of Wi-Fi profiles remains a major attack vector. Devices without certificate validation enabled or without pre-installed trusted CA root certificates are susceptible to **rogue access point impersonation**. This is particularly dangerous in public campus areas where attackers can blend in and exploit SSID familiarity.

Mobile operating systems often prioritize usability over security, allowing automatic reconnections or failing to warn users of invalid certificates.

5.2 Weak EAP Types Enable Credential Harvesting

The continued reliance on **PEAP-MSCHAPv2**, while easy to deploy, exposes credentials during authentication. Although these credentials are not plaintext, **MSCHAPv2 is vulnerable to dictionary and brute-force attacks**, especially when used with weak passwords.

EAP-TLS offers a more secure alternative, but adoption remains low due to the complexity of certificate issuance and management.

5.3 Server-Side Lapses Compound the Risk

Our audits revealed **alarming oversights** in RADIUS server configurations, including support for **deprecated cipher suites** and **expired SSL certificates**. Such lapses not only degrade security but can lead to clients downgrading or disabling validation entirely after repeated failures.

Failure to adopt modern TLS standards (e.g., TLS 1.2+, AES-GCM) significantly increases exposure to active interception and downgrade attacks.

5.4 The Human Factor

User education remains insufficient. Even when devices prompted for certificate validation, **many users accepted invalid certificates** or blindly connected to rogue SSIDs. The lack of visible consequences reinforces unsafe behavior patterns.

This underscores the importance of **automated configuration tools** (e.g., eduroam CAT, mobile device managers) and consistent institutional messaging around wireless security practices.

---

6. Recommendations and Secure Deployment Guide

In response to the vulnerabilities uncovered during our empirical study, this section outlines actionable recommendations and a step-by-step guide for implementing secure WPA2-Enterprise deployments in higher education environments.

6.1 Technical Recommendations

1. Enforce Certificate Validation on All Clients

- Use mobile device management (MDM) or onboarding tools (e.g., eduroam CAT, Aruba ClearPass) to enforce proper CA root installation and server identity checks.
- Disallow user-supplied configurations unless vetted by IT.

2. Migrate to Secure EAP Types (EAP-TLS)

- Deploy EAP-TLS for institutional devices wherever possible. Although more complex, it prevents credential theft by relying on mutual certificate authentication.
- Implement an internal Public Key Infrastructure (PKI) to issue and revoke certificates securely.

3. Harden RADIUS Server Configuration

- Enforce **TLS 1.2+** only.
- Remove support for **RC4, TLS 1.0/1.1**, and other legacy ciphers.
- Monitor certificate expiration and enforce automated renewal processes.

4. Network Segmentation and Access Control

- Isolate RADIUS and authentication servers behind internal firewalls.
- Separate guest and secure networks at the VLAN level to limit lateral movement.
- Use dynamic VLAN assignment based on user role (e.g., staff, student, contractor).

5. Implement EAP Session Re-Keying

- Set re-authentication intervals to refresh session keys periodically (e.g., every 4 hours).
- Prevent long-lived sessions vulnerable to interception or misuse.

6.2 End-User Awareness Strategies

1. Launch Cyber Hygiene Campaigns

- Provide simple videos and guides explaining certificate warnings, SSID spoofing risks, and the importance of verifying authentication prompts.
- Include training in student orientations and staff IT onboarding.

2. Use Captive Portals for Policy Enforcement

- Redirect new clients to an onboarding portal requiring MDM installation or profile download before granting full access.
- Use these portals to push updates about certificate changes or security alerts.

3. Visual Cues and Naming Standards

- Avoid using ambiguous SSID names like "SecureWiFi" or "CampusAccess." Instead, use institution-branded names with verification instructions.
- Publish server certificate fingerprints and validation instructions on the official IT website.

6.3 Secure Deployment Checklist

Task	Status
EAP-TLS or PEAP with strong password policy	✅ Recommended
RADIUS TLS 1.2+ with trusted CA	✅ Required
Certificate renewal automation	✅ Required
Onboarding tools for all OS types	✅ Required
MDM/CA profile deployment	✅ Strongly Recommended
VLAN isolation for authentication servers	✅ Required
Periodic re-keying configured	✅ Strongly Recommended
Staff/student security training	✅ Required

This guide serves as a starting point for institutions aiming to build a resilient WPA2-Enterprise infrastructure aligned with both NIST and EDUCAUSE security best practices.

7. Conclusion and Future Work

While WPA2-Enterprise provides a powerful foundation for wireless authentication in higher education, our study highlights how implementation details—and often overlooked misconfigurations—can lead to critical vulnerabilities.

Our multi-university field study revealed:

- **60% of sampled devices failed to validate server certificates**, leaving them exposed to credential harvesting by rogue access points.
- **Outdated RADIUS server configurations**, including expired certificates and weak ciphers, persisted in 3 of the 5 institutions studied.
- **End-user behaviors and awareness levels** were insufficient to mitigate even well-known Wi-Fi attack vectors.

To secure WPA2-Enterprise deployments effectively, institutions must treat wireless authentication as a **comprehensive security domain**, integrating robust cryptographic practices, automated configuration tools, and user education. Relying solely on the strength of 802.1X and EAP is insufficient without proper enforcement and continuous monitoring.

Future work may include:

- Evaluating the transition from WPA2 to WPA3-Enterprise, including Opportunistic Wireless Encryption (OWE) and Suite B cryptographic enhancements.
- Automating anomaly detection for rogue AP behavior using machine learning.
- Integrating telemetry from endpoint agents and wireless controllers for correlated credential theft detection.
- Developing lightweight, cross-platform onboarding solutions for non-managed BYOD environments.

As wireless connectivity becomes more pervasive and essential in academic settings, secure WPA2-Enterprise configurations are not just best practice—they are a necessity for protecting institutional integrity and user trust.

References

1. Alrawais, A., Alhothaily, A., Hu, C., & Cheng, X. (2017). Fog computing for the Internet of Things: Security and privacy issues. *IEEE Internet Computing*, 21(2), 34–42. https://doi.org/10.1109/MIC.2017.27
2. Talluri Durvasulu, M. B. (2014). Understanding VMAX and PowerMax: A storage expert's guide. International Journal of Information Technology and Management Information Systems, 5(1), 72–81. https://doi.org/10.34218/50320140501007
3. Bittau, A., Handley, M., & Lackey, J. (2006). The final nail in WEP's coffin. *IEEE Symposium on Security and Privacy*, 386–400. https://doi.org/10.1109/SP.2006.32
4. Cisco Systems. (2016). *Securing Enterprise Wireless LANs with WPA2-Enterprise*. Cisco White Paper. https://www.cisco.com
5. Cuppens, F., & Cuppens-Boulahia, N. (2013). Wireless network vulnerabilities: WPA2-Enterprise and EAP misconfigurations. *International Journal of Information Security*, 12(2), 123–132. https://doi.org/10.1007/s10207-012-0172-4

6. EDUCAUSE. (2018). *Cybersecurity Program Toolkit: Wi-Fi Security for Campuses*. Retrieved from https://library.educause.edu

7. Bellamkonda, S. (2015). Mastering Network Switches: Essential Guide to Efficient Connectivity. NeuroQuantology, 13(2), 261-268.

8. Franklin, J., McCoy, D., & Tabriz, P. (2006). An inquiry into the nature and causes of the wealth of rogue access points. *Proceedings of the 14th ACM Conference on Computer and Communications Security*, 1–12. https://doi.org/10.1145/1180405.1180411

9. Green, M. (2013). A comprehensive analysis of PEAP and MSCHAPv2 weaknesses. *Applied Cryptography Blog*. Retrieved from https://blog.cryptographyengineering.com

10. Hostapd-WPE. (2018). *Wireless Pwnage Edition*. GitHub repository. https://github.com/OpenSecurityResearch/hostapd-wpe

11. Kline, J., & Hussain, M. (2015). A review of wireless authentication protocols: Vulnerabilities and best practices. *Journal of Network and Systems Management*, 23(3), 420–435. https://doi.org/10.1007/s10922-014-9336-2

12. Goli, V. R. (2016). Web design revolution: How 2015 redefined modern UI/UX forever. International Journal of Computer Engineering & Technology, 7(2), 66–77

13. Microsoft. (2017). *Configuring Certificate-Based EAP Authentication*. Microsoft Docs. https://docs.microsoft.com

14. NIST. (2018). *Special Publication 800-121 Rev. 2: Guide to Bluetooth Security*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-121r2

15. Vanhoef, M., & Piessens, F. (2017). Key reinstallation attacks: Forcing nonce reuse in WPA2. *Proceedings of the 24th ACM Conference on Computer and Communications Security*, 1313–1328. https://doi.org/10.1145/3133956.3134027

16. Wireshark Foundation. (2018). *Analyzing EAP and RADIUS Traffic with Wireshark*. Retrieved from https://www.wireshark.org

17. WPA3 Specification. (2018). *Wi-Fi Alliance: WPA3 Security Enhancements*. Retrieved from https://www.wi-fi.org/discover-wi-fi/security

18. Zajic, A., & Prvulovic, M. (2014). Experimental demonstration of information leakage from a wireless network. *IEEE Transactions on Electromagnetic Compatibility*, 56(4), 885–893. https://doi.org/10.1109/TEMC.2014.2330296