base/dynamic-routing-protocols-ospf-eigrp-ripv2-is-is-bgp/ta-p/4511577 (дата звернення: 20.04.2026).
3. Кульчинський І. Аналіз роботи протоколів динамічної маршрутизації. Збірник тез V Всеукраїнської студентської науково-технічної конференції „Природничі та гуманітарні науки. Актуальні питання “, 2012, 1: 67-67.

Analysis of Authentication-Based Attacks in Wireless Networks

UDC 004.7.056

Danylo Matiuk[1], Maryna Derkach[2],
Inna Skarga-Bandurova[3]

Ternopil Ivan Puluj National Technical University,
[1]matiuk.danylo@icloud.com, [2]m_derkach@tntu.edu.ua,
Oxford Brookes University,
[3]iskarga-bandurova@brookes.ac.uk

Modern wireless networks play a crucial role in data exchange and are widely deployed across commercial, governmental, educational, and residential environments. However, they remain among the most vulnerable components of both corporate and household security infrastructures. As their adoption increases, so does the number of potential targets for cyberattacks. Most attacks on wireless networks target authentication mechanisms, as these mechanisms are designed to prevent unauthorized access to access points.

Several widely used protocols provide secure authentication for wireless networks, including WPA, WPA2, and WPA3. These protocols differ in the data required for successful authentication, as well as in their encryption and validation methods. Each protocol supports two main authentication modes: WPA-Personal and WPA-Enterprise. The WPA-Personal mode relies on a pre-shared key (PSK), where all users and devices must know the same password to access the network. In contrast, WPA-Enterprise uses a RADIUS server for centralized authentication, where user credentials are verified individually.

Although WPA is considered obsolete for modern devices, it is still used in practice, particularly in low-power or legacy systems that rely on older algorithms. Similarly, WPA2, introduced in 2006 as the standard for secure Wi-Fi networks, remains widely used today. This is supported by the results of a wireless network scan (Fig. 1) performed using a portable NetScope device as part of ethical hacking activities [1].

SSID	RSSI	Channel	Security	Vendor	BSSID
[redacted]	-59 dBm	11	WPA*	Shenzhen	[redacted]
	-65 dBm	10	WPA2		
	-71 dBm	2	WPA*	TendaTec	
	-80 dBm	1	WPA2	Tp-LinkT	
	-81 dBm	1	WPA*		
	-82 dBm	10	WPA*	TendaTec	
	-83 dBm	6	WPA2		
	-88 dBm	8	WPA*		

Fig.1. Results of a wireless network scan

The compromise of wireless networks is rarely an isolated issue and often serves as an entry point for deeper intrusions into IT environments. By analysing information

broadcast over the air about wireless networks and associated client devices – including hidden SSID/BSSID, channels, signal strength, security mechanisms, and equipment manufacturers – an attacker can assess the level of radio-frequency security within a given environment and determine an appropriate attack strategy. In WPA2-Personal networks, authentication and key establishment are performed using a four-way handshake. Attacks targeting the four-way handshake aim to exploit vulnerabilities in the process of establishing a secure connection between a client device and a wireless access point. During the attack, adversaries attempt to exploit the four-way handshake used for authentication and key establishment by transmitting deauthentication frames, which belong to the IEEE 802.11 control frame subclass. These frames operate at the lower levels of the Wi-Fi protocol stack and are used to terminate connections. The presence of a deauthentication reason code field enables analysis of how control messages are processed by the receiving side and provides a formal description of connection termination events. As the network becomes destabilized, the attacker may deploy a rogue access point that mimics the target SSID. If the PSK is known, an Evil Twin attack can be performed, forcing the victim's traffic to pass through the attacker-controlled node and enabling Man-in-the-Middle scenarios, such as credential interception and content manipulation [2]. The Evil Twin attack is also relevant to WPA2-Enterprise networks. Although WPA2-Enterprise is generally considered more secure than WPA2-Personal, it remains vulnerable to online brute-force attacks. Since WPA2-Enterprise credentials often correspond to domain user accounts, compromised credentials may enable unauthorized access to additional systems within a corporate network.

In January 2018, the Wi-Fi Alliance introduced WPA3 as a successor to WPA2. WPA3 enhances security through the implementation of the Simultaneous Authentication of Equals (SAE) protocol and the Dragonfly key exchange mechanism, which provide stronger protection against password-based attacks. However, in 2019, several vulnerabilities were identified, including downgrade attacks exploiting backward compatibility, where a client can be forced to connect to a rogue WPA2 access point, allowing attackers to capture the handshake.

Based on the analysis of attacks on wireless security protocols, several conclusions can be drawn. WPA3 replaces the vulnerable PSK–based authentication approach, which allows attackers to capture Wi-Fi traffic and perform offline brute-force attacks, with a more secure SAE-based key exchange mechanism. Nevertheless, given the widespread use of WPA2, the following considerations remain important:

1) The Evil Twin attack on WPA2-Enterprise is ineffective against clients that use certificate-based authentication methods (e.g., EAP-TLS or PEAP with EAP-TLS), as no reusable credentials are exposed and server certificate validation is enforced during the initial authentication phase.
2) Protection against dictionary attacks relies on the use of strong and unique passwords. Additionally, the Pairwise Transient Key PTK, which is generated per session, ensures secure data transmission by encrypting communication between the client device and the access point.

1. Matiuk, D. S., & Derkach, M. V. (2025). NetScope: pentestinh bezdrotovykh merezh [NetScope: wireless network pentesting].

Proceedings of the XIV International Scientific and Technical Conference of Young Scientists and Students “Current Issues of Modern Technologies”, 11-12 December 2025, Ternopil, 302-304. PE Palianytsia V.A. [in Ukrainian].

2. Banakh, R., Nyemkova, E., Justice, C., Piskozub, A., & Lakh, Y. Data Mining Approach for Evil Twin Attack Identification in Wi-Fi Networks. Data, 2024, vol. 9(10), p. 119.

Налаштування безпечної мережевої інфраструктури для балансування навантаження та відмовостійкості

УДК 004.7:004.056

Вікторія Ваврічен[1], Тарас Лобур[2]

Тернопільський національний технічний університет імені Івана Пулюя, [1]viktoriavavrichen@gmail.com, [2]lobur_t@tntu.edu.ua

У сучасних комп’ютерних мережах важливим завданням є забезпечення стабільного й безпечного доступу до Інтернету та безперервної передачі даних. Для організацій, які використовують хмарні сервіси, відеозв’язок, віддалене адміністрування та інші онлайн-ресурси, навіть короткочасна втрата з’єднання може спричинити порушення робочих процесів. Тому актуальним завданням є використання кількох незалежних каналів зв’язку для балансування навантаження та автоматичного перемикання на резервний канал.

Під час дослідження було використано VMware Workstation, у якому створено віртуальне тестове середовище. VMware Workstation дозволяє використовувати віртуальні мережеві адаптери, комутатори та окремі віртуальні мережі, що є зручним для тестування мережевих сценаріїв, зокрема пропускної здатності, стабільності та безпеки з’єднання. Основним мережевим пристроєм виступив MikroTik RouterOS CHR.

У тестовому середовищі було змодельовано мережеву інфраструктуру з трьома незалежними каналами зв’язку, зокрема основний WAN-канал, Starlink та LTE як резервне підключення. На початковому етапі було виконано базове налаштування MikroTik RouterOS: призначено IP-адреси інтерфейсам, налаштовано шлюзи, DNS, локальну мережу та правила NAT [1]. NAT використовувались для забезпечення безпечного доступу внутрішньої мережі до зовнішніх ресурсів через кожен з каналів зв’язку. Наступним етапом було застосовано механізм Mangle з використанням алгоритму per-connection-classifier для реалізації балансування навантаження, що дало можливість розподілити трафік на три частини. Далі виконано маркування з’єднання і пакетів відповідно до таблиць маршрутизації, які забезпечують рівномірний розподіл трафіку між усіма трьома каналами, що забезпечує коректну маршрутизацію навіть у випадку відмови одного з них.

Після налаштування балансування навантаження та відмовостійкості на базі MikroTik RouterOS було проведено моніторинг мережевого трафіку. Для цього використовувалися такі інструменти, як Ping, Tracert, SpeedTest, а також Wireshark для глибшого аналізу пропускної здатності, стабільності та безпеки