УДК 621.396:004.7]:004.056
DOI https://doi.org/10.30837/IYF.PDICIMT.2024.168

ШИФРУВАННЯ WI-FI 6-МЕРЕЖ

Фодченко А.В.
Науковий керівник – к.т.н., доц. Золотарьов В.А.
Харківський національний університет радіоелектроніки, каф. IMI,
м. Харків, Україна
e-mail: anastasiia.fodchenko@nure.ua

The purpose of this article is to look at and analyze the main aspects of encryption in Wi-Fi 6 in order to understand its importance, effectiveness and impact on the security and privacy of data. The report aims to present the technical details of encryption, including the developed cryptographic algorithms and protocols, as well as evaluate its effectiveness against a variety of threats and attacks. In addition, the evidence can include continuous analysis of the latest versions of Wi-Fi protocols, highlighting the advantages and disadvantages of the new approach to encrypting Wi-Fi data.

Розвиток Wi-Fi технології потребує удосконалення методів шифрування для забезпечення конфіденційності та цілісності даних у бездротових мережах. Покращення шифрування Wi-Fi 6-мереж (802.11ax) – запорука безпеки бездротового з'єднання. У 2018 р. організація Wi-Fi випустила нове покоління протоколу шифрування відоме як WPA3, розроблене для забезпечення простішої конфігурації та надійнішого шифрування та безпеки ніж його попередник WPA2 [1]. WPA3 є останнім поколінням протоколу захисту Wi-Fi, розробленим для забезпечення високого рівня безпеки в бездротових мережах.

Одним із найбільших удосконалень захисту приватності у WPA3 є реалізація підвищеної політики безпеки паролів за допомогою системи обміну ключами Dragonfly також відому як Simultaneous Authentication of Equals (SAE), який замінює метод Pre-Shared Key (PSK) у WPA2. SAE ускладнює злом паролів за рахунок більш «тонкого» методу встановлення з’єднання з Wi-Fi та нейтралізує атаки зловмисників на основі словника, від яких страждає PSK, таким чином, ефективно запобігає автоматизованому пошуку паролів для WLAN.

WPA3 також блокує раніше дозволені небезпечні хеші, такі як SHA1 або MD5. Для хешованого пароля Wi-Fi тепер використовується криптографія з еліптичною кривою: client і Wi-Fi роутер. Учасники інформаційного обміну домовляються про параметри еліптичної кривої і за допомогою пароля створіть точку на цій кривій. Потім кожна сторона вибирає випадкове число; клієнт використовує випадкове U, Wi-Fi роутер використовує число V. Клієнт обчислює uR, тобто кратне R на еліптичній кривій, яка в свою чергу обчислює і відправляє vR. Потім обидві сторони обчислюють і порівнюють загальний добуток і багато іншого як ключ. Проблема зловмисників полягає в тому, що, хоча вони перехоплюють R і

uR, а також vR, вони не можуть обчислити u і v з них, тому що їм довелося б обчислювати дискретний логарифм. Ще одна перевага аутентифікації за допомогою SAE полягає в тому, що навіть після перехоплення інформації, зловмисники не можуть потім розшифрувати записані повідомлення. Цей принцип називається Perfect Forward Secrecy (PFS) [2].

WPA3 застосовує вдосконалений стандарт шифрування AES у режимі GCM, який є надійнішим за AES-CCMP, що використовується в WPA2. Використання в WPA3 режиму захисту Opportunistic Wireless Encryption (OWE) забезпечує захищене з'єднання без необхідності введення пароля навіть при підключенні до невідомих або ненадійних мереж.

WPA3 використовує уніфіковану криптографію з більш надійним 192-бітним шифруванням, допомагаючи уникнути об'єднання протоколів безпеки, визначених у стандарті 802.11. Також WPA3 вимагає узгодження MPF (Protected Management Frames). PMF додає додатковий рівень безпеки для захисту від атак деаутентифікації та деасоціації [3].

До того ж WPA3 надає індивідуальне шифрування для кожного бездротового з'єднання. Тобто злам зловмисником одного з'єднання не дозволяє йому автоматично отримати доступ до інших з'єднань у мережі. Нагадаємо, що WPA2 використовує спільний ключ шифрування для всіх пристроїв, підключених до однієї мережі, і у разі компрометації ключа створює ризики для безпеки, якщо ключ буде скомпрометований.

WPA3 захищає від атак типу KRACK (Key Reinstallation Attacks), до яких був вразливий WPA2, завдяки вдосконаленій методології аутентифікації та захисту від атак на основі бокового каналу.

Отже Wi-Fi 6 є безпечнішим за попередні версії протоколів Wi-Fi. Впровадження WPA3, удосконалене та індивідуальне шифрування даних дозволяють підвищити рівень безпеки та захисту приватності у бездротових мережах. Втім слід пам'ятати, що безпека мережі залежить не лише від технологічних рішень, але й від правильної конфігурації та використання заходів безпеки всіма користувачами.

Список використаних джерел:

1. WiFi 6 vs WiFi 5, Which is Better in Performace? [Електронний ресурс]. – 2022. – Режим доступу до ресурсу: https://www.vsolcn.com/blog/wifi-6-vs-wifi-5.html.

2. WPA3 на Fritzbox [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://www.chip.de/artikel/WPA3-Neue-WLAN-Verschluesselung-optimal-nutzen_148220425.html.

3. У 2019 був затверджений стандарт WiFi 6. Що це таке і якими функціями забезпечили Wi-Fi 6? [Електронний ресурс] / GDS. – 2023. – Режим доступу до ресурсу: https://realweb.net.ua/blog/u-2019-buv-zatverdzhenij-standart-wifi-6-sho-ce-take-i-yakimi-funkciyami-zabezpechili-wi-fi-6_1.