

УДК 004.056

Лізунов С.І.¹, Корольков Р.Ю.², Куцак С.В.³

¹ канд. техн. наук, доц. НУ «Запорізька політехніка»

² канд. техн. наук, ст. викл. НУ «Запорізька політехніка»

³ студ. гр. РТЗ-811м НУ «Запорізька політехніка»

ОГЛЯД ПРОТОКОЛІВ БЕЗПЕКИ БЕЗДРОТОВИХ МЕРЕЖ СТАНДАРТУ 802.11

Бездротова передача даних, що ґрунтується на сімействі стандартів IEEE 802.11, об'єднує декілька протоколів безпеки, затверджених у різні роки.

Основні протоколи, що застосовуються в бездротових мережах 802.11, відомі як Wired Equivalent Privacy (WEP) і WiFi Protected Access (WPA).

WEP був першим протоколом безпеки IEEE 802.11, представленим в 1999 році. Протокол WEP дозволяє шифрувати потік переданих даних на основі алгоритму RC4 (Ron's Code 4) з ключем розміром 64 або 128 біт.

Дані ключі мають так звану статичну складову довжиною від 40 до 104 біт і додаткову динамічну складову розміром 24 біта, т.зв. вектор ініціалізації (Initialization Vector, IV).

Використання короткого 24-бітного вектору ініціалізації (IV) в кінцевому підсумку і призвело до припинення використання WEP. До того ж, для забезпечення цілісності, WEP використовує алгоритм CRC-32. В силу лінійності CRC-32 підробити контрольну суму можна і без знання ключа.

Дослідниками в області інформаційної безпеки було показано, що WEP містить серйозні уразливості [1,2], і в 2004 році WEP- був відзначений як небезпечний та функціонально застарілий протокол не рекомендований до використання, за винятком випадків зворотної сумісності з існуючими пристроями IEEE 802.11.

У 2003 році було запущено нове покоління протоколів безпеки WPA, з метою усунення недоліків WEP без необхідності заміни обладнання. Даний протокол захисту став використовуватися в ролі проміжного рішення до прийняття IEEE 802.11i.

Одною з основних змін було введення протоколу інтеграції тимчасового ключа TKIP (Temporal Key Integrity Protocol). На відміну від WEP, WPA-TKIP дозволяє динамічне генерувати новий 128-бітний ключ шифрування для кожного пакета.

Крім довшого вектору ініціалізації (IV), розмір якого збільшений до 48 біт, він також використовує 64-бітний MIC (Message Integrity Code) для більш високого рівня безпеки для підтримки цілісності [3].

Проте, переваги протоколу TKIP не покривають його основний недолік - алгоритм шифрування RC4, що використовувався і раніше і який все також не задовольняє вимогам безпеки. У 2012 році протокол WPA оголошений застарілим [4].

У червні 2004 року остаточна версія, що реалізує специфікацію 802.11i, була ратифікована під назвою WPA ver.2 [5].

WPA2 покращує захист даних, вводячи обов'язкове використання протоколу шифрування CCMP (Counter-Mode-CBC-MAC Protocol), заснований на криптографічному алгоритмі AES (Advanced Encryption Standard), що є більш захищеним, ніж TKIP. AES є симетричним алгоритмом блочного шифрування (з розміром блоку 128 біт), який використовує один і той же ключ довжиною 128 біт як для шифрування, так і для дешифрування даних.

Варто відзначити, що в CCMP при кожній новій сесії використовуються нові тимчасові ключі.

WPA має декілька режимів роботи - корпоративний і для особистого використання.

Корпоративний режим, протокол WPA-Extensible Authentication Protocol (WPA-EAP), використовує більш сувору автентифікацію 802.1x і вимагає використання окремого сервера автентифікації.

Персональний режим, WPA-Pre-Shared Key (WPA-PSK), використовує попередні загальні ключі для спрощення впровадження та управління серед споживачів і малих офісів.

В даний час WPA2 є найпоширенішим і часто використовуваним стандартом безпеки.

Однак в ньому були виявлені серйозні вразливості. WPA/WPA2 вразливий для атак типу «відмова в обслуговуванні», які здійснюються на рівні MAC шляхом відправки підроблених повідомлень деавтентифікації і деасоціації клієнту або до точки доступу, в результаті чого порушується зв'язок [6].

Атаки з використанням словника або грубої атаки дозволяли підібрати слабкий пароль. А у 2017 році в протоколі WPA2 було виявлено серйозну вразливість і були опубліковані результати дослідження атаки з перевстановленням ключа, що отримала назву KRACK (Key Reinstallation Attack).

При атаці KRACK зловмисник, змушує жертву перевстановити криптографічний ключ на третьому етапі 4-етапного «рукоутискання».

Ця вразливість дозволяє зловмиснику перехоплювати трафік, що проходить між точкою доступу Wi-Fi та підключеними до неї пристроями/станціями.

Ці факти істотно знизили рівень безпеки протоколу WPA2, та підштовхнули Wi-Fi Alliance до розробки WPA ver.3.

WPA ver.3 - це оголошений альянсом Wi-Fi в січні 2018 року новий протокол [7], що підвищує рівень безпеки і усуває деякі недоліки попередніх версій WPA. WPA3 продовжує працювати в двох режимах: Personal і Enterprise. WPA3-Personal забезпечує 128-бітове шифрування даних. WPA3-Enterprise (Suite B) використовує новий криптографічний стандарт з 192-бітовим ключем, аналогічний алгоритму з комплексу CNSA (Commercial National Security Algorithms - Комерційних алгоритмів для захисту національної безпеки).

Розробкою цього набору займався Комітет з систем забезпечення національної безпеки США. WPA3 використовує шифрування AES за допомогою протоколу Galois/Counter Mode Protocol (GCM), який є більш безпечним і ефективним протоколом, ніж CCMP.

У цьому протоколі використовується шифрування AES з розміром ключа 256 біт, що вдвічі перевищує розмір ключа CCMP.

Крім того, для захисту цілісності даних використовується алгоритм SHA384 сімейства SHA2.

У протоколі WPA3, використовується новий метод одночасної рівноправної автентифікації SAE (Simultaneous Authentication of Equals), що надає додатковий захист від брутфорс-атак [8].

Також новою функцією WPA3 є опортуністичне бездротове шифрування Opportunistic Wireless Encryption (OWE), яке підвищує конфіденційність у відкритих мережах за рахунок забезпечення кожному користувачу індивідуального шифрування даних.

Ключ шифрування відрізняється для кожного клієнта, тому жодне з підключених пристроїв не може розшифрувати трафік, призначений для інших клієнтів. OWE використовує опортуністичне шифрування, визначене в стандарті Internet Engineering Task Force RFC 8110, з метою захисту від пасивного підслуховування.

WPA3 також використовує захищені кадри управління Protected Management Frames (PMF) під час обміну кадрами 802.11 між точкою доступу і клієнтами.

Цей механізм є частиною поправки IEEE 802.11w (2009 р.). Його мета - підвищити безпеку фреймів управління Wi-Fi за рахунок забезпечення конфіденційності, цілісності, автентичності та актуальності даних. Використання PMF було необов'язково в WPA і WPA2, але є обов'язковим в WPA3.

Слід зазначити, що хоча для захисту мереж Wi-Fi вже доступна WPA3, однак ця технологія майже не використовується, або через недостатню поінформованість користувачів про безпеку або через потребу у заміні застарілого обладнання.

Широке поширення WPA3 відбудеться тільки після заміни або поновлення маршрутизаторів. Через вразливості, що виявлено в WPA2 ми рекомендуємо використовувати WPA3. Новий стандарт безпеки WPA3 Wi-Fi спрямований на усунення вразливостей застарілих стандартів безпеки та забезпечення високого рівня безпеки.

У випадках, коли потрібно забезпечити найвищий ступінь безпеки, слід використовувати WPA3 Enterprise, який дозволяє використовувати кращі методи автентифікації, такі як використання сертифікатів і стандарт шифрування AES-GCMP.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. B. Jerman-Blažič and W. S. Schneider, Security and Privacy in Advanced Networking Technologies. NATO science series: Computer and systems sciences, IOS Press, 2004.

2. E. Tews and M. Beck, "Practical Attacks Against WEP and WPA," in Proceedings of the Second ACM Conference on Wireless Network Security, pp. 79–86, ACM, 2009. [137] N. AlFardan and D. J. Bernstein and K. G. Paterson and B. Poettering and J. C. N. Schuldt, "On the Security of RC4 in TLS," in Presented as part of the 22nd USENIX Security Symposium, pp. 305–320, USENIX, 2013.

3. Arif Sari, Mehmet Karay "Comparative analysis of wireless security protocols: WEP vs WPA," International Journal of Communications, Network and System Sciences, vol. 8, no. 12, p. 483-491, 2015. DOI: 10.4236/ijcns.2015.812043

4. "IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," in IEEE Std 802.11-2012 (Revision of IEEE Std 802.11-2007), vol., no., pp.1-2793, 29 March 2012, doi: 10.1109/IEEESTD.2012.6178212
5. IEEE, "IEEE Std 802.11i," Amendment 6: Medium Access Control Security Enhancement, 2004.
6. R. Cheema, D. Bansal, Dr. Sanjeev Sofat, "Deauthentication/Disassociation Attack: Implementation and Security in Wireless Mesh Networks", International Journal of Computer Applications, Volume 23, No.7, June 2011.
7. Wi-Fi-Alliance, "WPA3 Specification Version 1.0." <https://www.wi-fi.org>, 2018. Accessed: 2020-01-19.
8. Kohlios, C.P.; Hayajneh, T. A Comprehensive Attack Flow Model and Security Analysis for Wi-Fi and WPA3. Electronics 2018, 7, 284. doi: 10.3390/electronics7110284