УДК 621.391

АНАЛІЗ ВРАЗЛИВОСТІ БЕЗДРОТОВОЇ МЕРЕЖІ WI-FI З НОВИМ ПРОТОКОЛОМ ЗАХИЩЕНОСТІ WPA3

Підпалий О.І., Романов О.І.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського,
E-mail: sashapidpalyi@gmail.com

Analysis of wireless vulnerability WI-FI with new WPA3 security protocol

To date, the issue of data confidentiality is one of the most important in the world. Most of the valuable information is contained on phones and laptops that are constantly connected to Wi-Fi. Therefore, the issue of wireless security is the highest priority to date[1,2]. The WPA2 security protocol has long been the best in this regard, but as time goes on, technology gets older and attackers become more creative and competent about hacking Wi-Fi. This is why the new WPA3 security protocol was created, with its new Wi-Fi security features.

На сьогоднішній день питання конфіденційності даних є одним із найважливіших в світі. Більшість цінної інформації містяться на телефонах і ноутбуках, які постійно підключенні до Wi-Fi. Тому питання захищеності бездротової системи є найпріорітетнішим на сьогодення [1,2]. Протокол захищеності WPA2 довгий час являвся найкращим в цьому плані, але з часом технологія старіє, а зловмисники стають більш креативними і компетентними в питанні взлому Wi-Fi. Саме для цього було створено новий протокол захисту WPA3, зі своїми новими засобами захисту Wi-Fi.

До 2017 року WPA2 вважався одним із найбільш безпечних протоколів. Але у 2017 році в протоколі WPA2 була виявлена серйозна вразливість, що отримала назву KRACK (**K** ey **R** einstallation **A** tta **ck**), яка дає можливість зловмиснику атакувати 4-х стороннє рукостискання протоколу WPA2, тобто ініціювання WPA2-з'єднання. Це рукостискання відбувається кожного разу, коли клієнт хоче приєднатися до захищеної Wi-Fi мережі WPA2, щоб підтвердити, що клієнт і точка доступу мають правильні облікові дані, тобто пароль Wi-Fi, перед тим, як клієнт приєднається до мережі. Під час того ж 4-х стороннього рукостискання встановлюється свіжий ключ шифрування, який використовується для шифрування подальшого трафіку. Маніпулюючи цим рукостисканням, зловмисник може обманути жертву перевстановши вже використаний ключ шифрування, тоді як ключ повинен бути встановлений і використаний лише один раз. Перевстановлення ключа шифрування змушує скинути два лічильника (відомі як "nonces"), використовувані протоколом шифрування, і це дозволяє атакувати на протокол, наприклад, повторення,

розшифрування або підробка пакетів. Потенційний зловмисник, який перебуває у фізичній близькості від захищеної мережі Wi-Fi і здійснює цю атаку, відому як "людина-в-середині".[3] Зловмисник може по суті перехоплювати та розшифровувати інтернет-трафік без володіння обліковими даними захищеної мережі Wi-Fi (тому зміна пароля Wi-Fi не допоможе). Ключова атака переустановки проілюстрована на спрощеному рис. 1.

Рис. 1. Ключова атака переустановки (KRACK).

Цей факт, поряд з усіма раніше відомими недоліками WPA2, підштовхнув Wi-Fi Alliance до розробки - WPA3. Вже в липні 2018 року Wi-Fi Alliance оповістив про початок сертифікації пристроїв, що підтримують WPA3 (Wi-Fi Protected Access 3) - найбільшого оновлення захисту за минулі 14 років. WPA3 став офіційним із запуском у червні програми сертифікації Wi-Fi Alliance для WPA3-Personal, що забезпечує більш індивідуальне шифрування, та WPA3-Enterprise, що збільшує криптографічну силу для мереж, що передають конфіденційну інформацію[4].

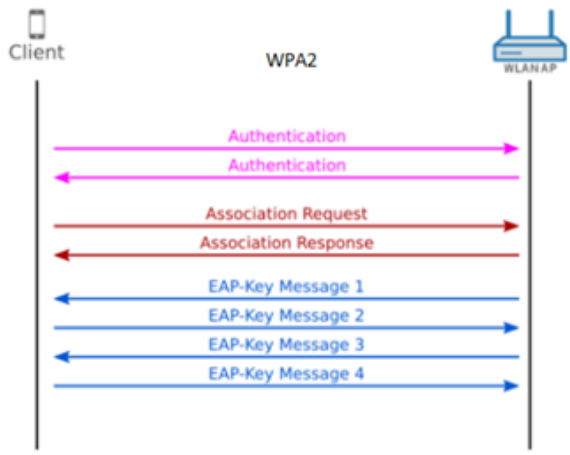

Рис. 2. Схема підключення WPA2.

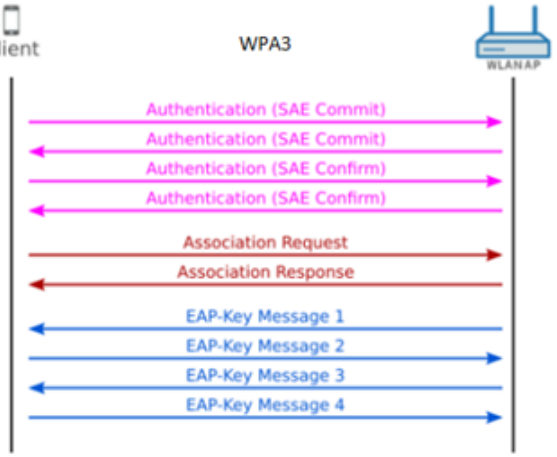

Рис. 3. Схема підключення WPA3.

У WPA2 завжди гострою проблемою залишалося використання слабких паролів. Якщо користувачі ставлять легкий пароль на бездротову мережу, то його запросто можна було підібрати через автоматизовані атаки з

використанням словників, таких як Dictionary і Brute-Force. WPA2 не мав варіантів для усунення такої проблеми. Якраз тому в WPA3 був вжитий новий механізм автентифікації SAE (Simultaneous Authentication of Equals), який замінює використовуваний в WPA2 метод PSK (Pre-Shared Key). SAE перекладається як "одночасна автентифікація рівних", і згідно з цим алгоритмом автентифікація пристроїв проводиться одночасно і на рівних правах. SAE надає допоміжне покращення безпеки, якого не було в PSK: пряму секретність [forward secrecy][5].

Рис. 4. Повідомлення автентифікації WPA3.

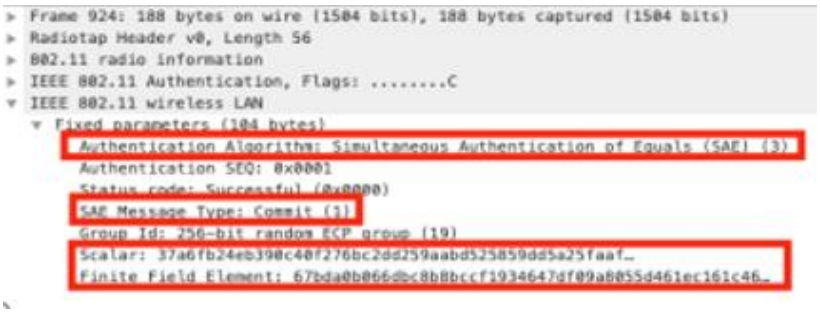

Рис. 5. Повідомлення SAE 1.

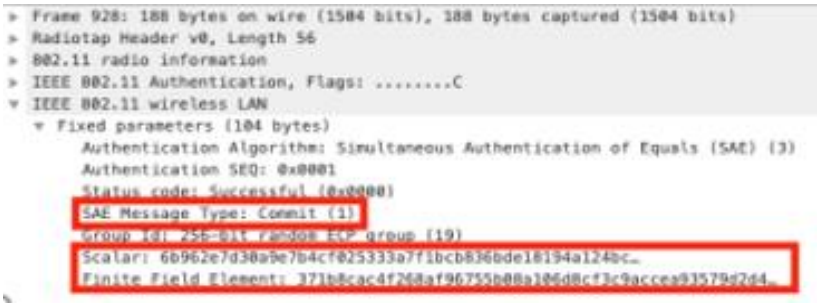

Рис. 6. Повідомлення SAE 2.

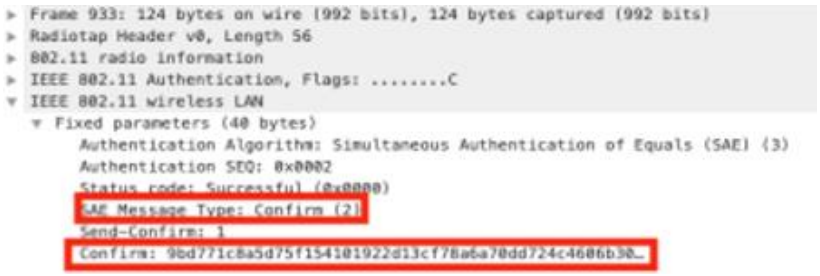

Рис. 7. Повідомлення SAE 3.

Повідомлення SAE 1 - Користувач надсилає повідомлення AP в AP з його ідентифікатором групи, скаляром та новою точкою на Еліптичній кривій (інформація про Кінцевий елемент поля).

Повідомлення SAE 2 - AP відправляє своє повідомлення "Здійснювати" на пристрій користувача зі своєю скалярною та ECC точкою.

Повідомлення SAE 3 - Користувач надсилає своє повідомлення підтвердження до AP з маркером підтвердження.

Повідомлення SAE 4 - AP відповідає своїм підтвердженням та маркером, і тепер асоціація може статися, якщо був встановлений захищений канал.

З використанням SAE при кожному новому з'єднанні встановлюється новий шифр пароля, тому

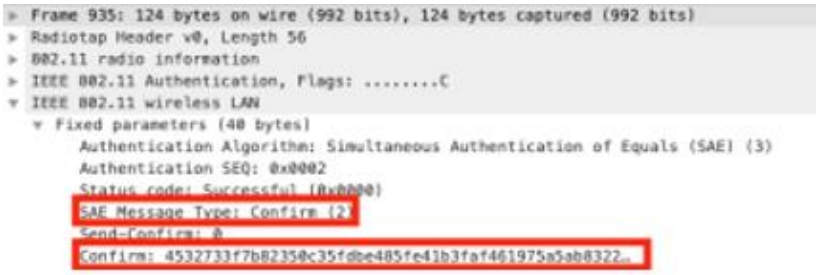

Рис. 8. Повідомлення SAE 4.

навіть якщо розбійник в якийсь момент і проникне в мережу, він зможе вкрасти тільки пароль від даних, переданих після цього моменту[6].

Виходячи з загального положення і спираючись на сукупність всіх вище перелічених фактів можна сказати, що на зміну, вже менш безпечного протоколу WPA2 приходить сучасний і більш ефективніший протокол WPA3, який має безліч переваг, таких як: більш безпечне рукостискання, заміна налаштувань на захист Wi-Fi (WPS), несанкціоноване шифрування і більші розміри ключів сеансу. Однак усі ці переваги WPA3 реалізуються лише тоді, коли всі пристрої будуть підтримувати цей протокол і розгортання цієї мережі почнеться лише тоді, коли на ринку з’явиться більше пристроїв кінцевих користувачів WPA3.

Література

1. Романов О.І., Осокін М.Г. Аналіз рівня безпеки сигналізації SS7. Матеріали 12-ої МНТК «Проблеми телекомунікацій», Київ, 2018 р. С 131-134.
2. Письменний І.С., Романов А.О. Мережа підприємства с програмним забезпеченням ASTERIISK PBX на основі PLC, Київ, 2018 р. С 119-122.
3. Огляд вразливості Wi-Fi WPA2 [Електронний ресурс] – Режим доступу до ресурсу: https://www.enisa.europa.eu/publications/info-notes/an-overview-of-the-wi-fi-wpa2-vulnerability
4. WPA2 vs. WPA3. [Електронний ресурс] – Режим доступу до ресурсу: https://www.diffen.com/difference/WPA2_vs_WPA3
5. WPA3 - Підвищення безпеки вашої WLAN [Електронний ресурс] – Режим доступу до ресурсу: https://wlan1nde.wordpress.com/2018/09/14/wpa3-improving-your-wlan-security/
6. Покращення безпеки Wi-Fi: WPA3-Perssonal(SAE) [Електронний ресурс] – Режим доступу до ресурсу: https://wificoops.com/2019/07/28/wi-fi-security-enhancements-part-1-wpa3-personal-sae/