УДК 621.396.42
DOI https://doi.org/10.32838/2663-5941/2021.3/13

Білевська О.С.
Український науково-дослідний інститут спеціальної техніки та судових експертиз
Служби безпеки України

АНАЛІЗ ВРАЗЛИВОСТЕЙ ПРОГРАМ СЕРТИФІКАЦІЇ WPA2 ТА WPA3 МЕРЕЖІ WI-FI

Більшість сучасних мереж Wi-Fi використовує програму сертифікації пристроїв бездротового зв'язку для захисту переданих даних WPA2 (Wi-Fi Protected Access). Проте, оскільки WPA2 понад 15 років, Wi-Fi Alliance (WECA) у 2018 р. анонсував новий і більш безпечний протокол WPA3. Wi-Fi Alliance – це неурядова організація, яка займається сертифікацією і випуском Wi-Fi-обладнання та є правовласником марки Wi-Fi. У склад альянсу входить 36 компаній, включаючи Apple, Microsoft, Qualcomm та ін.

Найбільш поширеним методом атаки на мережі Wi-Fi є перехоплення пакетів, які пов'язані з аутентифікацією клієнта (рукостискання – handshake) із подальшим перебором пароля за словником. На думку розробників, основна перевага WPA3 полягає у тому, що в її основі лежить аутентифікація клієнта Dragonfly, завдяки якій практично неможливо зламати пароль мережі. Проте якщо користувач не використовує додаткові методи захисту, такі як HTTPS (Hyper Text Transfer Protocol Secure), це дає змогу зловмиснику викрасти конфіденційну інформацію, таку як паролі, електронні листи та ін.

У разі використання вразливості зловмисник, що знаходиться в зоні дії мережі жертви, зможе відновити пароль Wi-Fi та проникнути в мережу цілі. Сьогодні бездротові мережі Wi-Fi знайшли своє застосування майже у всіх галузях завдяки високій мобільності користувачів, простоті використання мережі і простоті встановлення даної технології. Ця технологія стає обов'язковим складником не лише домашніх, а й корпоративних мереж. Рукостискання Dragonfly використовується в корпоративних мережах Wi-Fi, де для контролю доступу потрібні ім'я користувача та пароль.

Практично в будь-якому алгоритмі, для чого б він не був призначений, можна знайти слабкі місця. Оскільки протокол WPA3 знаходиться ще на відносно ранніх етапах упровадження, то є можливість більш детально його дослідити на предмет уразливостей.

Ключові слова: *Wi-Fi-мережа, аутентифікація, handshake, ідентифікатор, доступ, протокол, точка доступу, Key Reinstallation Attacks, Dragonfly, Dragonblood, Wi-Fi Protected Access.*

Постановка проблеми. Вади в налаштуваннях безпеки бездротових мереж або поява нелегальних точок доступу, які підключені до бездротової мережі, несуть велику загрозу несанкціонованого доступу до ресурсів корпоративної мережі.

Багато компаній змушені відмовитися від використання бездротових мереж виключно з міркувань безпеки та збереження конфіденційності інформації. Володіючи інформацією про вади протоколів безпеки бездротового зв'язку, Wi-Fi-зловмисники можуть приєднуватися до бездротової мережі і входити в дротову корпоративну мережу, як і офіційний її користувач, та отримувати доступ до внутрішніх ресурсів через мережу Інтернет.

Аналіз останніх досліджень і публікацій. Інформація про критичні проблеми програми сертифікації бездротового зв'язку WPA2 була розкрита у 2017 р. Ці вади дають змогу оминути захист і, як результат, прослуховувати трафік Wi-Fi, який курсує між точкою доступу і користувачем. Комплекс уразливостей у WPA2 отримав назву KRACK (Key Reinstallation Attacks). Він був виявлений зведеною групою дослідників із різних компаній і університетів. Керівник групи Меті Ванхоф повідомив про вразливості виробникам техніки та представникам організації US-CERT у липні 2017 р. Виробники обладнання випустили оновлення програмного забезпечення, які усувають цей комплекс уразливості, проте залишається ще достатньо велика кількість обладнання з не оновленим програмним забезпеченням.

Хоча протокол WPA3 покладається на більш безпечне рукостискання, відоме як Dragonfly, яке спрямоване на захист мереж Wi-Fi від автономних атак за словником, у квітні 2019 р. Меті Ванхоф та Еял Ронен знайшли п'ять вад нової програми сертифікації, які отримали назву Dragonblood, а в серпні 2019 р. було виявлено додаткові дві вразливості.

Водночас, незважаючи на значну кількість наукових публікацій, присвячених проблемам захищеності програм сертифікації Wi-Fi-мереж, стрімкий розвиток систем зв'язку та протоколів їх

захисту зумовлює потребу подальших досліджень цієї тематики.

Постановка завдання. Метою статті є огляд уразливостей найбільш поширених програм сертифікації WPA2 та WPA3, які дають змогу отримати паролі мереж Wi-Fi та, відповідно, нелегітимної активності з можливістю блокування несанкціонованих підключень до мережі або оповіщення сторонніх засобів фільтрації і блокування трафіку. Метою аналізу є своєчасне виявлення потенційних загроз і реагування на них, не надаючи негативного впливу на функціонування мережі зв'язку.

Виклад основного матеріалу дослідження. Першим протоколом безпеки Wi-Fi був WEP (Wired Equivalent Privacy), який забезпечував захист мережі, можна сказати, тими ж методами, що й захист у дротових мережах. Для перехоплення трафіку Wi-Fi-мережі з WEP потрібно перебувати в зоні прийому сигналу. Для шифрування трафіку WEP використовується ключовий потік, який отримується шляхом змішування пароля і вектора ініціалізації. Вектор ініціалізації в WEP – це постійно змінюване 24-бітове число. Зі зростанням обчислювальних потужностей персональних комп'ютерів довжина вектора ініціалізації стала недостатньою. Таким чином, незалежно від складності ключа розкрити будь-яку передачу стало можливо після статистичного аналізу достатньої кількості перехоплених пакетів.

Для вирішення проблеми Wi-Fi Alliance запропонував надбудову над WEP, яка давала змогу усунути уразливість без заміни обладнання. Основною ідеєю була зміна ключів. На базі IEEE 802.11 був розроблений стандарт WPA. Його основою став протокол цілісності тимчасових ключів TKIP (Temporal Key Integrity Protocol). Він значно посилював WEP за допомогою дворівневої системи векторів ініціалізації. Іншим нововведенням у WPA стала технологія WPS (Wi-Fi Protected Setup), яка дає змогу бездротовим пристроям спрощено отримати доступ до Wi-Fi за умови фізичного доступу до маршрутизатора.

У 2006 р. був створений та реалізований у багатьох бездротових пристроях протокол WPA2, який став обов'язковим для всіх сертифікованих простоїв. Кардинальною відмінністю WPA2 від WPA стало індивідуальне шифрування даних кожного користувача та більш надійний алгоритм шифрування – AES (Advanced Encryption Standart).

Довгий час основними методами зламу маршрутизаторів, які працювали по WPA2, були злам PIN-коду під час підключення через WPS або перехоплення рукостискання і підбір ключа методом підбору. Убезпечити себе можна було, відключивши WPS і встановивши досить складний пароль. Тому до недавнього часу WPA2 вважався надійним. У жовтні 2017 р. було опубліковано опис атаки KRACK (Key Reinstallation Attack), в основі якої лежить уразливість чотирьохелементного рукостискання WPA2. Проблема була знайдена у самому протоколі, а не в окремих пристроях, тому ця вразливість притаманна всім користувачам мережі Wi-Fi. Залежно від конфігурації мережі також існує можливість маніпулювання даними.

Рукостискання виконується тоді, коли клієнт хоче підключитися до захищеної мережі Wi-Fi. У процесі підтверджується, що обидва боки (клієнт і точка доступу) мають коректні облікові дані. Водночас рукостискання використовується для узгодження ключа шифрування, який згодом застосовуватиметься для захисту трафіку. Зловмисник може влаштувати атаку типу man in the middle (людина всередині) і примусити учасників мережі перевстановити ключі шифрування, які захищають трафік WPA2. Якщо мережа налаштована на використання WPA-TKIP або GCMP (Galois/Counter Mode Protocol), зловмисник зможе не лише прослуховувати трафік, а й уводити пакети в дані жертви.

Цей метод є універсальним і працює проти будь-яких пристроїв, які підключені до мережі та не захищені оновленим програмним забезпеченням. Головна умова цієї атаки полягає у тому, що зловмиснику необхідно перебувати в зоні дії мережі Wi-Fi, тобто атаку не можна проводити віддалено.

Заміна пароля не допоможе уникнути атаки. Для захисту необхідно оновити прошивки роутеров і всіх пристроїв. Також як додаткові заходи безпеки бажано використовувати VPN-мережі, але до їх вибору також варто підходити обережно, оскільки багато з них не можуть гарантувати безпечне підключення. Також для захисту від атаки KRACK у деяких випадках може захистити використання протоколу HTTPS. Сам протокол HTTPS не можна назвати абсолютно безпечним, проте він може бути додатковим елементом шифрування та захисту від атак, заснованих на прослуховуванні мережевого трафіку.

27 червня 2018 р. Wi-Fi Alliance оголосив про закінчення розроблення нового стандарту безпеки – WPA3. Під час розроблення WPA3 стояла необхідність усунути концептуальні недоробки, які були виявлені з появою KRACK. Оскільки ключова вразливість ховалася в чотирьохелементному

рукостисканні, у WPA3 додалася обов'язкова підтримка більш надійного методу з'єднання – SEA (Simultaneous Authentication of Equals), також відомого як Dragonfly. Технологія SEA вже застосовувалася в mesh-мережах і описана в стандарті IEEE 802.11s. Вона заснована на протоколі обміну ключами Діффі – Хеллмана з використанням кінцевих циклічних груп. SEA відноситься до протоколу типу PAKE (Password-authenticated key agreement) і надає інтерактивний метод, згідно з яким дві і більше сторін встановлюють криптографічні ключі, які засновані на знанні пароля однією або декількома сторонами. Результуючий ключ сесії, який отримує кожна зі сторін для аутентифікації з'єднання, вибирається на основі інформації з пароля, ключів і MAC-адрес обох сторін. Якщо ключ однією зі сторін виявиться зкомпрометованим, це не спричинить компрометації ключа сесії. Навіть дізнавшись пароль, зловмисник не зможе розшифрувати пакети. Ще одним нововведенням WPA3 є підтримка PMF (Protected Management Frames) для контролю цілісності трафіку. У WPA3 були розроблені, проте не потребують сертифікації, програми Wi-Fi Easy Connect і Wi-Fi Enhanced Open.

Wi-Fi Easy Connect дає змогу реалізувати спрощене налаштування пристроїв без екрану. Для цього можна використовувати інший пристрій, який уже підключений до бездротової мережі. Easy Connect заснований на застосуванні аутентифікації за відкритими ключами і може використовуватися в мережах з WPA2 і WPA3. Ще одна особливість Wi-Fi Easy Connect – це можливість заміни точки доступу без необхідності перенаглагоджування усіх пристроїв.

Wi-Fi Enhanced Open забезпечує шифрування всіх потоків даних між клієнтом і точкою доступу. Ця технологія дає змогу захистити приватність користувача в публічних мережах, де не потрібна аутентифікація. Для генерації ключів у таких мережах застосовується процес узгодження з'єднання, який реалізується розширенням OWE (Opportunistic Wireless Encryption).

Підтримка цих технологій не є обов'язковою для сертифікації по WPA3, проте виробник може за бажання сам додати їх підтримку в продукт.

Як і в WPA2, у WPA3 передбачено два режими роботи: WPA3-Personal і WPA3-Enterprise:

– WPA3-Personal забезпечує надійний захист, особливо якщо користувач задав стійкий пароль, який не можна отримати перебором за словником. Але якщо пароль не зовсім складний, то мають допомогти нове обмеження на число спроб аутентифікації в рамках одного рукостискання. Таке обмеження не дасть змоги підбирати пароль у режимі поза мережею. Замість ключа PSK (Pre-Shared Key) у WPA3 реалізована технологія SEA.

– WPA3-Enterprise забезпечує шифрування на основі мінімум 192-розрядних ключів. Для аутентифікованого шифрування рекомендовано застосування 256-розрядних ключів GCMP-256, для передачі і підтвердження ключів використовується HMAC із хешами SHA-384, для узгодження ключів і аутентифікації – ECDH і ECDSA із 384-розрядними еліптичними кривими, для захисту цілісності кадрів – протокол BIP-GMAC-256.

Уразливості протоколу Dragonfly отримали назву Dragonblood та налічують сім різних уразливостей. Перші п'ять були виявлені у квітні 2019 р. Їх можна розділити за принципом на три види, а саме: атака типу «відмова в обслуговуванні», дві атаки зі зниженням стандарту протоколу передачі даних та дві атаки з витоку інформації по каналу передачі службової інформації. У серпні 2019 р. було виявлено додаткові вразливості класу Dragonblood у стандарті WPA3. Подібно попереднім нові вразливості також дають змогу зловмиснику отримувати інформацію через криптографічні операції WPA3 і здійснювати перебор паролів за словником для авторизації в мережах Wi-Fi.

Атака типу «відмова в обслуговуванні» не так важлива, оскільки вона призводить тільки до збою WPA3 сумісних точок доступу, інші чотири можна використовувати для відновлення паролів користувача.

Дві атаки на зниження стандарту протоколу передачі даних, і дві атаки з витоку по службовим каналам використовують недоліки опублікованого проєкту обміну ключами Dragonfly стандарту WPA3 – механізму, за допомогою якого клієнти проходять аутентифікацію на маршрутизаторі WPA3 або точці доступу.

У разі атаки зі зниженням на більш ранні версії протоколу мережі з підтримкою Wi-Fi WPA3 можуть бути змушені використовувати більш старі і небезпечні системи обміну паролями, які дають змогу зловмисникам отримувати паролі мережі з використанням існуючих недоліків і уразливостей.

Під час атаки за типом витоку інформації під час використання службового каналу бездротової мережі з підтримкою Wi-Fi WPA3 зловмисник може «обдурити» пристрій, використовуючи більш слабкі алгоритми, які пропускають обмежені обсяги інформації про пароль мережі. За декількох ітерацій у підсумку може бути відновлений повний пароль.

Якщо клієнт і точка доступу підтримують WPA2 і WPA3, зловмисник може налаштувати підроблену точку доступу, яка буде обмежена проколом обміну даними WPA2. Це призводить до того, що клієнт підключається за допомогою чотирьохелементного рукостискання WPA2. Даних, отриманих у процесі обміну рукостисканнями до моменту зниження протоколу з WPA3 до WPA2, достатньо для запуску атаки за словником в автономному режимі.

Розглянемо атаку по бічному каналу на основі кеша. Алгоритм кодування пароля в Dragonfly, також відомий як алгоритм «полювання та клювання» (hunting and pecking), містить умовні гілки. Якщо зловмисник може визначити, яка гілка з гілки if-then-else була взята, він може дізнатися, чи був знайдений елемент пароля в конкретній ітерації цього алгоритму. На практиці було виявлено, якщо зловмисник може запустити непріоритетний код на комп'ютері-жертві, то може використовувати атаки на основі кеша, щоб визначити, яка гілка була зроблена в першій ітерації алгоритму генерації пароля. Ця інформація може бути використана для виконання атаки з поділом пароля (це схоже на автономну атаку за словником).

Ця уразливість відстежується з використанням ідентифікатора CVE-2019-9494. Захист полягає у заміні умовних гілок, які залежать від секретних значень та утилітами вибору з постійним часом. Реалізації повинні також використовувати обчислення символу Лежандра з постійним часом.

У разі атаки по бічному каналу на основі синхронізації, коли рукостискання Dragonfly використовує певні мультиплікативні групи, алгоритм кодування пароля використовує змінне число ітерацій для кодування пароля. Точна кількість ітерацій залежить від пароля, який використовується, і MAC-адреси точки доступу і клієнта. Зловмисник може виконати віддалену тимчасову атаку на алгоритм кодування пароля, щоб визначити, скільки ітерацій знадобилося для кодування пароля. Відновлена інформація може бути використана для виконання парольної атаки, яка також схожа на автономну атаку за словником. Ця уразливість теж відстежується з використанням ідентифікатора CVE-2019-9494 завдяки схожості реалізації атаки.

Під час використання еліптичної кривої Brainpool за кодування пароля алгоритмом Dragonfly виконується кілька попередніх ітерацій із паролем, пов'язаних зі швидким вирахуванням короткого хеша до початку застосування еліптичної кривої. Знаходження короткого хеша операції, яка виконуються, безпосередньо залежить від пароля і MAC-адреси клієнта. Час виконання (корелюється з числом ітерацій) і затримки між операціями під час виконання попередніх ітерацій може бути виміряний і використаний для визначення характеристик пароля, який можна використовувати в offline для уточнення правильності вибору частин пароля в процесі його підбору. Для проведення атаки необхідна наявність доступу до системи користувача, який приєднується до бездротової мережі. Додатково виявлена друга уразливість (CVE-2019-13456), яка пов'язана з витоком інформації в реалізації протоколу EAP-pwd та використовує алгоритм Dragonfly. Проблема специфічна для RADIUS-сервера FreeRADIUS і на підставі витоку відомостей по сторонніх каналах, як і перша уразливість, дає змогу істотно спростити підбір пароля.

У поєднанні з поліпшеним методом відсіювання шумів у процесі вимірювання затримок для визначення числа ітерацій досить провести 75 вимірювань для однієї MAC-адреси. Методи по підвищенню безпеки протоколів дають змогу блокувати виявлені проблеми, які вже внесені в чорнові варіанти майбутніх стандартів Wi-Fi WPA 3.1 і EAP-pwd. На жаль, без порушення зворотної сумісності в поточних версіях протоколів усунути витоку по сторонніх каналах не вийде.

Внутрішній протокол EAP-pwd також використовує Dragonfly і забезпечує аутентифікацію на основі імені користувача і пароля у визначених корпоративних мережах Wi-Fi. Він уразливий для тих самих атак, які виявлені проти WPA3.

Відправляючи спеціально створені точки еліптичної кривої, зловмисник може повністю обійти аутентифікацію. Це можна використовувати проти сервера для підключення до будь-якої мережі Wi-Fi, яка підтримує EAP-pwd.

Висновки. Після публічного розкриття дослідниками Меті Ванхофа та Еяла Ронена недоліків Dragonblood, Wi-Fi Alliance оголосив про оновлення специфікацій безпеки для стандарту WPA3. Усі проблеми можна вирішити за допомогою оновлень програмного забезпечення, не впливаючи на здатність пристроїв працювати спільно. Постачальникам продуктів Wi-Fi необхідно інтегрувати зміни у свої продукти за допомогою оновлень програмного забезпечення.

Оскільки 15-річний протокол WPA2 широко використовувався мільярдами пристроїв, широке поширення WPA3 не може здійснитися водночас. Для підтримки старих пристроїв сертифіковані WPA3-пристрої пропонують «перехідний режим роботи», який можна налаштувати для прийому з'єднань із використанням як WPA3-SAE, так і WPA2.

Список літератури:

1. Mathy Vanhoef, Key Reinstallion Attacks. Breaking WPA2 by forcing nonce reuse. URL: http://www.krackattacks.com.
2. Mathy Vanhoef, Eyal Ronen, Dragonblood. Analysing WPA3's Dragonfly Handshake of WPA3 and EAP-pwd. URL: http://wpa3.mathyvanhoef.com.
3. Stewart S. Miller, Wi-Fi Security –McGraw-Hill Networking Professional Publishing, 2003, 309 p.

Bilevska O.S. ANALYSIS OF PROTECTION OF CERTIFICATION PROGRAMS WPA2 AND WPA3 WI-FI NETWORK

Most modern Wi-Fi networks use the Wi-Fi Protected Access (WPA2) wireless certification program. However, since WPA2 is over 15 years old, the Wi-Fi Alliance (WECA) announced a new and more secure WPA3 protocol in 2018. The Wi-Fi Alliance is a non-governmental organization that certifies and releases Wi-Fi equipment, and is the copyright holder of the Wi-Fi brand. The alliance includes 36 companies, including Apple, Microsoft, Qualcomm and others.

The most common method of attacking Wi-Fi networks is packet interception, which is associated with client authentication (handshake) followed by a dictionary search for a password. According to the developers, the main advantage of WPA3 is that it is based on Dragonfly client authentication, thanks to which it is almost impossible to crack the network password. However, if the user does not use additional security methods, such as HTTPS (Hyper Text Transfer Protocol Secure), this allows an attacker to steal confidential information such as passwords, emails, and so on.

In case of exploitation of vulnerabilities, an attacker who is in the zone of the victim's network can recover the Wi-Fi password and penetrate the target's network. Today, Wi-Fi wireless networks have found their application in almost all industries due to the high mobility of users, the ease of use of the network, and the ease of installation of this technology. This technology is becoming an indispensable component of not only home, but also corporate networks. The Dragonfly handshake is used on corporate Wi-Fi networks where a username and password are required for access control.

Weaknesses can be found in almost any algorithm, whatever it is intended for. Since the WPA3 protocol is still at a relatively early stage of implementation, it is possible to investigate it in more detail for vulnerabilities.

Key words: *Wi-Fi network, authentication, handshake, identifier, access, protocol, access point, Key Reinstallation Attacks, Dragonfly, Dragonblood, Wi-Fi Protected Access.*