УДК 621.396.42
DOI https://doi.org/10.32838/2663-5941/2021.2-1/16

Гарист А.В.
Український науково-дослідний інститут спеціальної техніки та судових експертиз
Служби безпеки України

АНАЛІЗ ЗАХИЩЕНОСТІ WI-FI МЕРЕЖ

Використання бездротових технологій надає користувачам можливість вільного пересування без втрати зв'язку, операторам мережі – більше можливостей для організації з'єднань і доступ у мережу безлічі нових пристроїв. Сьогодні бездротові Wi-Fi мережі використовуються майже всюди завдяки простоті використання мережі, високій мобільності користувачів і простоті встановлення цієї технології. Ця технологія дедалі частіше стає обов'язковим складником не тільки домашніх, але й корпоративних мереж.

Аналіз захищеності – це процес перевірки інфраструктури організації на наявність можливих вразливостей мережевого периметра, віртуальної інфраструктури, які спричинені помилками конфігурації, програмного забезпечення й вихідного коду додатків. Інакше кажучи, під час аналізу захищеності перевіряється безпека різних інформаційних систем – як внутрішніх, так і зовнішніх.

Стандарт Wi-Fi розроблено на основі IEEE 802.11 (Institute of Electrical and Electronics Engineers) та використовується для широкосмугових бездротових мереж зв'язку. Від самого початку технологія Wi-Fi була орієнтована на організацію точок швидкого доступу в Інтернет (hotspot) для мобільних користувачів. Переваги бездротового доступу очевидні, а технологія Wi-Fi від самого початку стала стандартом, якого дотримуються виробники мобільних пристроїв. Поступово мережі Wi-Fi стали використовувати малі й великі офіси для організації внутрішніх мереж і підмереж, а оператори – створювати власну інфраструктуру надання бездротового доступу в мережу Інтернет на основі технології Wi-Fi.

Переваги, які бездротові мережі Wi-Fi дають людям, величезні, проте такі мережі несуть із собою й додаткові загрози інформаційної безпеки в разі неправильного їх використання. З погляду безпеки треба враховувати не тільки загрози, які властиві дротовим мережам, але й середовище поширення сигналу. У бездротових мережах отримати доступ до інформації набагато простіше, ніж у дротових мережах, а також вплинути на канал передачі даних.

Ключові слова: *Wi-Fi мережа, аутентифікація, хендшейк, ідентифікатор, доступ, радіоканал, протокол, адміністратор, трафік, шифрування, сканування, клієнт, точка доступу, хендшейк, Key Reinstallation Attacks.*

Постановка проблеми. Загроза несанкціонованого доступу до ресурсів корпоративної мережі передачі даних пов'язана з вадами в налаштуваннях безпеки бездротової мережі або появою нелегальної точки доступу до бездротової мережі, яка під'єднана до неї. Зловмисники можуть приєднуватися до бездротової мережі та входити в дротову корпоративну мережу, як і офіційний її користувач, та отримувати доступ до внутрішніх ресурсів через мережу Інтернет. З огляду на це багато компаній були змушені відмовитися від використання бездротових мереж суто з міркувань збереження конфіденційності інформації. Під час побудови мережі бездротового зв'язку, основаної на технології Wi-Fi, напрацьовано різні варіанти побудови стійких до зламу систем.

Аналіз останніх досліджень і публікацій. У 2017 році було розкрито інформацію про критичні проблеми програми сертифікації бездротового зав'язку WPA2, які дають можливість обійти захист і, як наслідок, прослуховувати трафік Wi-Fi, який курсує між точкою доступу і користувачем. Комплекс вразливостей у WPA2, який отримав назву KRACK (Key Reinstallation Attacks), було виявлено зведеною групою дослідників із різних університетів і компаній. Керівник групи Меті Ванхоф розповів, що йому вдалося знайти проблеми, з яких формується KRACK, ще в 2016 році, проте більш ніж рік він удосконалював свою атаку. Дослідник повідомив про вразливості виробникам і представникам організації US-CERT в липні 2017 року. Виробники обладнання випустили оновлення прошивок, які усувають вразливості, проте залишається велика кількість неоновленого обладнання.

У 2019 році Меті Ванхоф та Еял Ронен знайшли п'ять вад нового стандарту Dragonblood, який є основним механізмом обміну ключами для

аутентифікації користувачів маршрутизатором або точкою доступу з підтримкою програми сертифікації бездротового зав'язку WPA3.

Водночас, незважаючи на значну кількість наукових публікацій, присвячених проблемам захищеності Wi-Fi мережі, стрімкий розвиток систем зв'язку та протоколів їхнього захисту зумовлює потребу подальших досліджень цієї тематики.

Постановка завдання. Метою статті є аналіз захищеності Wi-Fi мереж і виявлення нелегітимної активності з можливістю блокування несанкціонованих під'єднань до мережі або оповіщення сторонніх засобів фільтрації та 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. Розгляньмо актуальні загрози інформації, яка циркулює в бездротовій мережі:

– перехоплення й порушення цілісності конфіденційної інформації, яка передається бездротовими мережами. Зловмисник, який перебуває в зоні дії точок доступу, може перехоплювати радіосигнал, розшифровувати й ретранслювати дані, водночас залишаючись майже непоміченим. Використання антен і підсилювачів дає змогу зловмисникові перебувати на значному віддаленні від цілі в процесі перехоплення;

– порушення доступності інформації, яка циркулює в бездротових мережах. Інформація може бути обмежена як перешкодами в каналі зв'язку, так і атаками зловмисників, які спрямовані на вузли бездротової мережі.

Є також і загрози інформації, яка зберігається на вузлах абонентів бездротової мережі:

– ідентифікаційні дані абонентів бездротової мережі можуть бути як перехоплені під час пересилання по бездротовій мережі, так і отримані зловмисником під час отримання доступу до мобільного станції. Ці дані можуть бути використані для під'єднання до бездротової мережі від імені легального користувача;

– несанкціонований доступ до інформації, що зберігається локально на вузлах мережі, може бути отримано завдяки неправильним налаштуванням безпеки абонента бездротової мережі.

Радіоканал передачі даних, який використовується у Wi-Fi мережах, потенційно схильний до втручання з метою порушення конфіденційності, цілісності й доступності інформації. Під час під'єднання до мережі передбачено аутентифікацію та шифрування, але ці елементи захисту мають свої вади.

Шифрування значно знижує швидкість передачі даних, і найчастіше воно усвідомлено вимикається адміністратором для оптимізації трафіку. Початковий стандарт шифрування WEP (Wired Equivalent Privacy) був дискредитований через вразливості в алгоритмі розподілу ключів RC4 (Rivest Cipher 4). У 2003 році створено стандарт WPA (Wi-Fi Protected Access). Стандарт WPA використовує протокол цілісності тимчасових ключів TKIP (Temporal Key Integrity Protocol). Також у ньому використовується метод контрольної суми MIC (Message Integrity Code), який дає змогу перевіряти цілісність пакетів. У 2004 році створено стандарт WPA2, який являє собою поліпшений WPA. Основна відмінність між WPA і WPA2 полягає в технології шифрування, який поєднує симетричний алгоритм блочного шифрування AES (Advanced Encryption Standart) та TKIP. WPA2 забезпечує більш високий рівень захисту мережі, оскільки TKIP дає змогу створювати ключі завдовжки до 128 біт, а AES – до 256 бітів.

Більшість атак починається з розвідки, під час якої виконуються сканування мережі, збір і аналіз пакетів. Багато службових пакетів у мережі Wi-Fi передається у відкритому вигляді. Водночас украй проблематично з'ясувати, хто легальний користувач, який намагається під'єднатися до мережі, а хто збирає інформацію. Після розвідки ухвалюються рішення про подальші кроки можливої атаки.

Захист мережі за допомогою від'єднання відповіді на широкомовний запит ідентифікатора бездротової мережі ESSID (Extended Service Set Identification) і приховування назви мережі в службових пакетах Beacon frame є недостатнім, оскільки мережу все одно видно на певному радіоканалі та зловмисник чекає авторизованого під'єднання до мережі, адже водночас у незашифрованому вигляді передається ESSID. На цьому захисний захід втрачає сенс. Деякі системи безперервно розсилають ім'я мережі в ефір, намагаючись під'єднатися. Це також є цікавою атакою, оскільки в такому випадку можна «пересадити» користувача на свою точку доступу й отримувати всю інформацію, яку він передає по мережі.

Можна зменшити схильність розвідці, розмістивши точку доступу так, щоб вона забезпечувала необхідне покриття й це покриття мінімально виходило за контрольовану територію. Потрібно регулювати потужність точки доступу й використовувати спеціальні інструменти для контролю

поширення сигналу. Також можна повністю екранувати приміщення з точкою доступу для повної невидимості мережі ззовні.

Насамперед атакам піддаються некоректно сконфігуровані пристрої, пристрої зі слабкими й не досить довгими ключами шифрування, а також пристрої, які використовують вразливі методи аутентифікації. Велика частина успішних зламів відбувається завдяки неправильним налаштуванням точок доступу та програмного забезпечення.

Найбільш поширеними є два технічних сценарії атак на мережі Wi-Fi – це перехоплення пакетів, які пов'язані з аутентифікацією клієнта (рукостискання – handshake) з подальшим перебором пароля за словником, і створення підробленої точки доступу з паралельним проведенням атаки «відмови в обслуговуванні» на справжню точку доступу.

Для шифрування переданих даних у мережі Wi-Fi переважно використовується алгоритм WPA2 з від'єднаною технологією WPS. Нині алгоритм WPA2 є найбільш поширеним алгоритмом захисту бездротових мереж.

Найбільш поширена атака на мережу Wi-Fi, захищену протоколами WPA-PSK або WPA2-PSK, – це атака за словником. Протокол захисту WPA-PSK або WPA2-PSK використовує ключ попередньої сесії (PTK – Pairwise Transient Key), який, відповідно, складається з попереднього загального ключа (PSK – Pre-Shared Key) та п'яти інших параметрів, таких як SSID (символьна назва бездротової точки доступу Wi-Fi), Authenticator Nounce (ANounce), Supplicant Nounce (SNounce), Authenticator MAC-address (MAC-адреса точки доступу) та Suppliant MAC-address (MAC-адреса wifi-клієнта). Цей ключ надалі використовує шифрування між точкою доступу та клієнтом. Зловмисник, який прослуховує ефір, може перехопити всі п'ять параметрів, окрім PSK. PSK отримується завдяки використанню парольної фрази WPA-PSK, яку відправляє користувач разом із SSID. Комбінація цих двох параметрів пересилається за стандартом формування ключа на основі пароля PBKDF2 (Password Based Key Derivation Function), який генерує 256-бітовий загальний ключ. У звичайній WPA-PSK/WPA2-PSK атаці за словником зловмисник може використовувати програмне забезпечення, яке виводить 256-бітний PSK для кожної парольної фрази й використовувати її з іншими параметрами, які було описано під час створення PTK. PTK буде використовуватися для перевірки контрольної суми (MIC – Message Integrity Check) в одному з пакетів handshake. Якщо вони збігатимуться, то парольна фраза в словнику буде правильною. Водночас використовуються вразливості протоколу аутентифікації користувачів – відкрито передачу ANounce, SNounce, MAC-адреси точки доступу і MAC-адреси WiFi-клієнта. Якщо під час відтворення алгоритму аутентифікації відбудеться успішна авторизація користувача, значить обраний зі словника пароль є істинним й атака призвела до успішного злому мережі.

Розгляньмо атаку KRACK, в основі якої лежить вразливість чотирьохелементного хендшейка WPA2. Хендшейк виконується тоді, коли клієнт хоче під'єднатися до захищеної мережі Wi-Fi. У процесі під'єднання підтверджується, що обидва боки (клієнт і точка доступу) мають коректні облікові дані. Одночасно хендшейк використовується для узгодження свіжого ключа шифрування, який буде застосовуватися для захисту трафіку.

Зловмисник може влаштувати атаку типу «людина в середині» (man in the middle) та змусити учасників мережі перевстановити ключі шифрування, які захищають трафік WPA2. До того ж, якщо мережа налаштована на використання WPA-TKIP або GCMP, зловмисник зможе не тільки прослуховувати трафік WPA2, але й змінювати зміст пакетів даних жертви. Під час використання цієї помилки можна здійснювати розкодування трафіку, перехоплювати TCP-з'єднання і багато іншого. Головна умова полягає в тому, що зловмиснику доведеться перебувати в зоні дії мережі Wi-Fi, яка піддається атаці, тобто атаку не можна проводити віддалено.

Також можна відокремити так звані DoS-атаки, які спрямовані на порушення якості функціонування мережі або абсолютне припинення доступу користувачів. У випадку мережі Wi-Fi відстежити джерело, яке перевантажує систему «сміттєвими» пакетами, украй складно – його місце розташування обмежується лише зоною покриття. До тому ж є апаратний варіант цієї атаки – це встановлення досить сильного джерела перешкод у потрібному частотному діапазоні.

У 2018 році створено новий стандарт безпеки – WPA3. Творці WPA3 спробували усунути концептуальні недоробки, які випливли з появою атаки KRACK. Оскільки ключова вразливість ховалася в чотирьохелементному рукостисканні, у стандарт WPA3 додалася обов'язкова підтримка більш надійного методу з'єднання – SEA (Simultaneous Authentication of Equals), також відомого як Dragonfly. Технологія SEA основана на протоколі обміну ключами Діффі–Геллмана

з використанням кінцевих циклічних груп. SEA надає інтерактивний метод, відповідно до якого дві й більше сторін встановлюють криптографічні ключі, що 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 однієї зі сторін виявиться скомпрометованим, це не спричинить компрометації ключа сесії. І навіть дізнавшись пароль, атакуючий не зможе розшифрувати пакети.

Ще одним нововведенням WPA3 є підтримка захисту керівних пакетів PMF (Protected Management Frames) для контролю цілісності трафіку.

Стандарт WPA3 передбачає два режими роботи: WPA3-Personal і WPA3-Enterprise. WPA3-Personal забезпечує надійний захист, особливо якщо користувач задав стійкий пароль, який не можна отримати словниковим перебором. Але якщо пароль не зовсім тривіальний, то має допомогти нове обмеження на кількість спроб аутентифікації в межах одного рукостискання. WPA3-Enterprise забезпечує шифрування на основі 192-розрядних ключів.

Нині стандарт IEEE 802.11 також дає можливість під'єднання до мережі Wi-Fi за допомогою протоколу захисту OWE (Opportunistic Wireless Encryption). Протокол OWE забезпечує безпеку даних, які передаються по незахищеній мережі, шляхом їх шифрування. Водночас від користувачів не потрібно будь-яких додаткових дій і введення паролів для під'єднання до мережі. Атаки, які відбуваються у відкритій мережі, належать до пасивних. Коли до мережі під'єднується багато клієнтів, зловмисник може зібрати дуже багато даних, просто фільтруючи інформацію, яка проходить через нього. Протокол OWE використовує опортуністичне шифрування, щоб захищатися від пасивного підслуховування. Воно також запобігає атаці з внесенням пакетів, коли зловмисник намагається порушити роботу мережі, створюючи й передаючи особливі пакети даних, що видаються частиною нормальної роботи мережі.

Проте, незважаючи на переваги та усунуті вади, протокол WPA3 має і два типи вад, яких припустилися під час проєктування. Перший призводить до атак зі зниженням рейтингу, а другий – до витоків бічного кеша. Алгоритм кодування пароля в Dragonfly містить умовні гілки. Якщо зловмисник може визначити, яку гілку ланцюга «if-then-else» було вилучено, він може дізнатися, чи було знайдено елемент пароля в конкретній ітерації цього алгоритму. В основі атаки по бічному каналу на основі синхронізації лежить атака на метод рукостискання Dragonfly. Цей метод використовує певні мультиплікативні групи, алгоритм кодування пароля використовує змінну кількість 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, щоби визначити, скільки ітерацій знадобилося для кодування пароля. Відновлена інформація може бути використана для виконання парольної атаки, яка схожа на автономну атаку за словником.

Незважаючи на розглянуті методи атаки на бездротову мережу, необхідно не забувати й про виток інформації з провідної мережі. Зазвичай бездротові мережі з'єднуються з дротовими. Значить через точку доступу можна атакувати дротову мережу. Якщо є в наявності помилки в налаштуваннях як провідної, так і бездротової мережі, то відкривається багато можливостей для атак. Наприклад, точки доступу, які працюють у режимі моста (Layer 2 Bridge), під'єднані в мережу без маршрутизаторів або з порушенням сегментації й передають у радіоефір широкомовні пакети з дротової частини мережі (ARP-запити, DHCP, кадри STP і д.р.).

Висновки. Отже, можна виділити основні рекомендації із забезпечення безпеки бездротових Wi-Fi мереж:

– для забезпечення безпеки даних, які передаються по бездротовій мережі, необхідно використовувати шифрування WPA2/WPA3 зі стійким паролем;

– не під'єднуватися до відкритих Wi-Fi мереж. Ці мережі можуть прослуховуватися або навіть повністю контролюватися зловмисниками. За нагальної потреби під'єднання до такої мережі необхідно використовувати VPN-з'єднання.

З огляду на вищевикладене для захисту Wi-Fi мереж потрібно впроваджувати комплексний підхід до забезпечення інформаційної безпеки. Необхідно приділяти увагу підвищенню обізнаності співробітників у питаннях інформаційної безпеки та перекривати потенційні вектори атак на мережу. Впроваджувати безпечні методи аутентифікації з перевіркою сертифікатів, обмежувати доступ клієнтів гостьової мережі до локальної обчислювальної мережі, проводити регулярний аналіз захищеності бездротових мереж, виявляти й від'єднувати несанкціоновані точки доступу.

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. URL: http://wpa3.mathyvanhoef.com.
3. Stewart S. Miller, Wi-Fi Security –McGraw-Hill Networking Professional Publishing, 2003, 309 p.

Haryst A.V. WI-FI NETWORK SECURITY ANALYSIS

The use of wireless technologies allows users to move freely without losing communications, and network operators have more opportunities to establish connections, and create many new devices to access the network. Today, wireless Wi-Fi networks are used almost everywhere due to the ease of use, high user mobility and ease of installation of this technology. This technology is increasingly becoming a mandatory component of not only home, but also corporate networks.

Security analysis is the process of checking an organization's infrastructure for possible vulnerabilities in the network perimeter, virtual infrastructure, caused by configuration errors, as well as software and application source code. In other words, the security analysis checks the security of various information systems, both internal and external.

The Wi-Fi standard is developed based on IEEE 802.11 (Institute of Electrical and Electronics Engineers) and is used for broadband wireless communication networks. Initially, Wi-Fi technology was focused on organizing hotspots for mobile users. The superiority of wireless access is clear, and Wi-Fi technology has become the standard followed by mobile device manufacturers. Gradually, small and large offices began to use Wi-Fi networks to organize internal networks and subnets, and operators to create their own infrastructure for providing wireless Internet access based on Wi-Fi technology.

The advantages that Wi-Fi wireless networks bring to people are enormous, but such networks also pose additional threats to information security if they are misused. From a security point of view, it is necessary to consider not only the threats that are inherent in wired networks, but also the middle of the signal transmission. It is much easier to access information in wireless networks than in wired networks, and also to influence the data transmission channel.

Key words: *Wi-Fi network, authentication, handshake, identifier, access, radio channel, protocol, administrator, traffic, encryption, scanning, client, access point, handshake, Key Reinstallation Attacks.*