УДК 621.391.18
Д.А. Мирошніков, В.С. Димов
Херсонський національний технічний університет
E-mail: denverys@gmail.com, vdymov@rambler.ru

ДОСЛІДЖЕННЯ МЕТОДІВ ПІДВИЩЕННЯ РІВНЯ ЗАХИЩЕНОСТІ БЕЗДРОТОВИХ МЕРЕЖ

Проведено аналіз наявних методів і способів захисту точок бездротового доступу які відносяться до стандарту IEEE 802.11 (Wi-Fi). Було оглянуто вразливості які в них присутні. Розглянуто сучасні методи атак на бездротові точки доступу та перехоплення даних в них. Розроблено вимоги до налаштувань бездротових мереж стандарту IEEE 802.11 які потрібні для створення комплекса протидії зловмисникам. В даний час існують різні способи захисту Wi Fi мереж які були розглянуті в даній статті і опираючись на які було розроблено сучасний та актуальний комплекс наявних методів для забезпечення максимального захисту бездротових точок доступу Wi-Fi.
Ключові слова: бездротові мережі, безпека Wi-Fi мереж, стандарт IEEE 802.11.

D. Myroshnikov, V. Dymov. Research of methods of increasing the level of security of wireless networks. The analysis of available methods for protecting wireless access points related to the IEEE 802.11 (Wi-Fi) standard is carried out. The vulnerabilities that were present in them were examined. Modern methods of attacks on wireless access points and interception of data in them are considered. Requirements for setting up IEEE 802.11 wireless networks are required to create a countermeasures complex. Currently, there are various ways to protect Wi Fi networks that were discussed in this article and based on which up-to-date set of available methods has been developed to provide maximum protection for wireless Wi-Fi access points.
Keywords: wireless networks, Wi-Fi network security, IEEE 802.11 standard.

Д.А.Мирошников, В.С.Дымов. Исследование методов повышения уровня защищенности беспроводных сетей. Проведен анализ существующих методов и способов защиты точек беспроводного доступа относящихся к стандарту IEEE 802.11 (Wi-Fi). Были рассмотрены уязвимости которые в них присутствуют. Рассмотрены современные методы атак на беспроводные точки доступа и перехвата данных в них. Разработаны требования к настройкам беспроводных сетей стандарта IEEE 802.11 необходимые для создания комплекса противодействия злоумышленникам. В настоящее время существуют различные способы защиты Wi Fi сетей которые были рассмотрены в данной статье и опираясь на которые был разработан современный и актуальный комплекс имеющихся методов для обеспечения максимальной защиты беспроводных точек доступа Wi-Fi.
Ключевые слова: беспроводные сети, безопасность Wi-Fi сетей, стандарт IEEE 802.11.

Вступ. Як правило, процедура розгортання бездротової мережі має на увазі ряд заходів, спрямованих на забезпечення безпеки підсумкової інфраструктури. Однак складність полягає в тому, що лише іноді мається на увазі дійсно впровадження продуманої політики безпеки, часто, на жаль, для цього не робиться взагалі нічого. На даний момент сімейство стандартів 802.11 активно використовується, публічні бездротові мережі функціонують у безлічі місць, починаючи від ресторанів і закінчуючи залами очікування аеропортів і готелями. Широкий вибір різних пристроїв підтримують стандарт 802.11.

Проблема безпеки мереж Wi-Fi з початку момента їх появи являється однією з найскладніших. Безпека Wi-Fi мережі – це два основних питання: конфіденційність даних інформації, а також захист від несанкціонованого доступу. Стовідсотково вирішити дані проблеми неможливо, але розробники мережевого обладнання та розробники програмного забезпечення приділяють велику увагу цій проблемі. На даний момент є достатньо необхідних технічних засобів які призначені для того щоб запобігти злому або ускладнити злом бездротових точок доступу. Більшість бездротових мереж в яких встановлено стандартні параметри захисту мають достатній ризик бути зламаними. Крім того, проникнути в бездротову Wi-Fi мережу значно простіше, ніж в звичайну, немає необхідності підключатися до проводів, достатньо знаходитись в зоні прийому сигналу. Небезпечно підключати незахищену бездротову мережу до кабельної мережі.

Незахищена точка доступу, під'єднана до локальної мережі, являє собою можливість злому для зловмисників. Для підприємств це загрожує тим, що конкуренти можуть отримати доступ до конфіденційних документів. Незахищені бездротові мережі дозволяють хакерам обійти міжмережеві екрани і налаштування безпеки, які захищають мережу від атак через мережу Internet. Хоча для забезпечення безпеки Wi-Fi-мереж можуть застосовуватись складні математично алгоритмічні аутентифікаційні моделі шифрування даних і контролю цілісності їх при передачі, але тим не менш, вирогідність доступу до інформації сторонніх осіб є дуже великою. У випадку якщо для мережі не приділити певної уваги зловмисник зможе: отримати доступ до ресурсів і дисків користувачів Wi-Fi-мережі, сканувати трафік, мати доступ до конфіденційної інформації, змінювати в мережі інформацію, використати інтернет-трафік, атакувати комп'ютери користувачів і сервери мережі, створювати підроблені точки доступу, розсилати спам або здійснювати інші протиправні дії від імені мережі яка зламана.

Поширеність бездротових мереж і доступність обладнання для їх організації породжує проблему їх безпеки. Дійсно, у багатьох пристроях доступу використовуються SSID і інші налаштування за замовчуванням: не вибраний оптимальний метод ідентифікації користувачів і існує ще маса можливостей для несанкціонованого доступу до даних, що передаються. Для забезпечення безпеки бездротових мереж, перш за все необхідно встановити, що може їм загрожувати. Перехоплення сигналів бездротової мережі аналогічне прослуховуванні радіопередач. Досить мати ноутбук або смартфон і аналізатор бездротових протоколів. Широко поширена помилка, що несанкціоноване підключення до бездротової мережі поза офісом можна припинити, контролюючи вихідну потужність сигналу. Це не так, оскільки використання зловмисником бездротової карти підвищеної чутливості і спрямованої антени дозволяє легко це подолати. Навіть зменшивши вирогідність несанкціонованого підключення до мережі, не слід залишати без уваги можливість сканування трафіку, тому для безпечної роботи в бездротових мережах необхідно шифрувати передану інформацію.

Загальним завданням даної статті являється пошук та дослідження методів підвищення рівня захищеності бездротових мереж. На даний момент у звичайних користувачів та системних адміністраторів бездротових мереж є всі потрібні засоби для гарантовано надійного захисту Wi-Fi мережі, і при відсутності значних помилок (людський фактор) можна забезпечити рівень безпеки, відповідний цінності інформації, що знаходиться в такій мережі. На сьогоднішній день бездротову мережу можна вважати захищеною, якщо в ній працюють три основних складових системи безпеки: конфіденційність даних, цілісність даних при їх передачі, аутентифікація користувача. Для отримання належного рівня безпеки потрібно скористатися певними правилами при організації і налаштуванні приватної Wi-Fi-мережі.

Види атак на Wi-Fi мережі. Розвиток протоколів забезпечення безпеки бездротових мереж змушує зловмисників шукати обхідні шляхи для їх злому. Найбільш поширеними в даному контексті є комп'ютерні атаки, які спрямовані на користувачів Wi-Fi мережі. Можна виділити чотири основні загрози безпеці, пов'язані з мобільними клієнтами:

- Атаки на ОС і прикладне ПО клієнтів бездротової мережі;
- Перехоплення трафіку при використанні незахищених бездротових з'єднань;
- Атаки «Man in the middle», які можуть бути використані для реалізації інших атак;
- Використання бездротових клієнтів в якості каналу віддаленого доступу до корпоративної мережі.

Дослідження основних протоколів безпеки виявило вразливі місця, через які атакуючий може отримати повний доступ до мережевого трафіку. Найпоширенішими видами атак на Wi-Fi мережі є:

на протокол WEP:

- Plaintext-атака;
- Повторне використання шифра;
- Атака Fluhrer-Mantin-Shamir;
- Атака Low-Hanging-Fruit.

на протоколи WPA / WPA2:

- Атака перебором всіх можливих комбінацій ключа до його
- визначення;
- Атака з використанням вразливостей фіксованого пароля;
- Атаки по словнику;

- Глушіння клієнтської станції.

на протокол WPS:

- Перехоплення ключа на основі розбиття пароля навпіл.

Дії зловмисника також можуть бути спрямовані на виведення бездротової Wi-Fi мережі з ладу. Цьому можуть сприяти деякі проблеми. Ними є, наприклад:

- Можливість проведення атаки на відмову в обслуговуванні на фізичному рівні шляхом глушіння радіосигналу або канальному рівні шляхом експлуатації уразливості методу доступу до несучої;
- Реалізація функції енергозбереження, тобто коли легальний користувач може не отримати чи призначалася йому інформації при виході з режиму очікування;
- Наявність уразливості протоколу аутентифікації PEAP дозволяє послати клієнту помилкові фрейми успішної аутентифікації або від'єднання від мережі.

В цілому можна згрупувати види атак на бездротові точки доступу Wi-Fi наступним чином:

- Атака на WEP алгоритм;
- Злом паролів алгоритмів WPA/WPA2;
- Злом Пін-коду для стандарту WPS;
- Пониження WPA алгоритму;
- Заміна істинної точки доступу фальшивою;
- Шахрайська точка доступу;
- Атака на Wi-Fi точки доступу з глобальної та локальної мереж;
- Атаки виду відмова в обслуговуванні (DoS Wi-Fi).

Атака на WEP алгоритм. В цю групу атак входять не тільки розшифровка пароля у вигляді простого тексту. Для WEP алгоритму відкритий і реалізований ряд різноманітних атак, які дозволяють отримати бажаний результат навіть без розшифровки парольної фрази. На даний момент популярність злому WEP алгоритму йде на другий план, оскільки постійно зменшується кількість точок доступу, які його використовують. Далі у таблиці 1 представлено порівняння характеристик стандартів WEP, WPA і WPA2. [6]

Злом паролів алгоритмів WPA/WPA2. Це найбільш універсальна атака на Wi-Fi. Її плюсом є те, що вона може бути застосовна на всі точки доступу, які використовують WPA/WPA2 (таких більшість). Є й мінуси, які виявляються з надійності WPA/WPA2-шифрування, вони полягають в тому, що для реалізації атаки до точки доступу повинні бути підключені клієнти; розшифровка паролів ведеться методом перебору (brute force). Тобто при надійному паролі зламати Wi-Fi мережу за прийнятний час не вийде. До 2017 року основними методами злому WPA2 PSK-шифрування були такі як атаки по словнику і метод грубої сили. У жовтні 2017 року було опубліковано атаку з перевстановленням ключа на стандартах захисту WPA і WPA2, названа KRACK. Активний атакуючий може скинути випадкове число генеруєме точкою доступу і клієнтом при встановленні з’єднання (nonce) і викликати його перевикористання. У режимі AES-CCMP атака дозволяє атакуючому відтворювати раніше відправлені пакети і полегшує розшифровку даних, що пересилаються. У режимах WPA TKIP і GCMP – атакуючий має можливість як розшифровувати, так і впроваджувати пакети в з'єднання. [6] Key Reinstallation Attack (KRACK) — повторне використання ключа. Вразливість типу атаки «повторного використання» в протоколі WPA. Ця вразливість була виявлена в 2016 році дослідниками Меті Вангофом (Mathy Vanhoef) та Френком Пісенсом (Frank Piessens) з університету KU Leuven в Бельгії. Дослідники оприлюднили своє дослідження в жовтні 2017 року. Виявлена вразливість дозволяє повторно встановлювати один і той самий криптографічне випадкове число генеруєме точкою доступу і клієнтом при встановленні з’єднання на третьому кроці в процедурі відкриття сеансу (так зване «рукостискання») за протоколом WPA2. Завдяки цьому зловмисник має можливість здійснити криптоаналіз та встановити сеансовий ключ. Таким чином, зловмисник може сканувати дані, а в деяких випадках, навіть заміняти дані, що передаються між клієнтом та точкою доступу. Дана вразливість наявна у протоколах WPA та WPA2 та для всіх визначених стандартом алгоритмів шифрування: WPA-TKIP, AES-CCMP, та GCMP. Дану вразливість можна усунути оновленням програмного забезпечення клієнтів та точок доступу Wi-Fi. [7]

Злом Пін-коду для стандарту WPS. Даний злом схожий на злом WEP стандарту. Злом Пін-коду добре піддається злому, недавно була виявлена нова вразливість, яка вимагає на злом кілька секунд. Суть вразливості як і у WEP - відсутність універсальності. На даний момент зменшується кількість точок доступу, в яких WPS включений. [8]

Пін-код, за допомогою якого і проводиться автентифікація, складається з восьми цифр, які при переборі можна розбити на дві частини, оскільки при відгадуванні першої половини Пін-коду точка доступу почне відправляти повідомлення про те, що друга половина не є вірною. Окрім того остання цифра є контрольною сумою перших семи цифр, і може бути відновлена за формулою:

$$f(n) = f\left(\left[\frac{n}{10}\right]/10\right) + 3(n \bmod 10) + \left(\left[\frac{n}{10}\right] \bmod 10\right) \quad (1)$$

Отримавши f(n), можемо отримати контрольну суму (останній символ Пін-коду)

$$S_C: \quad S_C = (10 - f(n) \bmod 10) \bmod 10. \quad (2)$$

Пін-код складається з восьми цифр - отже, існує 10^8 варіантів перебору або якщо перевести, то 100 000 000 варіантів.

Якщо Пін-код розбити на дві частини виходить 10^4 і 10^3. Відповідно до цього зловмисникові необхідно перебрати всього лиш 10^4+10^3 варіантів.

Якщо перевести 10^4, то відповідно отримаємо 10 000 варіантів перебору для першої половини і для останніх 3 цифр тобто для 10^3 отримаємо 1000 варіантів перебору. У підсумку це становить лише 11 000 варіантів для повного перебору, що більше ніж в 9000 разів менше вихідного числа варіантів 10^8.

Комплекс методів захисту точок доступу Wi-Fi.

Відповідно до підвищених вимог безпеки необхідно використовувати тунелювання і при цьому необхідно використовувати взаємну аутентифікацію обох кінців тунелю. Під час аутентифікації клієнт і аутентифікатор перевіряють справжність один одного і переходять до процесу чотиристороннього рукостискання (4-way handshakekey) для вироблення ключів. Цей механізм завершує процедуру аутентифікації. Рукостискання ініціюється аутентифікатором, при цьому використовується формат пакета EAPoL-key. Процедура рукостискання починається з обчислення клієнтом і аутентифікатором парного майстер-ключа (PMK). Після генерації PMK починається обмін повідомленнями EAPoL-key. У першому повідомленні аутентифікатор посилає кадр EAPoL-key, що містить ANonce (Authenticator Nonce). ANonce - одноразове випадкове або псевдовипадкове число, яке генерується за допомогою лічильника глобальних ключів розміром 256 біт, що міститься в кожній бездротової станції. Він ініціалізується при завантаженні системи. Значення лічильника встановлюється за допомогою псевдовипадкової функції Nonce. [5]

Nonce ← PRF-256(Random number + "Init Counter"+ Local MAC Address || Time) (3)

де PRF-256 – псевдовипадкова функція (Pseudorandom Function), результат якої має розмір 256 біт; Random number - випадкове число; "Init Counter" - символьний рядок; Local MAC Address - MAC-адресу пристрою; Time - значення поточного часу в форматі протоколу NTP (Network Time Protocol).

Для захисту мереж стандарту 802.11 повинен бути передбачений наступний комплекс заходів щодо безпеки передачі даних. Необхідно встановити маршрутизатор в безпечному місці, де бездротовий сигнал доступний тільки всередині будинку. Рекомендується обновити ПЗ маршрутизатора, щоб виправити його відомі уразливості. Необхідно вимкнути віддалене управління маршрутизатором через Інтернет. Необхідно використовувати WPA2-шифрування і складний та стійкий пароль. Якщо використовувати простий пароль для шифрування WPA2, то він може бути зламаний. Рекомендовано створювати стійкий пароль при цьому можна використати генератори пароля чи фразу, яку можливо легко запам'ятати. Цілком відповідним паролем буде являтися пароль в 10-15 символів, бажано з великими і малими буквами та цифрами і рекомендується використати спецсимволи. Якщо використовується шифрування WPA2 з складним паролем і WPS в роутері відключений - мережа в певній мірі достатньо захищена. Необхідно приховувати SSID-ім'я бездротової мережі. Необхідно вимкнути функцію WPS. Функція фільтрації MAC-адрес надає істотну можливість підвищити безпеку. Рекомендується протидіяти атаці яка має назву ром-0 (тобто доступ до секретних даних, що зберігаються на роутері: комбінацію ім'я/пароль і пароль WiFi) тобто перенаправити порт 80 на неіснуючу адресу.

Для запобігання CSRF атак не рекомендовано використовувати IP адреси і діапазони адрес за замовчуванням. Іншим методом підвищення рівня безпеки бездротових Wi-Fi мереж, є використання статичних ір-адрес для пристроїв. В маршрутизаторах з стандартними налаштуваннями може бути включений сервер DHCP. Під час підключення комп'ютера чи можливо пристрою до бездротової мережі, пристрій робить запит маршрутизатору про IP-адресу і DHCP-сервер призначає її. Якщо відключити DHCP-сервер, то кожен пристрій повинен бути налагоджений вручну для того, щоб підключитися до мережі Рекомендується використання VLAN мережі для більш надійного захисту мережі, слід також використовувати мережеві екрани з підвищеними налаштуваннями політики безпеки. Також рекомендується вимкнути IPv6 на маршрутизаторі, або, в разі якщо є необхідність послуги IPv6, необхідно обрати маршрутизатор з сертифікованим IPv6 стандартом. Щодо конфігурації точки бездротового доступу рекомендується не використовувати в цьому випадку веб-браузер. Краще робити такі дії за допомогою SNMP-утиліти налаштування, яка йде в комплекті з усіма точками доступу, або telnet-клієнта (або за допомогою підключення до послідовного порту точки доступу), якщо ця можливість передбачена виробником, причому саме з проводового сегмента мережі.

Висновок. Для забезпечення високого рівня безпеки бездротових мереж було розроблено комплекс заходів. Бездротова мережа може мати достатній рівень захисту лише при виконанні розглянутих вимог безпеки. Відповідно до високих вимог безпеки бездротову мережу можна вважати захищеною, якщо в ній працюють три основних складових системи безпеки: конфіденційність даних, цілісність даних при їх передачі. аутентифікація користувача . В даний час існують різні способи захисту Wi Fi мереж які були розглянуті в даній статті і за умови правильного налаштування, э певна гарантія в забезпеченні необхідного рівня безпеки. На даний момент, більш безпечними можна вважати мережі стандарту 802.11, які захищені за допомогою стандарту WPAv2 при умові використання протоколів EAP різних типів з підтримкою тунелювання і двосторонньої аутентикації обох кінців тунелю. До додаткових типів протоколів EAP відносяться EAP-TLS і EAP-FAST. При цьому, для використання EAP-TLS потрібна наявність сертифікатів аутентифікації на клієнтських пристроях. На основі отриманих даних при обчисленні злому Пін-коду для стандарту WPS можна оцінити складність злому цієї функції. Оскільки увімкнений механізм WPS лише погіршує захищеність точки доступу то комбінація даного механізму навіть з використанням методів аутентифікації стандартів WPA/WPA2 може представляти собою загрозу бездротовій мережі. В даній роботі метод аутентифікації WPA2 представлений як найстійкіший механізм захисту бездротових мереж. Метод аутентифікації WPA2 потребує окремого розгляду та детальної оцінки.

ПЕРЕЛІК ДЖЕРЕЛ І ПОСИЛАНЬ:

1. Владимиров А.А. Wi-фу: "боевые" приемы взлома и защиты беспроводных сетей / А.А. Владимиров, К.В. Гавриленко, , А.А. Михайловский – М.:издательство НТ Пресс, 2005. – 462 с.
2. Cisco Visual Networking Index: Forecast and Methodology, 2013–2018. – Cisco Public, 2014, June 10.
3. Certified Wireless Security Professional Official Study Guide. Coleman D., Westcott D., Harkins B., Jackman S. – Wiley Publishing, Inc., 2010.
4. Скляров Д.В. Искусство защиты и взлома информации / Д.В. Скляров. – СПб.: БХВ-Петербург, 2004. – 288 с.
5. 802.11 Wireless Networks Security and Analysis. Holt A., Chi-Yu Huang. – Springer, 2010.
6. Защита в сетях Wi-Fi [Електронний ресурс] // Wikimedia Foundation, Inc.. – 2017. – Режим доступу до ресурсу: https://ru.wikipedia.org/wiki/Защита_в_сетях_Wi-Fi.
7. KRACK [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/KRACK.
8. Виды атак на Wi-Fi [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: https://hackware.ru/?p=158.