УДК 004.056

П.П. Процик, к.т.н. В.Л. Дунець
Тернопільський національний технічний університет імені Івана Пулюя, Україна

ОБҐРУНТУВАННЯ МЕТОДІВ ЗАХИСТУ МЕРЕЖ Wi-Fi

У роботі розглянуто методи захисту Wi-Fi мереж від несанкціонованого доступу, проаналізувати їхні переваги та недоліки.

Ключові слова: інформація, метод захисту, автентифікація, Wi-Fi мережа.

P.P. Protsyk, V.L. Dunets

REFERENCE TO PROTECTION METHODS WI-FI NETWORK

The paper considers methods of protecting Wi-Fi networks from unauthorized access, analyze their advantages and disadvantages.

Keywords: information, security method, authentication, Wi-Fi network.

Функціонування більшості сучасних підприємств базується на використанні комп'ютерних мереж. Для ефективного вирішення задач, пов'язаних із мобільністю та масштабністю мережі, доцільно використовувати бездротові комп'ютерні мережі стандарту IEEE 802.11. В той же час використання бездротових мереж створює нові виклики, пов'язані з розробкою систем захисту від кіберзагроз. Якщо захисту мережі не приділити належної уваги, може трапитись втрата конфіденційної інформації користувачів, втрата доступу до ресурсів і дисків користувачів Wi-Fi-мереж і ресурсів LAN, спотворення інформації, що проходить в мережі, впровадження підроблених точок доступу і т.п. [1]

Класифікувати методи захисту бездротової мережі можна за різними ознаками, в першу чергу існують методи фізичного, технічного та програмного захисту. В дослідженні акцент робиться на останньому, як такому, що є найбільш прогресивним. Методи програмного захисту у свою чергу поділяються на методи обмеження доступу, методи автентифікації і шифрування [2].

Одним із методів обмеження доступу є фільтрування MAC-адрес. Даний метод дозволяє визначити список пристроїв і дозволити лише цим пристроям доступ до вашої мережі Wi-Fi (whitelist), або навпаки заборонити певним пристроям доступ (blacklist).

Ще одним методом обмеження доступу є режим прихованого SSID. SSID (Service Set Identifier) – це ідентифікатор мережі, який за замовченням надсилається маршрутизатором або точкою доступу бездротової мережі у режимі broadcast, тобто всім. Зазвичай точки доступу мережі Wi-Fi надсилають своє мережеве ім'я як один з інформаційних елементів, які входять до деяких кадрів керування, ці елементи, або маяки, з інформаційним елементом, ідентифікатором якого є 0. Приховати SSID, тобто припинити його транслювати в ефір, також вважається одним із методів захисту. Проте, на мою думку, це ще один не ефективний і скоріше теоретичний метод захисту. Один із фахівців Microsoft Стів Райлі про даний метод висловився так: «SSID – це мережеве ім'я, а не пароль. Бездротова мережа має SSID, щоб відрізняти її від інших бездротових мереж поблизу. SSID ніколи не розроблявся, щоб бути прихованим, і тому не забезпечить вашу мережу будь-яким захистом, якщо ви намагаєтесь сховати його» [3]. Даний метод не є ефективним, через те, що ідентифікатор "прихованої" мережі дуже легко знайти з допомогою короткочасного програмного сканування всіх доступних мереж в радіусі доступу.

Наступним методом обмеження доступу є статична IP-адресація. Цей метод захисту полягає у відключені динамічного призначення локальних IP-адрес

центральною станцією (маршрутизатором), натомість вимагаючи від користувачів вручну налаштовувати відповідні параметри мережі (адресу, маску, DNS-сервер, шлюз, тощо). Про те цей метод також не є досить ефективним, адже не забезпечує достатнього захисту від злому. До того ж, такий спосіб адресації значно ускладнює адміністрування мережі, зокрема в частині додавання нових вузлів та погіршує масштабування мережі, що неприпустимо в бездротових мережах, адже вони, навпаки, мають покращувати цей параметр.

Наступна категорія методів захисту - це методи автентифікації. До них належать відкрита автентифікація, автентифікація зі спільним ключем (WEP, WPA) і автентифікація за допомогою RADIUS-сервера.

Відкрита автентифікація дозволяє будь-якому бездротовому пристрою автентифікуватись, а потім намагатися встановити зв'язок з точкою доступу. Це не завжди означає, що одразу після автентифікації буде надано доступ до мережі. Після автентифікації може бути запитано пароль, ключову фразу, додаткові ідентифікаційні дані, тощо. Проте, такий метод автентифікації також не захищає мережу від зловмисників і може використовуватись лише на точках доступу, що відділені від основної мережі додатковими засобами захисту, наприклад брандмауером.

Автентифікація зі спільним ключем (WEP, WPA). Даний метод автентифікації є найпопулярнішим, а його ефективність залежить від стандарту захисту, який використовується для його реалізації. Під час автентифікації за допомогою спільного ключа, ключі клієнта та точки доступу повинні співпадати. Першим стандартом захисту з використанням спільного ключа був WEP (Wired Equivalent Privacy), проте попри свою гучну назву (Захист еквівалентний дротовому) цей стандарт має слабкі місця, через які процес несанкціонованого доступу до мережі стає дуже простим. До переваг даного алгоритму можна віднести лише швидкодію та простоту реалізації. Що ж стосується недоліків, то основним є те, що існують дієві методи атаки на цей алгоритм, що робить його використання не доцільним в сучасних системах. На зміну стандарту WEP прийшов стандарт WPA (Wi-Fi Protected Access) і цей стандарт виключив можливість простого способу атаки через прослуховування трафіка і, відповідно, прибрав необхідність повторно використовувати ключі шифрування. В основі стандарту WPA лежить протокол тимчасової цілісності ключів TKIP (Temporary Key Integrity Protocol). TKIP динамічно генерує новий 128-бітний ключ для кожного пакета і тим самим запобігає WEP-скомпрометованим типам атак. TKIP та відповідний стандарт WPA реалізують три нові функції безпеки для вирішення проблем безпеки, що виникали в WEP-захищених мережах [5]. По-перше, TKIP реалізує ключову функцію змішування, яка поєднує таємний корінний ключ з вектором ініціалізації, перш ніж передавати його до ініціалізації. По-друге, WPA реалізує лічильник послідовності, щоб захистити мережу від повторних атак. Пакети, що надходять не по встановленому порядку, будуть відхилені точкою доступу. По-третє, TKIP реалізує 64-розрядну перевірку цілісності повідомлень (MIC). TKIP гарантує, що кожен пакет даних надсилатиметься з унікальним ключем шифрування. Змішування ключів збільшує складність розшифровування ключів, надаючи зловмиснику суттєво менше даних, які були зашифровані за допомогою будь-якого одного ключа. Перевірка цілісності повідомлення запобігає прийняттю підроблених пакетів. У WEP було можливим змінити пакет, вміст якого був відомий, навіть якщо він не був розшифрований. Проте, незважаючи на ці зміни, слабкість захисту деяких з цих доповнень дозволила створити нові, хоч і більш складні, способи атак. Протокол TKIP не вважається надійним і офіційно не підтримується стандартом 802.11 з 2012 року [4].

Із різноманітності методів захисту для побудови бездротової Wi-Fi мережі найбільш ефективним є комбінація використання стандарту захисту WPA2 та

протоколу шифрування CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol) з використанням складного ключа доступу (наприклад 14-и значного набору випадкових цифр та літер).

WPA2 виправила помилки попереднього стандарту і в основі даного стандарту лежить протокол шифрування CCMP, який в свою чергу базується на принципово новому алгоритмі шифрування AES (Advanced Encryption Standard). AES працює на принципі проектування, відомому як мережа заміщення-перестановки, що поєднує як заміщення, так і перестановку, і швидко працює як у програмному, так і в апаратному забезпеченні. Вдала атака на мережу, захищену за стандартом WPA2 з ключем, розміром 256 біт хоча і можлива теоретично, проте вимагає високої кваліфікації зловмисника, спеціального програмного/технічного забезпечення, та, що найголовніше, значного проміжку часу. Проте, і ці методи організації захисту не є досконалими і, окрім програмного захисту, потрібно також враховувати необхідність постійного моніторингу роботи мережі, організацію технічного та фізичного захисту [6].

Автентифікація за допомогою RADIUS-сервера. Remote Authentication Dial In User Service (RADIUS) або Віддалений ідентифікаційний набір в службі користувача - це протокол, що забезпечує трирівневу систему: автентифікація, авторизація та облік і використовується для віддаленого доступу до мережі. Ідея полягає в тому, що існує сервер, який виконує функції «охоронця», перевіряючи ідентифікацію через ім'я користувача та пароль, які вже заздалегідь визначені користувачем. Сервер RADIUS також може бути налаштований для виконання політик та обмежень користувачів, а також запису облікової інформації, такої як час підключення для таких цілей, як платіж. Такий метод захисту досить надійний, проте вимагає додаткового обладнання, налаштування та може застосовуватись лише в комбінації з іншими методами захисту. Такий підхід захисту бездротових мереж, як правило застосовують у великих корпоративних мережах.

Провівши аналіз та порівнявши особливості методів захисту слід зауважити, що технології обмеження доступу не є надійними при побудові систем захисту комп'ютерних мереж стандарту IEEE 802.11, а що стосується методів авторизації та шифрування, то лише використання комбінації сучасних протоколів/алгоритмів та коректне налаштування мережевого обладнання дозволяє тримати прийнятний рівень безпеки.

Література

1. О. Юдін, Г. Конахович, О. Корченко, Захист інформації в мережах передачі даних: підруч. К.: Вид-во ТОВ НВП "ІНТЕРСЕРВІС", 2009, 714 с.
2. «Защита беспроводных сетей, WPA: теория и практика» [Електронний ресурс] : [Веб-сайт]. – Режим доступу: https://www.ixbt.com/comm/prac-wpa-eap.shtml (дата звернення: 14.04.2019).
3. «S. Riley, Myth vs reality: Wireless SSIDs». [Електронний ресурс] [Веб-сайт]. - Режим доступу: https://blogs.technet.microsoft.com/steriley/2007/10/16/myth-vs-reality-wireless-ssids. [дата звернення: 14.04.2019].
4. Щербаков В.Б., Ермаков С.А. «Безопасность беспроводных сетей: стандарт IEEE 802.11». - М: РадиоСофт. - 2010. - 255 с.
5. Кіберполіція: захист мереж WI-FI - на дуже низькому рівні, 2017. [Електронний ресурс]. Режим доступу: https://www.ukrinform.ua/rubric-technology/ 2281044-kiberpolicia-zahist-merez-wifi-na-duze-nizkomu-rivni.html [дата звернення: 14.04.2019].
6. Пролетарский А.В., Баскаков И.В., Чирков Д.Н. «Беспроводные сети Wi-Fi». - М:Бином. Лаборатория знаний, 2007. - 178 с.