УДК 658.52; 681.3

ІНФОРМАЦІЙНА БЕЗПЕКА БЕЗДРОТОВИХ МЕРЕЖ

Губик О.З.

Гриник Р.О., ЛДУ БЖД, викладач КУІБ

ЛДУ БЖД

На сьогоднішній час широкого застосування набули без провідникові Wi-Fi мережі стандарту 802.11. Гаджети з підтримкою стандарту 802.11 організовують зв'язок один з одним, використовуючи в якості каналу передачі даних певний діапазон радіочастот. Дані передаються по радіоканалу відправником, за замовчування вважається, що приймач також працює в обраному радіодіапазоні радіочастот. Основним недоліком використання даного механізму є те, що будь-яка третя особа, яка використовує цей діапазон, теж здатна прийняти ці дані та обробити їх. Для організації захисту даних що передаються необхідно використовувати який-небудь механізм захисту, щоб забезпечити мінімальний захист мережа повинна включати в себе наступні компоненти:

- Засіб прийняття рішення, що до того хто має право доступу до мережі. Дана вимога реалізується за допомогою аутентифікації користувача.
- Механізм захисту повідомлення підчас його руху по мережі. Дана вимога реалізуються за допомогою алгоритмів шифрування інформації.

В сучасних мережах захист інформації здійснюється одночасним використанням аутентифікації користувача та шифруванням повідомлення що передається. Стандарт IEEE 802.11 підтримує використання двох методів аутентифікації [1]:

- Відкрита аутентифікація. Даний метод аутентифікації здійснює захист на основі обмеження доступу до мережі по фільтрації MAC адрес.
- Аутентифікація із загальним ключем. Даний метод здійснює захист на основі шифрування повідомлення, тобто абонент робить запит у точки доступу на що у відповідь отримує 128 байт інформації, котрі шифрує за допомогою ключа і відправляє назад до точки доступу, точка розшифровує повідомлення і порівнює з вихідним, якщо воно ідентичне надає права доступу абоненту.

Уразливість мережі при використанні відкритої аутентифікації полягає в тому, що MAC-адреси передаються за допомогою незашифрованих фреймів стандарту 802.11, що дає можливість зловмиснику прослухати мережу, дізнатись MAC-адресу яка знаходиться в «довірчому списку» точки доступу та імітувавши її підключитись до мережі.

Уразливість мережі при використанні методу аутентифікації із загальним ключем є значно нижчою ніж при використанні відкритої аутентифікації, але якщо зловмисник володіє необхідними навичками і має необхідне програмне забезпечення то через невеликий проміжок часу він отримає доступ до мережі. Уразливість обумовлена як раз тим, що

механізм WEP застосовує алгоритм складання ключа на основі поточного шифру RC4. Частина векторів ініціалізації можуть розкрити біти ключа в результаті проведення статистичного аналізу. Дослідники компанії AT&T і університету Rice скористалися цією вразливістю і з'ясували, що можна дістати WEP-ключі довжиною 40 або 104 біт після обробки 4 мільйонів фреймів, це означає що для пасивного взлому мережі з довжиною ключа 104 біти зловмиснику знадобиться менше години часу. Зловмисник також може використовувати активні атаки на мережу, зміст цих атак полягає у тому що порушник впливає на мережу для отримання певної інформації для індуктивного обчислення секретного ключа. В основі активної атаки WEP лежить те, що при потоковому шифруванні відбувається XOR початкового повідомлення і ключа для обчислення зашифрованого повідомлення. Індуктивне обчислення ключа ефективне в силу відсутності хорошого методу контролю цілісності повідомлень. Значення ідентифікатора ключа (ICV), завершального кадру WEP, обчислюється за допомогою функції CRC32 (циклічний надлишковий 32-бітний код), схильною до атак з маніпуляцією бітами. В результаті існують атаки, засновані на повторному використанні вектора ініціалізації (IV Replay) і маніпуляції бітами (Bit-Flipping) [2].

Отже зі всього вище сказаного можна зробити висновок, що бездротові мережі мають багато недоліків і являються вразливими як до пасивних так і до активних атак, а тому при передачі даних через Wi-Fi мережу необхідно звертати увагу на їх зміст і якщо вони мають конфіденційну інформації краще захистити її з допомогою додаткового шифрування.

ЛІТЕРАТУРА

1. Захист у мережах Wi-Fi [Електронний ресурс] Режим доступу: https://uk.wikipedia.org/wiki/Захист_у_мережах_Wi-Fi
2. Юдін О.К., Весельська О., Аналіз захищеності бездротових мереж з використанням WEP-технології, Наукоємні технології №3, 2012, с.62-67