Секція 5

АВТОМАТИЧНІ СИСТЕМИ БЕЗПЕКИ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

УДК 004.7719

СПОСОБИ ЗАХИСТУ БЕЗДРОТОВИХ МЕРЕЖ

Антонюк В.І., НУЦЗУ
НК – Маляров М.В., к.т.н., доц., НУЦЗУ

У теперішній час технологією, стрімкого розвитку набувають бездротові локальні мережі, передача інформації в яких відбувається за допомогою радіохвиль (за рахунок перетворення необхідної інформації в радіохвилі, та передачі даних за допомогою вбудованих антен). Бездротові мережі на даний час працюють на частотах 2.4 ГГц чи 5 ГГц. Використання бездротової технологій призводить до того, що такі мережі досить сильно схильні до ризику несанкціонованого доступу, отже на їх захист слід звернути особливу увагу.

В [1] приведено результати опитування користувачів бездротових мереж, щодо використання протоколів захисту. Найбільша кількість користувачів (60% опитаних) використовує шифрування WPA/WPA 2 (Wi-Fi Protected Access) протокол базується на тимчасовому протоколі цілісності ключів (TKIP), завдання якого – не допустити повторного використання кодуючих ключів. Довжина пароля при цьому захисту випадкова та коливається від 8 до 63 байт, завдяки чому його підбір стає досить складним.

Інша велика категорія (17% опитаних) використовують у якості захисту фільтрацію за MAC-адресою. Оскільки кожен бездротовий пристрій має унікальну MAC-адресу, бездротові маршрутизатори та точки доступу можуть відмовити в підключенні до мережі бездротовим пристроям, якщо MAC-адреси цих пристроїв не є авторизованими. При цьому сама передача інформації через мережу не має ніякого захисту. Це означає, що точка доступу, як і клієнт, не маскують передачу даних. Так як майже будь-який бездротовий адаптер має можливість "прослуховування" (замість прийому пакетів, призначених тільки собі, будуть прийматися всі можливі пакети), цей спосіб захисту взагалі та є неактуальним.

Інші способи поділилися приблизно на рівні. Стандарт напівавтоматичного створення бездротової мережі WPS (8% опитаних) дозволяє клієнту підключитися до точки доступу за 8- символьним кодом, що складається з цифр (PIN). А завдяки помилці у стандарті потрібно підібрати лише 4 символи. Отже, достатньо лише 10000 спроб підбору. На подив були люди (6% опитаних), які взагалі не використовували у своїх мережах жодного захисту, аргументуючи це тим, що їм нічого приховувати. Застарілому протоколу шифрування шифрування WEP, що заснований на алгоритмі шифрування з 40 або 104 – бітовим ключем довіряє 5% опитаних. Мінусом цього алгоритму безумовно є 40-бітний ключ та незмінність ключа, що значно спрощує злом. І на останню, приховуванням імені точки доступу (прихована SSID) довіряє 4% опитаних.

Не слід нехтувати безпекою своєї бездротової мережі і бути завжди уважними, використовувати лише довгі паролі, через деякий проміжок часу слід змінювати паролі.

ЛІТЕРАТУРА

1. Бездротова технологія Wi-Fi. Вразливості та методи захисту. В.І. Вязмін, А.В. Чернишова. ДНТУ Інформатика та кібернетика № 2 (12), 2018, Донецьк, ДонНТУ.