УДК 004.056
Лізунов С.І.[1], Корольков Р.Ю.[2], Верещака М.П.[3]
[1] канд. техн. наук, доц. НУ «Запорізька політехніка»
[2] канд. техн. наук, старш. викл.НУ «Запорізька політехніка»
[3] асп. НУ «Запорізька політехніка»

АТАКА НА ВИЧЕРПАННЯ ЗАРЯДУ БАТАРЕЇ БЕЗДРОТОВИХ ПРИСТРОЇВ

Технології підключення до Інтернету речей (IoT) стали необхідними в усіх сферах повсякденного життя. Суспільство вступило в епоху IoT, де технології комунікаційних мереж дозволяють взаємодіяти один з одним [1,2]. Пристрої обмінюються даними з іншими бездротовими гаджетами, незалежно від того чи належать вони до однієї інформаційної мережі, чи ні. Для цього не потрібно знати паролі або мати спеціальні дозволи, самі відповіді та запити можуть взагалі не містити жодної важливої інформації.

Подібно до більшості технологій, механізми енергозбереження Wi-Fi були розроблені та стандартизовані з акцентом на продуктивність і QoS, а не на безпеку.

Щоразу, з представленням нового стандарту Wi-Fi, робоча частота стає вище, щоб ще більше підвищити швидкість передачі, охопити якомога більше послуг і якість обслуговування (QoS). Разом з цим у технології Wi-Fi впроваджено різні енергозберігаючі механізми і протоколи для зниження динаміки енергоспоживання і підвищення енергоефективності. Отже, протоколи ефективні з точки зору продуктивності і можуть використовуватися без проблем коли такі сценарії, як атаки на енергоспоживання від батарей, не розглядаються.

Постійний обмін інформацією пристроїв з Wi-Fi, що працюють від автономних джерел живлення (батарей, акумуляторів, тощо) не дозволяє гаджетам перейти до режиму сну, через що швидше виснажується заряд таких джерел з обмеженою ємністю.

Базовий механізм енергозбереження технологій Wi-Fi має дві вразливості безпеки.

По-перше, бездротові станції перемикаються в режим пробудження виключно в залежності від бітової карти індикації трафіку (TIM – Traffic Indication Map), що передається у beacon кадрах, які не піддаються перевірці. Якщо з прийнятого кадру beacon стало відомо, що для станції немає буферизованих пакетів, станція повертається до сну відразу після закінчення прийому кадру beacon. Таким чином, зловмисник може тримати станцію в активному стані, прослуховуючи ефір та відправляючи підроблені beacon

кадри. Після пробудження цільової станції зловмисник змушує споживати додаткову енергію, обробляючи підроблені кадри.

По-друге, реалізовані системи підтримують та покращують швидкість обробки та QoS, розширюючи режим пробудження таким чином, щоб був отриманий новий кадр, у той час, коли потрібно ввести інтервал енергозбереження. Тому, коли зловмисник постійно надсилає підроблені кадри, цільовий пристрій постійно продовжує режим пробудження. Отже, режим енергозбереження не може бути активований і відбувається підвищене енергоспоживання.

На перший погляд, розрядка акумуляторів здається малоймовірним у такий спосіб, але це може забезпечити можливість небезпечної атаки в комбінації з використанням інших вразливостей. Наприклад, зловмисники можуть знеструмити в такий спосіб акумулятори камер відеоспостереження. Причому згодом подібні атаки можуть ставати більш вишуканими, а кількість випадків їх використання збільшуватися.

Коли створюються протоколи неможливо передбачити як саме ними зловживатимуть. Фактично, при «творчому» підході, кількість таких способів може виявитися просто нескінченною.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Palattella, M.R.; Dohler, M.; Grieco, A.; Rizzo, G.; Torsner, J.; Engel, T.; Ladid, L. Internet of things in the 5G era: Enablers, architecture, and business models. IEEE J. Sel. Areas Commun. 2016, 34, 510–527.

2. Lin, J.; Yu, W.; Zhang, N.; Yang, X.; Zhang, H.; Zhao, W. A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. IEEE Internet Things J. 2017, 4, 1125–1142.