АНАЛІЗ СПУФІНГ АТАК НА BLUETOOTH-ПРИСТРОЇ

Штангей В.О., Наконечний М.В., В'юхін Д.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасний світ наповнений Bluetooth-пристроями, від мобільних пристріїв, IoT-систем, медичних приладів та промислового обладнання. Однак відкритий характер технології створює значні ризики для користувачів, зокрема вразливість до спуфінг-атак, що дозволяють зловмисникам підміняти ідентифікаційні дані пристроїв для отримання несанкціонованого доступу або їх відмови [1].

Метою доповіді є розгляд методу атаки на Bluetooth-пристрої з використанням атаки через l2ping, яка дозволяє надсилати пакети заданого розміру на цільовий пристрій, викликаючи його нестабільність або навіть тимчасовий вихід з ладу. Такий спосіб впливу порушує нормальне функціонування Bluetooth-модуля жертви, що може призвести до зниження продуктивності або розриву бездротового з'єднання.

Атака передбачає підміну ідентифікаційних даних Bluetooth-пристрою, зокрема MAC-адреси або імені, щоб змусити інші пристрої вважати зловмисника довіреним партнером. Вона може бути реалізована за допомогою спеціального програмного забезпечення, що імітує роботу справжнього пристрою, або методів перехоплення й модифікації трафіку.

Головна особливість цієї атаки полягає в її простоті. Виконання команди l2ping не потребує складних налаштувань і може бути здійснене всього одним запуском, що робить її швидкою та ефективною. Атакуючий може заздалегідь підготувати файл із параметрами і просто виконати його, запустивши атаку без додаткових дій. Команда ініціює відправлення пакетів зазначеного розміру до пристрою з вказаною MAC-адресою. У процесі атаки час відповіді цільового пристрою почне поступово збільшуватися, а його Bluetooth-модуль може вийти з ладу або тимчасово відключитися.

Ефективне виявлення спуфінг-атак передбачає аналіз поведінки Bluetooth-з'єднань, виявлення аномалій у процесі підключення та застосування криптографічних методів для перевірки автентичності пристроїв. Для підвищення безпеки використовуються механізми шифрування переданих даних, що ускладнюють можливість їхнього перехоплення або модифікації [2, 3].

Список літератури

1. Д'якова, Н.Є., Сєвєрінов О.В. Аналіз загроз безпеки у системах розумного будинку. ВА ЗС АР; НТУ" ХПІ"; НАУ, ДП "ПДПРОНДІАВІАПРОМ"; УмЖ, 2021.

2. Польська Б. Ю. Методи захисту інформації в IoT – https://openarchive.nure.ua/entities/publication/89c3cc5e-8b01-43d5-be13-8fc837ad0ae4.

3. Matheus E. Garbelini, Sudipta Chattopadhyay, Vaibhav Bedi, Sumei Sun, Ernest Kurniawan (2021), Braktooth: Causing Havoc on Bluetooth Link Manager.