Дослідження стійкості до атак повторного відтворення протоколів дистанційного керування, які використовують радіоканал 433 МГц

УДК 004.738.5

Тарас Наконечний[1], Ольга Михайлова[2]

Національний університет "Львівська політехніка",
[1]taras.i.nakonechnyi@lpnu.ua, [2]mykhaylovaolga1@gmail.com

Протокол EV1527 використовується у багатьох системах дистанційного керування. Він складається з преамбули та основної частини, що містить код ключа та дані. Основною вразливістю є використання статичного коду, що дозволяє виконувати атаки повторного відтворення. Аналіз протоколів EV1527 та PT2262 показав, що жоден з них не має механізмів захисту від подібних атак. Протокол EV1527, розроблений компанією Silvan Chip Electronics Tech. Co. Ltd, використовує формат повідомлень, де кожне повідомлення складається з преамбули та основної частини. Переамбула складається з 32 бітів і використовується для синхронізації передавача та приймача. Основна частина повідомлення містить код ключа та чотири біти даних, що кодуються за допомогою послідовностей «3-1» для передачі логічної одиниці та «1-3» для передачі логічного нуля.

Атака повторного відтворення полягає у перехопленні зловмисником комунікації між двома легітимними сторонами та повторному надсиланні перехоплених даних з метою активації віддалено керованої системи. Демонстрація виконання подібної атаки показала, що передавачі EV1527 є вразливими до таких атак. Використання трансивера з програмним керуванням HackRF One дозволяє зловмиснику перехопити сигнал, відтворити його та отримати доступ до системи безпеки. Схема атаки повторного відтворення включає три основні етапи: перехоплення сигналу, збереження перехопленого сигналу та його відтворення. Перший етап полягає в прослуховуванні радіочастотного діапазону, в якому працюють передавач та приймач. Після цього зловмисник записує перехоплений сигнал та зберігає його у цифровому форматі. На останньому етапі зловмисник відтворює сигнал, що призводить до активації віддалено керованої системи, наприклад, відкриття воріт або вимкнення сигналізації.

Для ефективного перехоплення сигналів необхідно використовувати антени, що відповідають діапазону робочих частот цільових систем. У даному дослідженні було проведено порівняльний аналіз антен чотирьох типів: телескопічної антени, чотирьохдіапазонної автомобільної антени, антени типу "Ground plane" та антени з фіксованою довжиною. Результати показали, що телескопічна антена з мінімальною довжиною 17 см має найкращі характеристики для роботи з сигналами у діапазоні 433 МГц, забезпечуючи мінімальний коефіцієнт стоячої хвилі та оптимальні значення імпедансу. Чотирьохдіапазонна автомобільна антена виявилася менш ефективною через значні втрати сигналу при використанні магнітної підставки. Антена типу "Ground plane" продемонструвала прийнятні результати, але нестабільність параметрів вказує на необхідність додаткового налаштування для досягнення оптимальної роботи.

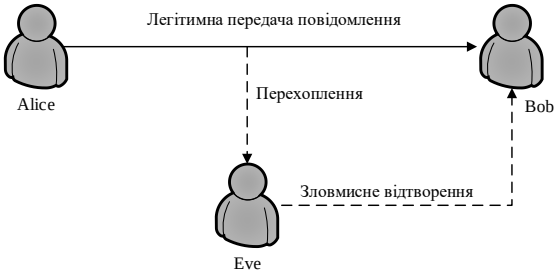

Рис.1.Схема повторного відтворення

Для проведення атаки повторного відтворення було використано такі обладнання та програмне забезпечення: трансивер HackRF One, програмний комплекс Universal Radio Hacker, приймач сигналу з виконавчим механізмом та комп'ютер під керуванням Kali Linux. Послідовність виконання атаки включала наступні кроки: підготовка системи, програмування приймача, оцінка радіочастотного спектру, перехоплення сигналу та його аналіз, відтворення сигналу. Перехоплені сигнали з передавачів аналізувалися за допомогою Universal Radio Hacker, що дозволило розшифрувати повідомлення протоколу EV1527 та відтворити їх для активації приймача.

Використання систем дистанційного керування з статичним кодом є небезпечним. Ця публікація показала вразливість протоколу EV1527 до атаки повторного відтворення, продемонструвала методи виконання даної атаки в лабораторних умовах та обгрунтувала вибір обладнання для здійснення даної атаки. В результаті даного дослідження можна зробити висновок про недоцільність використання протоколу EV1527 з точки зору безпеки. Рекомендується перехід від систем з фіксованим кодом до систем з динамічним кодом, таких як HCS301, які використовують криптографічні протоколи для забезпечення безпеки передачі даних по радіоканалу або відмова від простих протоколів дистанційного керування на користь більш надійних протоколів загального або спеціалізованого призначення, які використовують рішення для запобігання атакам різних видів.

1. Van Capelleveen T. Security analysis of aftermarket remote keyless entry systems for consumer vehicles: магістерська робота. Nijmegen, 2020. 84 p.
2. Silvan Chip Electronics Tech. Co. EV1527 OTP encoder. Sunrom Electronics. URL: https://www.sunrom.com/download/EV1527.pdf.
3. Princeton Technology Corp. PT2262 remote control encoder. LCSC. URL: https://datasheet.lcsc.com/lcsc/1809291408_PTC-Princeton-Tech-PT2262-S_C42793.pdf.