# АНАЛІЗ БЕЗПЕКИ ПРОТОКОЛІВ РОЗУМНОГО БУДИНКУ: ВРАЗЛИВОСТІ ВЕНДОРСЬКОЇ КРИПТОГРАФІЇ В БЕЗДРОТОВИХ ЗАМКАХ

Бойко М.С., В'юхін Д.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Поширення бездротових технологій інтернету речей (IoT) зробило смарт-замки на базі протоколу Bluetooth Low Energy (BLE) ключовим засобом фізичного контролю доступу.

На відміну від побутових сенсорів або кліматичних датчиків, помилки в конфігурації замків створюють пряму загрозу проникнення сторонніх осіб до приміщення [1, 2].

Незважаючи на вбудовані у стек BLE механізми безпеки, комерційні реалізації часто мають вразливості, зумовлені бажанням виробників спростити процес підключення або заощадити обчислювальні ресурси мікроконтролера [3].

Метою дослідження є аналіз можливих атак, пов'язаних із помилками у вендорській криптографії, а також дослідження роботи основних бездротових протоколів розумного будинку. Також у роботі проводиться їхнє техніко-економічне порівняння та визначаються найбільш стійкі до атак технології [3].

Намагаючись зробити підключення замка максимально простим і не вимагати від користувача системного підтвердження ОС смартфона, виробники нерідко вимикають стандартне спарювання канального рівня (*LE Secure Connections*) і реалізують власні протоколи шифрування безпосередньо в коді GATT-характеристик застосунку.

Показовим прикладом такої помилки є вразливості CVE-2023-7003 та CVE-2023-7009, виявлені в прошивках платформи Sciener / TTLock (базовий OEM-модуль, інтегрований у понад 100 брендах смарт-замків по всьому світу) [4]:

1. Статичне повторне використання ключів (CVE-2023-7003): Замість динамічного узгодження сесійних ключів за допомогою ECDH розробник використав один статичний ключ AES, який був вбудований у код мікропрограми. Якщо зловмисник зможе отримати цей ключ із одного замка або Android-застосунку за допомогою реверс-інжинірингу, він зможе використати його для отримання несанкціонованого доступу до інших замків того самого виробника в зоні дії радіосигналу. Це також означає, що компрометація ключа не обмежується одним конкретним пристроєм. При цьому для проведення атаки спочатку необхідно отримати сам криптографічний ключ.

2. Помилка під час дешифрування (CVE-2023-7009): Функція дешифрування AES неправильно перевіряє довжину вхідного буфера. Якщо пакет містить менше 16 байтів, дешифрування не виконується, але система все одно передає отримані дані на подальшу обробку як коректну команду. Ця вразливість є особливо небезпечною, оскільки для атаки не потрібно

отримувати ключ шифрування або проходити авторизацію. Зловмиснику достатньо надіслати через BLE коротку незашифровану команду, яку система може сприйняти як команду на відкриття замка.

Для порівняльного аналізу обрано поширені технології розумного будинку з різними підходами до безпеки. BLE є основним об'єктом дослідження завдяки прямому підключенню до смартфона без шлюзу, але дозволяє використовувати власні механізми криптографії. Zigbee 3.0 використовує mesh-архітектуру та централізоване керування ключами через Trust Center. Matter over Thread застосовує стандартизовані механізми PASE і CASE [6]. NFC розглядається як локальна технологія короткої дії, яка може використовувати захищені чипи з апаратною криптографією.

Для комплексної оцінки доцільності вибору тієї чи іншої технології необхідно враховувати як параметри інформаційної безпеки та енергоефективності, так і фінансові витрати виробника та кінцевого користувача. Зведені дані наведено в таблиці 1.

Таблиця 1 – Техніко-економічне порівняння технологій для бездротових смарт-замків

| **Критерій порівняння** | **Bluetooth Low Energy (BLE 5.3/6.0)** | **Zigbee 3.0 (IEEE 802.15.4)** | **Matter over Thread (Ipv6 / 802.15.4)** | **Near Field Communication (NFC)** |
|---|---|---|---|---|
| Базове шифрування | AES-128-CCM | AES-128-CCM | DTLS 1.3 / CASE | ISO/IEC 14443-A (AES-128) |
| Стійкість до вендорських помилок | Низька | Середня | Найвища | Висока |
| Приватність IP-адреси | Resolvable Private Address | Статична 64-бітна адреса | Тимчасові IPv6-адреси | Рандомізований UID |
| Захист від статичних ключів CVE-2023-7003 | Вразливий через однаковий ключ у прошивці | Захищений завдяки оновленню ключів через Trust Center | Захищений завдяки унікальним ключам для кожної сесії | Стійкий завдяки зберіганню ключів у захищеному чипі |
| Стійкість до CVE-2023-7009 (обхід шифрування) | Вразливий через виконання коротких команд без шифрування | Захищений завдяки апаратній перевірці цілісності пакетів | Захищений завдяки обов'язковій перевірці розміру даних | Стійкий завдяки апаратному контролю формату команд |

Зіставлення результатів таблиці 1 показує суттєві відмінності між бездротовими технологіями за рівнем захисту та вартістю реалізації. Для BLE

основною проблемою є залежність безпеки від реалізації виробника: використання власної криптографії може призводити до вразливостей, що підтверджується CVE-2023-7003 [4] та CVE-2023-7009 [5]. У Zigbee 3.0 захист доповнюється механізмом Trust Center, оновленням ключів та перевіркою цілісності пакетів. Matter over Thread використовує PASE та CASE [6], а також унікальні ключі для сесій, що зменшує ризик повторного використання одного ключа. NFC забезпечує локальну взаємодію та може використовувати захищене зберігання ключів в апаратному чипі.

За техніко-економічними показниками BLE має нижчу вартість чипсета – до $1,80 – та не потребує окремого шлюзу для взаємодії зі смартфоном. Для Matter вартість чипсета становить близько $4,80, а для роботи Thread може знадобитися Thread Border Router. Тому BLE є простішим для реалізації автономних смарт-замків, але його безпека значною мірою залежить від правильності реалізації додаткових механізмів захисту. Zigbee, Matter та NFC потребують більшої уваги до інфраструктури або апаратної частини, але використовують додаткові механізми контролю ключів, цілісності та автентифікації.

Для підвищення захисту BLE доцільно використовувати стандартні механізми LE Secure Connections замість власних криптографічних рішень виробника.

Додатковим заходом може бути апаратна автентифікація через NFC, що дозволяє посилити початкову перевірку користувача та зменшити залежність системи від програмної реалізації криптографії.

Таким чином, під час вибору технології для смарт-замка необхідно враховувати не лише вартість чипсета, а й використані механізми керування ключами, перевірки команд та необхідну інфраструктуру.

**Список літератури**

1. Padgette J., Scarfone K., Chen L. Guide to Bluetooth Security. *NIST Special Publication 800-121*, Rev. 2. 2017. 60 p. DOI: https://doi.org/10.6028/NIST.SP.800-121r2

2. Тарасов А.С. Аналіз методів забезпечення інформаційної безпеки в IoT мережах. ХНУРЕ, 2021. Вип. 204. С. 138–147. URI: https://openarchive.nure.ua/handle/document/20849

3. Bluetooth Core Specification v6.0 (Channel Sounding). Kirkland : Bluetooth Special Interest Group (SIG), 2024. 412 p.

4. National Vulnerability Database. CVE-2023-7003 Detail: Cryptographic Issues in Sciener TTLock Firmware. NIST, 2023. URL: https://nvd.nist.gov/vuln/detail/CVE-2023-7003

5. National Vulnerability Database. CVE-2023-7009 Detail: Incomplete AES Decryption Validation in Sciener TTLock. NIST, 2023. URL: https://nvd.nist.gov/vuln/detail/CVE-2023-7009

6. Matter Core Specification Version 1.2. Davis : Connectivity Standards Alliance (CSA), 2023. 1148 p.