УДК 621.396.42
DOI https://doi.org/10.32838/2663-5941/2022.4/06

Гарист А.В.
Український науково-дослідний інститут спеціальної техніки та судових експертиз
Служби безпеки України

АНАЛІЗ ВРАЗЛИВОСТЕЙ ТЕХНОЛОГІЇ BLUETOOTH

В області телекомунікацій технологія Bluetooth є техніко-промисловим стандартом передачі даних для персональних бездротових мереж (Wireless personal area network, WPAN). Ця технологія забезпечує стандартний, економічний та безпечний спосіб обміну інформацією між різними пристроями за допомогою безпечної радіочастоти ближньої дії. Разом з розвитком технології розвивалися також і кіберзагрози. У 2010-х роках були виявлені перші вразливості технології Bluetooth, які дозволяли отримати контроль над пристроєм.

Bluetooth-пристрої оточують нас повсюди, це колонки, розумні годинники, фітнес-браслети та навушники. У зв'язку із цим функція Bluetooth на пристрої залишається завжди активною. Пристрої обмінюються даними між собою, завантажуючи якусь частину в додатки. У той же час Bluetooth-з'єднання дуже вразливе і може стати причиною зламу пристрою. Це дозволяє завантажити шкідливі програми та відстежувати не тільки місцезнаходження власника, але й читати особисте листування, дані банківських карт та облікових записів.

Bluetooth корисний у повсякденному житті, але досить вразливий, як і Wi-Fi підключення. Зловмисники використовують спеціальні програми, які допомагають знайти активні Bluetooth-з'єднання поблизу. Вони не тільки бачать, хто є поруч, але й можуть відстежувати, до яких пристроїв та мереж пристрій підключався раніше. Це досить серйозно, адже пристрій розглядає ці підключення як довірені та підключається до них автоматично, коли вони поряд.

В даній статті представлені результати аналізу вразливостей протоколу Bluetooth. Зазвичай атаки на пристрої відбуваються в людних місцях. Шахраї заздалегідь прораховують план дій і готують пристрій, з якого планується злам. Для цього підходить скинутий до заводських налаштувань планшет або смартфон. Отримані дані можуть бути використані для шантажу або зламу банківських облікових записів. З кожним роком доступних пристроїв стає дедалі більше, а зловмисники вигадують нові способи зламу.

Ключові слова: *Bluetooth-з'єднання, вразливість, злам, протокол, аутентифікація, шифрування.*

Постановка проблеми. Стандарт Bluetooth, включаючи його недавню еволюцію – Bluetooth Low Energy (BLE), продовжує використовуватись на великій кількості пристроїв. З багатьох стандартів зв'язку для з'єднання двох пристроїв Bluetooth характеризується простотою використання та великими можливостями.

Незважаючи на те, що для передачі даних в основному використовується технологія Wi-Fi, яка використовує свої протоколи шифрування, проблеми безпеки технології Bluetooth будуть залишатися актуальними ще довгий час, так як вона використовується на мільярдах пристроїв усіх типів. В статті розглянуті вразливості цієї технології, а також опис можливих атак, надані приклади застосування цих вразливостей.

Аналіз останніх досліджень і публікацій. Перший злам Bluetooth-пристрою здійснив громадянин Великобританії Оллі Уайтхаузу у квітні 2004 року. Запропонована ним методика мала серйозний недолік, злам ставав можливим лише в тому випадку, якщо зловмисник отримував можливість перехопити два пристрої безпосередньо перед їхньою першою взаємодією один з одним – процедурою з'єднання, при якій вони обмінюються ідентифікаційною інформацією. Якщо перше з'єднання було встановлено поза межами досяжності зловмисника, подальший обмін даними між двома пристроями ризику не представляв.

У 2017 році компанія Armis виявила так звану вразливість BlueBorne, яка торкнулася пристроїв з Bluetooth з'єднанням на операційних системах Android, iOS, Linux і Windows. Було підраховано, що на той час потенційно вразливих пристроїв становить близько 8,2 мільярди.

Дослідники з німецької компанії ERNW (Enno Rey Netzwerke), виявили вразливість у Bluetooth на Android-пристроях. Експлуатація вразливості дозволяє зловмиснику, який знаходиться в радіусі дії Bluetooth, отримувати доступ до даних, що зберігаються на пристрої, а також робить мож-

ливим завантаження шкідливого програмного забезпечення, причому без будь-яких дій з боку жертви. Цю вразливість було виявлено в листопаді 2019 року, після чого дослідники повідомили про неї розробників із компанії Google. Зрештою, проблема була вирішена у лютневому оновленні безпеки для платформи Android.

У серпні 2021 року група дослідників безпеки опублікувала докладну інформацію про набір з 16 вразливостей, які впливають на стек програмного забезпечення Bluetooth. Ці вразливості стали відомі під загальною назвою BrakTooth та дозволяють зловмисникам виводити з ладу пристрої або запускати шкідливий код і захоплювати цілі системи.

Водночас, незважаючи на значну кількість наукових публікацій, присвячених проблемам вразливостей технології Bluetooth, стрімкий розвиток технологій зумовлює потребу подальших досліджень цієї тематики.

Постановка завдання. Метою даної статті є аналіз вразливостей технології Bluetooth в режимі реального часу і виявлення нелегітимної активності з можливістю блокування несанкціонованих повідомлень або оповіщення. Метою аналізу є своєчасне виявлення потенційних загроз і реагування на них, не надаючи негативного впливу на функціонування мережі.

Виклад основного матеріалу дослідження

Bluetooth – це технологія бездротового зв'язку малого радіусу дії, яка дозволяє здійснювати обмін даними між фіксованими та мобільними пристроями. З швидким розвитком Інтернету речей (IoT) технологія Bluetooth також прискорила темпи свого розвитку, щоб адаптуватися до ринку, що постійно зростає і потреб користувачів. Розробники постійно працюють над збільшенням швидкості передачі даних, щоб технологія Bluetooth могла краще інтегруватися до різних пристроїв IoT.

Розглянемо процедуру встановлення з`єднання за технологією Bluetooth.

Процедуру встановлення з'єднання або інакше кажучи ініціалізацію з'єднання Bluetooth можна розділити на три етапи:

– генерація ключа Kinit;
– генерація ключа зв'язку – link key;
– аутентифікація.

Етапи генерації ключів Kinit та link key входять до процедури з'єдання. Під час цієї прицедури відбувається процес зв'язку двох (або більше) пристроїв з метою створення загального секретного значення Kinit, яке вони будуть використовувати при спілкуванні. Перед з'єднанням з обох боків необхідно ввести PIN-код. Kinit формується за алгоритмом E22, який оперує наступними величинами:

– BD_ADDR – унікальна адреса Bluetooth-пристрою (довжина 48 біт);
– PIN-код та його довжина;
– IN_RAND (довжина 128 біт).

Для створення ключа зв'язку пристрої обмінюються 128-бітними словами LK_RAND(A) і LK_RAND(B), що генеруються випадковим чином. Далі йде побітова операція XOR із ключем ініціалізації Kinit і знову обмін отриманим значенням. Потім обчислюється ключ за алгоритмом E21.

На даному етапі процедура з'єднання закінчується і починається останній етап ініціалізації Bluetooth – взаємна аутентифікація, яка заснована на схемі запит-відповідь. Один із пристроїв стає верифікатором, генерує випадкову величину AU_RAND(A) і надсилає його сусідньому пристрою. Як тільки пред'явник одержує це «слово», починається обчислення величини SRES за алгоритмом E1 і відправляється назад верифікатору. Сусідній пристрій здійснює аналогічні обчислення та перевіряє відповідь пред'явника. Після чого процедуру встановлення з'єднання вважатиметься закінченою.

В технології Bluetooth для захисту з'єднання передбачені деякі механізми, такі як шифрування даних та авторизація пристроїв. Також алгоритм псевдовипадкового переналаштування робочої частоти (Frequency Hopping Spectrum Spreading – FHSS), на основі якого працює Bluetooth, входить в систему захисту конфіденційності при передачі інформації: перехід між несівними частотами відбувається за псевдовипадковим алгоритмом і визначається індивідуально для кожного з'єднання. Шифрування в Bluetooth відбувається за допомогою ключа, ефективна довжина якого – від 8 до 128 біт. Це дозволяє встановлювати рівень стійкості результуючого шифрування, що відповідає законодавству кожної країни. Тому правильно налаштовані Bluetooth-пристрої спонтанно з'єднуватися не можуть і тому випадкових витоків інформації до сторонніх осіб статися не може.

Класична технологія Bluetooth може працювати в одному з чотирьох режимів безпеки:

Режим 1 – (не захищений) зазвичай використовується за замовчуванням. У цьому режимі не використовується ні шифрування, ні аутентифікація, а сам пристрій працює в широкомовному режимі. Найчастіше використовується лише для тестування. Існує для підтримки зворотної сумісності із застарілими пристроями.

Режим 2 – захищений на рівні програми/служби. У цьому режимі після встановлення з'єднання менеджер безпеки здійснює аутентифікацію, що дозволяє обмежити доступ до пристрою.

Режим 3 – захищений лише на рівні каналу зв'язку. В даному випадку аутентифікація проводиться до встановлення з'єднання, при цьому застосовується прозоре шифрування, але навіть за такого режиму пристрій може бути зламаний.

Режим 4 – це удосконалений режим безпеки 2. Функції безпеки реалізуються після встановлення з'єднання. Для того, щоб згенерувати ключ з'єднання використовується протокол Діффі-Хеллмана на еліптичних кривих (Elliptic curve Diffie–Hellman, ECDH).

У всіх специфікаціях Національний інститут стандартів та технологій США (NIST) рекомендує використання саме режиму 4. Основою захисту з'єднання є процедура генерації ключів при встановленні з'єднання.

Розглянемо основні найбільш розповсюджені методи атаки, якими активно користуються зловмисники.

Bluejacking – атака, під час якої шахрай використовує з'єднання для проникнення в телефон та надсилання анонімних повідомлень на інші пристрої, що знаходяться поблизу. Такі атаки можуть використовуватись для дорогих дзвінків до інших країн.

Bluesnarfing – злам, що супроводжується крадіжкою конфіденційної інформації, наприклад інтернет-акаунтів, фотографій та відео. Дана атака переважно використовує недоліки в програмному забезпеченні пристроїв.

Bluebugging – найгірший варіант, при якому зловмисник має можливість контролювати пристрій, прослуховувати смартфон і отримувати доступ до всіх даних, які є в його пам'яті. Спочатку bluebugging був зосереджений на підслуховуванні чи прослуховуванні комп'ютера з підтримкою Bluetooth. Зі зростанням використання смартфонів кіберзлочинці переключилися на злам мобільних телефонів. Ця атака часто обмежена через діапазон Bluetooth-з'єднання, що досягає всього 10–15 метрів. Деякі зловмисники використовують антени-підсилювачі для розширення діапазону атаки.

Btlejacking – це відносно нова техніка, яка дозволяє зловмисникам заблокувати та взяти під контроль будь-який пристрій Bluetooth з низьким енергоспоживанням (BLE).

Blueprinting – атака, яка дозволяє отримати детальну інформацію про віддалений пристрій. Як уже зазначалося раніше, кожен Bluetooth-пристрій має унікальну Bluetooth-адресу. Ця адреса складається з 6 байт і зазвичай представляється, подібно до MAC-адреси, у форматі MM:MM:MM:XX:XX:XX. Перші три байти, зазначені як M, містять відомості про виробника мікросхеми. На жаль, з трьома байтами X, що залишилися, не все так просто, і модель пристрою не можна визначити однозначно. Проте, кожен Bluetooth-пристрій надає ті чи інші послуги. Які саме можна дізнатися через SDP (Service Discovery Protocol). На запит про сервіси можна отримати інформацію певного формату, а на основі відповіді можна обчислити конкретну модель пристрою.

DoS-атаки із застосуванням BSS (Bluetooth Stack Smasher). В даному методі атаки використовується неправильно сформовані L2CAP (Logical Link Control and Adaptation Protocol) пакети даних для реалізації зависання, вимкнення, перезавантаження пристрою, що атакується.

Влітку 2019 року експерти CISPA (Cyber Intelligence Sharing and Protection Act) та компанії-члени ICASI (Industry Consortium for Advancement of Security on the Internet) – Microsoft, Apple, Intel, Cisco та Amazon скоординовано розкрили інформацію про нову Bluetooth-вразливість, що отримала назву KNOB (Key Negotiation of Bluetooth). Проблема торкається Bluetooth BR/EDR (він же Bluetooth Classic) і дозволяє зловмисникам ефективно скоротити довжину ключа шифрування, що використовується під час з'єднання пристроїв. В результаті зловмисник може здійснювати моніторинг або маніпулювати трафіком, що передаються між двома пристроями.

В грудні 2019 року цими ж експертами знайдено нову проблему в протоколі Bluetooth, що отримала назву BIAS (Bluetooth Impersonation AttackS). Корінь нової проблеми BIAS полягає в тому, як пристрої з підтримкою Bluetooth обробляють ключ зв'язку (link key). Цей ключ генерується, коли два Bluetooth-пристрої вперше з'єднуються. По суті вони "домовляються" про довгостроковий ключ, який будуть використовувати для отримання ключів сесій у майбутньому, щоб не змушувати власників пристроїв щоразу знову проходити тривалий процес з'єднання. Дана вразливість дозволяє зловмиснику видати себе за раніше з'єднаний пристрій, пройти аутентифікацію і підключитися до іншого пристрою, не знаючи ключа зв'язку, який раніше було встановлено між ними.

1 вересня 2019 року дослідники з Сінгапурського університету технологій та дизайну опублікували інформацію про 20 вразливостей, виявлених у поширених bluetooth-чіпах різних виробників, які отримали назву Braktooth. Всі вразливості можна експлуатувати без попередньої авторизації, в більшості випадків досить перебувати неподалік пристрою, який атакується, але необхідно також знати його унікальну адресу (BD_ADDR). Наслідки – від тимчасового збою в роботі мікросхеми до повного зависання, яке усувається тільки перезавантаженням пристрою. У найскладнішому випадку дослідники реалізували виконання коду, що міститься у прошивці, за довільною адресою.

У 2020 році фахівцями з Федеральної політехнічної школи Лозанни та Університету Пердью було виявлено вразливість під назвою Blurtooth у компоненті стандарту CTKD (Cross-Transport Key Derivation), яка дозволяє зловмисникам перехоплювати ключі аутентифікації. Дана вразливість діє на пристрої, які використовують стандарт Bluetooth з 4.0 до 5.0.

Компонент CTKD використовується для узгодження та налаштування ключів аутентифікації при з'єднанні двох пристроїв. Він працює шляхом налаштування двох різних наборів ключів аутентифікації для стандартів BLE (Bluetooth Low Energy) та BR/EDR (Basic Rate/Enhanced Data Rate). Роль CTKD полягає в тому, щоб підготувати ключі та дозволити пристроям вирішити, яку версію стандарту Bluetooth вони хочуть використовувати. Зловмисники можуть маніпулювати компонентом CTKD, щоб перезаписати ключі аутентифікації Bluetooth на пристрої, та отримати доступ до інших служб та програм з підтримкою Bluetooth на ньому. У деяких версіях атаки Blurtooth ключі аутентифікації повністю перезаписували, а в інших просто змінювали версію для використання слабкого шифрування.

У 2019 році дослідники виявили іншу вразливість у Bluetooth-протоколі. З'ясувалося, що специфікації BR/EDR дозволяють зламати зашифровані повідомлення через Bluetooth. Для цього зловмиснику потрібно просто зайти до зони покриття пристроїв. Вразливість містилася у можливості Bluetooth-пристроїв самостійно призначати довжину ключа для шифрування інформації.

Одна з головних відмінностей версії Bluetooth 5.0 від попередніх – здатність обробляти вчетверо більше даних за рахунок підвищення швидкості передачі. Вона була збільшена до 2 Мбіт/с, причому дальність для підключення зросла до 200 м на відкритій місцевості.

Стандарт Bluetooth 5.1 вже має функції, які можна активувати, щоб запобігти атакам Blurtooth. Для інших версій патчів поки немає, а єдиним способом захисту від атак є контроль середовища, в якому з'єднані пристрої.

13 липня 2021 року було прийнято базові специфікації технології Bluetooth 5.3, де для захисту з'єднання було поліпшено керування розміром ключа шифрування. Так як Bluetooth BR/EDR розміри ключа шифрування узгоджуються контролерами у підключених пристроях, ця зміна дозволяє хост-пристрою повідомити свого контролера Bluetooth BR/EDR мінімально допустимий розмір ключа за допомогою інтерфейсу хост-контролера (HCI). Це вдосконалення також підвищує ефективність, з якою контролери Bluetooth BR/EDR можуть інформувати хост-пристрій про результати узгодження довжини ключа.

Враховуючи вище викладене, опишемо одні з найголовніших рекомендацій від NIST для профілактики запобігання зламу при використанні з'єднання Bluetooth.

Необхідно встановлювати пристрої Bluetooth на найнижчий і достатній рівень потужності, щоб радіус сигналу залишався в захищеному периметрі. Справа в тому, що встановлення пристроїв Bluetooth з мінімальним необхідним та достатнім рівнем потужності дозволяє забезпечити безпечний доступ авторизованим користувачам.

Не можна використовувати режим з'єднання "Just Works", в якому відсутня безпека та аутентифікація, для пристроїв Bluetooth 2.1 та вище і використовують звичайне захищене з'єднання SSP (Secure Simple Pairing). При створенні пари в режимі "Just Works" немає гарантій захисту від атаки типу «людина всередині» (Man in the middle – MITM).

Необхідно встановлювати PIN-коди, які є досить випадковими, довгими та приватними. Довгі PIN-коди набагато стійкіші до атак за методом "грубої сили" (brute-force).

Пристрої Bluetooth повинні бути налаштовані за замовчуванням, як "не видимі", за винятком випадків, коли це необхідно для з'єднання. У цьому режимі Bluetooth пристрій приховано від інших пристроїв.

Також необхідно використовувати шифрування з'єднання. Без використання шифрування з'єднання відкрито для прослуховування.

Виконуйте з'єднання якомога рідше, в ідеальному випадку в безпечній зоні, де зловмисники не можуть перехопити кадри з обміном ключами

доступу під час з'єднання. У випадку, якщо зловмисник зможе отримати деякі кадри пов'язані з аутентифікацією з'єднання, виникає ризик зламу ключа.

Висновки. Використання технології Bluetooth відкриває великі можливості для використання бездротових технологій, але варто пам'ятати, що поряд з цим відкриваються все більше потенційних загроз як для витоку конфіденційної інформації, так і для зламу та віддаленого доступу до чужого обладнання. Тому для профілактики таких загроз варто дотримуватись рекомендацій NIST щодо використання технології Bluetooth.

Список літератури:

1. Matheus E. Garbelini, Sudipta Chattopadhyay, Vaibhav Bedi, Sumei Sun, Ernest Kurniawan (2021), Braktooth: Causing Havoc on Bluetooth Link Manager, URL: https://asset-group.github.io/disclosures/braktooth/
2. Key Negotiation of Bluetooth Attack: Breaking Bluetooth Security, URL: https://knobattack.com/
3. BlueBorne vulnerabilities impact Amazon Echo and Google Home, URL: https://www.armis.com/research/blueborne/

Haryst A.V. BLUETOOTH TECHNOLOGY VULNERABILITY ANALYSIS

In the field of telecommunications, Bluetooth technology is the technical and industrial standard for data transmission for personal wireless networks (Wireless personal area network, WPAN). This technology provides a standard, cost-effective, and secure way to exchange information between different devices using a secure, short-range radio frequency. As technology has evolved, cyber threats have also evolved. In the 2010s, the first vulnerabilities in Bluetooth technology were discovered, allowing to gain control over the device.

Bluetooth devices surround us everywhere, these are speakers, smart watches, fitness bracelets and headphones. Therefore, the Bluetooth function on the device remains always active. Devices exchange data with each other, loading some part into applications. At the same time, the Bluetooth connection is very vulnerable and can cause the device to be hacked. This allows you to download malware and track not only the location of the owner, but also read personal correspondence, bank card and account data.

Bluetooth is useful in everyday life, but is quite vulnerable, like a Wi-Fi connection. Attackers use special applications that help to find active Bluetooth connections nearby. They not only see who is nearby, but they can also track which devices and networks the device has previously connected to. This is serious enough, because the device considers these connections as trusted and connects to them automatically when they are nearby.

This article presents the results of the vulnerability analysis of the Bluetooth protocol. Typically, attacks on devices occur in crowded places. Fraudsters calculate the action plan in advance and prepare the device from which they plan to hack. A factory reset tablet or smartphone is suitable for this. The data obtained can be used to blackmail or hack bank accounts. Every year there are more and more available devices, and attackers come up with new ways to hack.

Key words: *Bluetooth-connection, vulnerability, hacking, protocol, authentication, encryption.*