DOI: https://doi.org/10.36910/6775-2524-0560-2022-49-02
УДК 004.056
Тогоєв Олексій Романович, аспірант.
https://orcid.org/0000-0003-3465-7767
Чорноморський національний університет імені Петра Могили, м. Миколаїв, Україна

МЕТОД ДЕАНОНІМІЗАЦІЇ КОРИСТУВАЧІВ IOS ЧЕРЕЗ ПРОТОКОЛ AIRDROP

Тогоєв О.Р. Метод деанонімізації користувачів iOS через протокол Airdrop. У статті запропоновано алгоритм відстеження для пристроїв iOS, які використовують динамічно рандомізовані MAC-адреси та Advertising-повідомлення під час зв'язку за стандартом BLE.
Ключові слова: iOS, BLE, рандомізована MAC-адреса, Advertising-повідомлення, визначення місцезнаходження смартфона

Tohoiev O.R. A method for deanonymizing iOS users through the Airdrop protocol. The paper proposes a tracking algorithm for iOS devices using dynamically randomized MAC addresses and BLE advertisements.
Keywords: iOS, BLE, randomized MAC address, Advertising messages, definition of smartphone location

Постановка наукової проблеми.

Технологія Bluetooth сприяла поширенню миттєвого бездротового підключення, починаючи від особистих підключених аксесуарів, закінчуючи розумними будинками, локалізованим та персоналізованим досвідом покупок на основі розташування. З моменту своєї першої появи в мобільних телефонах в 2000 році, Bluetooth зазнав п'яти основних специфікацій, редакцій з численними поправками [1].

У ранніх версіях специфікації Bluetooth постійна Bluetooth MAC-адреса пристроїв регулярно транслювалася у відкритому вигляді, що викликало серйозні побоювання з приводу конфіденційності через можливість небажаного відстеження. Це було вирішено у базовій специфікації Bluetooth 4.0 із введенням стандарту Bluetooth Low Energy (BLE), також відомого як Bluetooth Smart. BLE дозволяє виробникам пристроїв використовувати тимчасові випадкові адреси бездротового зв'язку замість їх постійної адреси для запобігання відстеження [2]. Однак ці функції анонімізації визначаються таким чином, що залишають виробникам певний ступінь гнучкості. Необов'язковість таких функцій захисту конфіденційності має особливе значення, оскільки стандарт BLE був розроблений спеціально для підтримки пристроїв з низьким енергоспоживанням, таких як смарт-годинник та інші пристрої, що носяться, і є привабливою метою для ворожого відстеження своїх користувачів.

Пристрої BLE транслюють так званий "Advertising" на незашифровані загальнодоступні канали, щоб сигналізувати про свою присутність іншим пристроям [3]. Термін "advertising" з англійської перекладається як "рекламний". Однак це не є точним технічним описом процесу. Застосовують також і термін "широкомовні пакети". Він також не точним, але загально зрозумілий. З метою дотримання максимальної точності, на наш погляд, можна уживати термін без перекладу.

Описана вище публічна трансляція містить всю необхідну інформацію для виконання функції пристрою, не допускаючи витоку непотрібної особистої інформації про пристрій або його користувача. У деяких випадках, однак, пристрої можуть передавати дані, які розкривають конфіденційну інформацію про них самих або навіть про інші пристрої. Дослідженню таких випадків присвячена публікація.

Аналіз досліджень.

Проблеми з конфіденційністю та безпекою Bluetooth акцентуються та вивчаються дослідниками та практиками з моменту його появи. Анонімізація пристроїв у загальнодоступних каналах зв'язку стала доступною лише з впровадженням BLE у Bluetooth 4.0. Багато досліджень ефективності рандомізації MAC-адрес зосереджені на Wi-Fi, де вирішення проблеми конфіденційності аналогічне та існує проблема широкомовних постійних ідентифікаторів.

Однак, вирішення проблеми вразливості, яке пропонується для Wi-Fi, нелегко перенести на Bluetooth, оскільки вони засновані на різних технологіях та сферах і залежить від мережевого стека Wi-Fi. Тому відстеження Bluetooth та Wi-Fi здійснюється методам та утилітам, специфічним для BLE.

Існує кілька методів прослуховування зв'язку Bluetooth 2.0 з використанням Bluetooth-сніфера на основі GNU Radio та програмно-визначеного радіообладнання USRP [4]. Такі підходи

засновані на перехопленні пакетів і реінжинірингу всіх параметрів, необхідних для підслуховування зв'язку засобами Bluetooth. Проте, висновки, що стосуються реалізації Bluetooth 2.0, втратили актуальність з появою BLE та Bluetooth 5.

У 2015 році M. I. Jameel та J. Dungen представили бібліотеку з відкритим вихідним кодом для сканування Bluetooth Low Energy (LE) та активними широкомовними пакетами RFID [5]. Їхня робота узагальнює різні доступні протоколи Beacon, які використовують широкомовні протоколи на основі близькості та дозволяють всі види локалізованих взаємодій зі смартфонами та іншими пристроями Bluetooth через широкомовні канали BLE. Крім того, автори опублікували бібліотеку під назвою advlib, яка обробляє необроблені Advertising-повідомлення BLE і декодує їх у формат відкритих даних. Ця бібліотека дозволяє розробникам програмного забезпечення легко інтегрувати Advertising-функції BLE в їх програмне забезпечення без необхідності декодувати вручну низькорівневі протоколи. Бібліотека також підтримує "колаборативний репозиторій" з відкритим вихідним кодом Sniffypedia, який представляє велику кількість загальновідомих Advertising-ідентифікаторів BLE у зручному для пошуку та доступному форматі. Ця платформа може допомогти класифікувати класи пристроїв Bluetooth для розвідувальних цілей, але пристрій не пропонує можливості відстеження.

Використовуються також методи отримання доступу до постійних MAC-адрес шляхом використання запитів у Wi-Fi [6]. Такі алгоритми залежать від часових характеристик та знайдених порядкових номерів у запитах перевірки Wi-Fi для ідентифікації пристроїв незалежно від своєї MAC-адреси. Також вони описують варіант так званої "кармічної атаки", використовуючи той факт, що багато пристроїв надаватимуть інформацію нібито відомим та довіреним мережам шляхом створення універсального доступу. Часто подання своєї постійної MAC-адреси відбувається у довіреному контексті.

Незважаючи на наявність рандомізації MAC-адрес із збереженням конфіденційності в Bluetooth 4.0 LE, не всі пристрої використовують цю функціональність і, отже, уразливі для відстеження. Крім того, зловмисне розповсюдження відповідного програмного забезпечення для відстеження серед кількох мобільних пристроїв – "BLE Botnet" – розширює можливості відстеження далеко за межами локальної дальності передачі звичайного Bluetooth-зв'язку.

Рандомізація MAC-адрес часто зазнає невдачі через неправильну або послідовну реалізацію, частково засновану на попередніх підходах. Крім того, недоліки рандомізації адрес Android-телефонів полягають у тому, що можливо зробити висновок про типи пристроїв через префікси адрес, а також їх глобальні MAC-адреси через інформацію, знайдену у широкомовних атрибутах WPS. Також атака контрольного кадру ефективно розкриває постійну MAC-адресу Wi-Fi пристрою.

Виділення раніше невирішених питань.

Незважаючи на наявність ґрунтовних розробок, недостатньо дослідженим залишається поєднання конфіденційності BLE з поняттям потенційно глобального ботнету, яке розширює загрозу конфіденційності з боку локального виявлення присутності для відстеження місцезнаходження цільових користувачів серед великої кількості пристроїв.

У той час, як більшість наведених досліджень зосереджені на визначенні пристроїв, які використовують статичні адреси, доцільно зупинитися на відстеженні пристроїв, які використовують динамічно рандомізовані адреси. Ці адреси змінюються залежно від параметрів регенерації, встановлених виробниками. Підхід, запропонований нижче, не отримує інформацію через звернення хешей або інших методів зворотного проектування, а використовує повністю пасивне сніф-«вивчення» для отримання інформації, яка дозволить відстеження пристрою. Метод заснований на вилученні ідентифікуючих токенів з корисного навантаження Advertising-повідомлень та використовує певні функції Bluetooth. Цим він відрізняється від описаних іншими дослідниками.

Формулювання мети і завдань дослідження.

Метою статті є висвітлення можливостей деанонімізації користувачів за допомогою використання вразливості Airdrop-технології обміну файлами між пристроями Apple без підключення до Інтернету – та демонстрація того, що така вразливість стосується всіх девайсів на платформі iOS.

Методи.

Спочатку необхідно виявити різні типи Advertising-пакетів та показати так звані ідентифікаційні токени, які є унікальними для пристроїв і залишаються незмінними протягом

достатньо тривалого часу, щоб слугувати вторинними ідентифікаторам. Також розроблено онлайн-алгоритм, який використовує незмінність ідентифікаційних токенів та випадкових адрес, щоб синхронно, постійно перевіряти пристрій, незважаючи на впровадження заходів анонімізації. Такий підхід може бути застосований до усіх Windows 10, iOS та пристроїв MacOS. Алгоритм не вимагає розшифровки повідомлень або порушення безпеки Bluetooth. Він повністю заснований на загальнодоступному незашифрованому Advertising-трафіку.

Виклад основного матеріалу й обґрунтування отриманих результатів дослідження.

Airdrop-технологія дозволяє обмінюватися файлами між пристроями Apple без підключення до Інтернету. AirDrop використовує Bluetooth для створення одноранговоі мережі Wi-Fi між пристроями. При цьому повинні бути включені і Wi-Fi, і Bluetooth. Відстань між пристроями має не перевищувати 9 метрів. Коли AirDrop включений, він запускає Bluetooth для пошуку інших пристроїв iOS з підтримкою AirDrop, що знаходяться поблизу. В момент активування AirDrop, пристрій починає відправляти Advertising-пакети BLE.

Advertising-пакети BLE є одним із найважливіших аспектів Bluetooth Low Energy. Вони допомогають знизити енергоспоживання, пришвидшити з'єднання та підвищити надійність. BLE Advertisements також є ключем до маяків, які допомагають визначити місцезнаходження та здійснювати відстеження.

Bluetooth Low Energy або також Bluetooth Smart має два способи зв'язку. Перший — це використання advertising-повідомлень, коли периферійний пристрій BLE транслює пакети на всі пристрої навколо нього. Пристрій-одержувач може діяти на основі цієї інформації або підключитися, щоб отримати додаткову інформацію. Отже, перший спосіб — це принцип маяка — проста передача пакетів. Другий спосіб зв'язку полягає в отриманні пакетів за допомогою з'єднання, де як периферійний, так і центральний пристрій надсилають пакети. Проаналізуємо, як працюють Advertising-повідомлення.

1. Користувач не може встановити з'єднання між двома пристроями без використання Advertising-повідомлення.
2. Велика кількість продуктів BLE «спить» більшу частину часу, прокидаючись лише для Advertising-повідомлень та підключення, коли це необхідно.
3. Користувачам потрібні адаптивні продукти, а інтервал транслювання Advertising-повідомлень має вирішальне значення для швидких з'єднань.
4. Advertising-оголошення є основою маяків iBeacon, EddyStone та інших, тому вони використовуються постійно.

Advertising-оголошення за задумом односпрямовані. Центральний пристрій не може надсилати дані на периферійний пристрій без підключення.

В кожному Advertising-пакеті є такі дані користувача:

- номер телефона;
- AppleId;
- Email;
- OS;
- ім'я пристрою;
- інше.

Ці конфіденційні дані Advertising-пакеті захешовані зазвичай за допомогою SHA-256 (рис. 1).

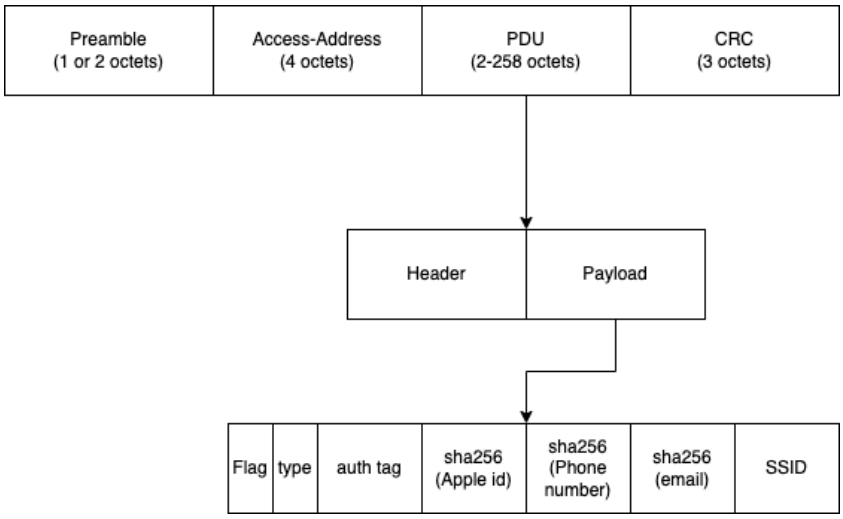

Рис. 1. Структура Advertising-пакета

Продемонструємо роботу розробленого алгоритму на прикладі визначення користувача мобільної системи України. База даних, що зберігає інформацію про кожного користувача мережі стільникового зв'язку, має абревіатуру HLR (англ. *The Home Location Register*). HLR зберігає інформацію про статус послуг, що пов'язані з певною SIM-карткою. Кожна картка має унікальний номер, IMSI, що використовується як ключ для HLR. В цій базі зберігається наступна інформація про абонента:

- номер телефону (MSISDN) абонента, що пов'язаний з даною SIM-карткою;
- GSM-сервіси, що доступні користувачеві;
- місце знаходження користувача (VLR та SGSN);
- налаштування переадресації;

Відомо, що всі номери в Україні починаються з +38, таким чином, з 13 символів залишиться 10. Але також відомо, що всі оператори використовують маски, та їх всього 15 (табл. 1).

Таблиця 1. Маски мобільних операторів України

Оператор	**Маска**
Київстар	039, 067, 068, 096, 097, 098
МТС	050, 066, 095, 099
life:)	063, 093
Utel	091
PEOPLEnet	092
Інтертелеком	094

На основі викладеного вище, алгоритм ідентифікації користувача може виглядати наступним чином:

1. Згенерувати номери телефонів.
2. Захешувати сгенеровані номери телефонів.
3. Порівняти перебором всі захешовані номери телефонів.
4. Відправити HLR-запит на встановлення валідності номеру і локації.

Нижче наведений приклад застосування запропонованого алгоритму.

Припустимо, що в Advertising-пакеті був номер +380634376494. Тоді хеш його буде cc3f08c8f31ba94d1677ced94e992c00979314f43783620a9f3f0561543d7e12.

Отже, в Advertising-пакеті передавались ***cc3f08***.

Для отримання усіх можливих хешів можна використати формулу (1):

$$p = u + m + r, \quad (1)$$

де *u* – це код України (+38);

m – маска оператора;

r – рандомні 7 цифр.

Таким чином можливо отримати 149'999'985 комбінацій. Для генерування і хешування у наведеному прикладі було витрачено біля 8 хвилин.

У згенерованому масиві номерів лише у 5 номерів хеш починається з «*cc3f08*» (табл.2).

Таблиця 2. Номери телефонів та їх хеші

Хеш	Номер телефону
cc3f084a1b3a342406d41531ff7b08d6a486322ecb8d48696d3c0e6d8f7f132a	+380671117394
cc3f0869a06859793951d31d2becd8f93c9a032dc67185f52424c826c422540c	+380966020098
cc3f08b465c5bb829abbb70bf2f5c1f6ad404f4ea4e6687edc10b18da6a2d73a	+380506610974
cc3f08c8f31ba94d1677ced94e992c00979314f43783620a9f3f0561543d7e12	+380634376494
cc3f080861729f449c63d55cfc841ebd1f239fa5035c19b1af07f837b99ba52f	+380948919817

Наступним кроком алгоритму є порівняння отриманих номерів із даними оператора HLR (табл. 3).

Таблиця 3. Результати порівняння згенерованих номерів та даних оператора HLR

Телефон	MCCMNC	Оператор	Статус
380671117394	25502 (Київстар)	Україна, Київстар, Миколаївська обл.	Доставлено
380966020098	25502 (Київстар)	Україна, Київстар, Кіровоградська обл.	Неможливо доставити, абонент не існує
380506610974	25501 (МТС)	Україна, МТС, Закарпатська обл.	Передано оператору
380634376494	25506 (lifecell)	Україна, lifecell, Київська обл.	Доставлено
380948919817	25505 (Інтертелеком)	Україна, Інтертелеком, Київська обл.	Неможливо доставити, абонент не існує

Отже, якщо відомо, в якому місті перебувають користувачі, можливо точно визначити, хто саме з них потрібний.

Таким чином, запропонований алгоритм, час роботи якого не перевищує 8 хвилин, може бути ефективно використаний для визначення місцеположення користувачів.

Висновки та перспективи подальшого дослідження.

Специфікація Bluetooth 5 розширює корисний діапазон зв'язку до сотень метрів у прямій видимості. У той час, як атака з відстеженням, запропонована в цій статті, розглядає відстеження одного противника в такій радіусі дій, можливо припустити, що локальне відстеження методів BLE може бути значно ускладнено за рахунок їх координації у ботнеті зловмисників. Зазначений підхід має значний потенціал у сфері спостереження.

Список бібліографічного опису

1. Padiya S. D., Gulhane V. S. Analysis of Bluetooth versions (4.0, 4.2, 5, 5.1, and 5.2) for IoT applications. In book: Implementing Data Analytics and Architectures for Next Generation Wireless Communications. Chapter: 10. IGI Global, 2021. P. 153-178. DOI: 10.4018/978-1-7998-6988-7.ch010.

2. Cha S.-C., Yeh K.-H., Chen J.-F. Toward a robust security paradigm for Bluetooth low energy-based smart objects in the Internet-of-Things. Sensors. 2017. Vol. 17, no. 2348. P. 1-17. DOI:10.3390/s17102348.
3. Gangwal A., Singh S., Spolaor R., Srivastava A. BLE Whisperer: Exploiting BLE Advertisements for data exfiltration. In book: Computer Security. ESORICS, 2022. DOI: 10.1007/978-3-031-17140-6_34.
4. Kim T.-Yo., Lee H.-J. Vulnerability analysis of Bluetooth communication based on GNU radio. The Journal of the Korean Institute of Information and Communication Engineering. 2016. Vol. 20, Is. 11. P. 2014-2020. DOI: 10.6109/jkiice.2016.20.11.2014.
5. Jameel I., Dungen J. Low-power wireless advertising software library for distributed M2M and contextual IoT. 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT). Jan. 2015. P. 597-602. DOI: 10.1109/WF-IoT.2015.7389121.
6. Vanhoef M. A time-memory trade-off attack on WPA3's SAE-PK. ACM Asia Conference on Computer and Communications Security (ASIA CCS '22), May 2022. P. 27-37. DOI:10.1145/3494105.3526235.

References

1. Padiya S. D., Gulhane V. S. Analysis of Bluetooth versions (4.0, 4.2, 5, 5.1, and 5.2) for IoT applications. In book: Implementing Data Analytics and Architectures for Next Generation Wireless Communications. Chapter: 10. IGI Global, 2021. P. 153-178. DOI: 10.4018/978-1-7998-6988-7.ch010.
2. Cha S.-C., Yeh K.-H., Chen J.-F. Toward a robust security paradigm for Bluetooth low energy-based smart objects in the Internet-of-Things. Sensors. 2017. Vol. 17, no. 2348. P. 1-17. DOI:10.3390/s17102348.
3. Gangwal A., Singh S., Spolaor R., Srivastava A. BLE Whisperer: Exploiting BLE Advertisements for data exfiltration. In book: Computer Security. ESORICS, 2022. DOI: 10.1007/978-3-031-17140-6_34.
4. Kim T.-Yo., Lee H.-J. Vulnerability analysis of Bluetooth communication based on GNU radio. The Journal of the Korean Institute of Information and Communication Engineering. 2016. Vol. 20, Is. 11. P. 2014-2020. DOI: 10.6109/jkiice.2016.20.11.2014.
5. Jameel I., Dungen J. Low-power wireless advertising software library for distributed M2M and contextual IoT. 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT). Jan. 2015. P. 597-602. DOI: 10.1109/WF-IoT.2015.7389121.
6. Vanhoef M. A time-memory trade-off attack on WPA3's SAE-PK. ACM Asia Conference on Computer and Communications Security (ASIA CCS '22), May 2022. P. 27-37. DOI:10.1145/3494105.3526235