УДК 004.771 **doi: 10.26906/SUNZ.2018.3.131**

В. Я. Певнев, К. Н. Лейченко

Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков, Украина

АНАЛИЗ ВЕКТОРА АТАКИ ТЕХНОЛОГИИ БЕСПРОВОДНОЙ ПЕРЕДАЧИ ДАННЫХ BLUETOOTH

В статье проанализирован вектор атаки на устройства, использующие Bluetooth. Показано, что данная технология не обеспечивает надежность канала связи. **Цель статьи.** Исследование возможности проведения атаки на технологию беспроводной передачи данных Bluetooth, анализ полученных данных и составление рекомендаций. **Результаты.** В статье рассмотрены программные средства, позволяющие провести пентестинг беспроводной технологии передачи данных Bluetooth, рассмотрены и проанализированы уязвимости в рамках исследования Armis – пакет эксплоитов BlueBorne. Представлена проблема сложности закрытия уязвимости и выведены рекомендации, которые помогут снизить вероятность несанкционированного доступа, утечки данных и иные зловредные манипуляции, которые возможны при использовании уязвимостей в Bluetooth. **Вывод.** Анализ вектора атаки на Bluetooth отображает ненадежность данной технологии, что наводит на мысль о нецелесообразности использования данного канала беспроводной связи в системах, где важна конфиденциальность и целостность данных.

Ключевые слова: информационная безопасность, BlueBorne, Bluetooth, беспроводные сети.

Введение

Использование информационных технологий в начале XXI столетия обеспечило их внедрение во все сферы жизни человека. В наше время можно наблюдать большой рост популярности интернет вещей. «Умный дом» позиционирует себя как средство обеспечения удобства и расширение функций, казалось бы, обычных бытовых приборов. Множество датчиков в приборах вызывает необходимость создания внутреннего канала связи с сервером, который обрабатывал бы данные и выводил актуальную информацию для человека. Казалось бы, что нет минусов в том, что наш дом «поумнел». Но все же довольно весомый минус есть, и этот минус – обеспечение конфиденциальности во время сеанса связи.

Для удобства, создается беспроводная сеть на основе технологий Wi-Fi или Bluetooth. Wi-Fi – это тема для отдельного обсуждения, но стоит обратить внимание на Bluetooth.

В дистрибутивах kali и parrot предустановлено семь инструментов для пентестинга Bluetooth [1]:

1) Bluelog;
2) Blueranger;
3) Bluesnarfer;
4) Btscanner;
5) Crackle;
6) Redfnang;
7) Spooftooph.

Также в 2017 году сразу несколько разработчиков обнаружили и выставили сразу несколько эксплоитов на такие операционные системы, такие как Android, Windows, iOS, Linux, которые направлены на эксплуатацию уязвимостей в Bluetooth. Все они вошли в пакет BlueBorne.

Данная уязвимость затрагивает более 8 миллиардов устройств по всему миру, и делает легкой мишенью всю сферу интернет вещей [2].

Цель данной статьи – исследовать вектор атаки Bluetooth и разобрать эксплоиты, которые входят в состав Blueborne.

1. Принцип работы Bluetooth

В статье проанализирован вектор атаки на устройства, использующие Bluetooth. Показано, что данная технология не обеспечивает надежность канала связи. Технология Bluetooth состоит из 2 видов связи: синхронный SCO (Synchronous Connection Oriented) и асинхронный ACL (Asynchronous Connectionless). SCO используется для связи типа «point - point», скорость передачи равна 64 Кбит/с, ACL используется в рамках «point - multipoint», скорость передачи данных в виде пакетов составляет порядка 721 Кбит/с. Пакет состоит из:

- 72 бит вначале блока – код доступа;
- 54 бит – заголовок пакета, хранящий в себе информацию о параметрах и контрольную сумму;
- последующая область отведена для пересылаемой информации. Размер от 0 до 2745 бит [3].

Принцип строение систем Bluetooth опирается на использование метода расширения спектра при скачкообразном измерении частоты. Весь частотный диапазон, выделенный для Bluetooth радиосвязи разбит на N частотных каналов, с полосой 1МГц каждый. Также используется частотная манипуляция при кодировании пакетной информации. На рис. 1 изображена частотно-временная плоскость, отображающая одновременную работу трех Bluetooth модулей [3].

Рис. 1. Частотно-временная плоскость

Как можно заметить, модули работают тактами по 625 мкс. Для каждого модуля назначается соответствующий канал в пределах каждого такта.

Пара любых соединенных устройств образуют пикосеть (рис. 2).

Пикосеть может содержать до 7 ведомых устройств, если в сети оказывается больше 8 устройств – создается следующая пикосеть и так далее [4].

Архитектура Bluetooth (рис. 3) состоит из следующих блоков [5]:

1) RF: преобразовывает битовые последовательности в радиосигналы;

2) Baseband: совершает управление физическими каналами, поверх которых устанавливаются соединения;

3) Link Manager: отвечает за установление, изменение и освобождение логических соединений;

4) L2CAP – высокоуровневый блок. Обеспечивает сегментацию и восстановление пакетных данных;

5) HCI – обрабатывает связь между хостом и модулем;

6) WAP, OBEX – интерфейсы для других протоколов связи;

7) TCS – поддерживает услуги телефонии.

8) SDP – позволяет обнаруживать службы другого Bluetooth устройства.

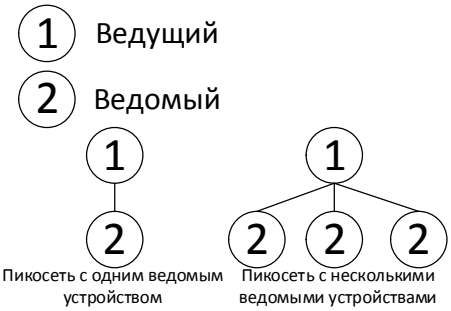

Рис. 2. Фундаментальная форма коммуникации в технологии Bluetooth

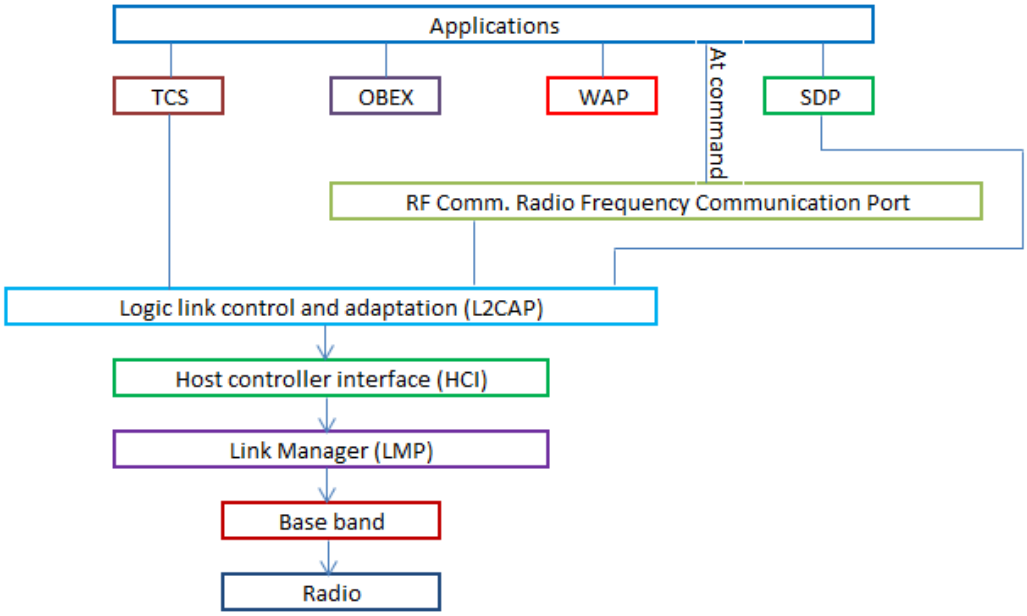

Рис. 3. Архитектура Bluetooth

2. Инструменты для пентестинга kali (parrot)

В дистрибутивах kali и parrot предустановлено 7 утилит для пентестинга Bluetooth:

1. Bluelog – это сканер Bluetooth, работающий на Linux, с опциональным режимом демона и веб-интерфейсом, он предназначен для исследований и мониторинга трафика. Подразумевается, что он должен запускаться на длительные периоды времени в одном месте для определения, как много обнаруживаемых Bluetooth устройств в окрестности [6];

2. Blueranger – простой скрипт, написанный на Python, который использует i2cap сигналы для обнаружения Bluetooth устройств и определения примерного расстояния до них [7];

3. Bluesnarfer – скрипт, который крадет данные с устройства [8];

4. Btscanner – этот инструмент, обладающий графическим интерфейсом, сканирует видимые устройства в пределах рабочего диапазона [9];

5. Crackle – используется для перехвата краткосрочного ключа, с помощью которого подбирает PIN сопряжения [10];

6. Redfnang – усовершенствованная версия, способная находит неподдающиеся обнаружению Bluetooth устройства [1];

7. Spooftooph предназначена для автоматической подмены (спуфинга) или клонирования имён, класса и адреса Bluetooth устройств. Клонирование этой информации позволяет Bluetooth устройству эффективно скрываться из вида. Программы по сканированию Bluetooth отобразят только одно устройство, если в диапазоне в режиме обнаружения доступны несколько устройств с одинаковой информацией (особенно это касается одинакового адреса) [11].

Особенности:

– клонирование и ведение записи информации об устройствах Bluetooth;

– генерация случайных Bluetooth профилей;

– изменение Bluetooth профиля каждые X секунд;

– можно установить информацию об устройстве для Bluetooth интерфейса;

– выбор из журнала сканирования устройства для клонирования.

3. Blueborne

Такое название имеют 8 опасных уязвимостей в реализации технологии Bluetooth. Особенность этих уязвимостей в том, что для их эксплуатации не требуется взаимодействие с целью, также не требуется сопряжение устройств.

Уязвимость покрывает почти все типы устройств на различных платформах.

BlueBorne совмещает в себе 8 критических уязвимостей на платформах [2]:

- Android:
  1. CVE-2017-0781;
  2. CVE-2017-0782;
  3. CVE-2017-0783;
  4. CVE-2017-0785.
- Linux:
  1. CVE-2017-1000251;
  2. CVE-2017-1000250.
- Windows:
  1. CVE-2017-8628.

Устройства iOS пока не получили своего CVE идентификатора.

Атака с использованием эксплоитов BlueBorne состоит из нескольких этапов.

В первую очередь необходимо обнаружить активные Bluetooth соединения вокруг. Примечательно, что даже выключенный режим «обнаружения» не защищает от идентификации устройства [13]. После необходимо получить MAC устройства, на который совершается атака. Определив тип операционной системы, производится настройка экспоита и совершается атака на уязвимый протокол Bluetooth. После, в зависимости от целей, есть возможность «прослушивать» устройство, используя атаку «Человек посередине», или же вообще получить полный доступ к данный или удаленному управлению [13].

Перечень уязвимостей представлен ниже:

1. CVE-2017-0785 (Android уязвимость, может привести к утечке информации). Уязвимость существует в Service Discovery Protocol, (позволяет устройству идентифицировать другие Bluetooth девайсы). Позволяет отправлять запрос на сервер, заставляя раскрыть байт памяти, при этом получив ключи шифрования;

2. CVE-2017-0781 (Android уязвимость. Возможность выполнить код удаленно). Уязвимость существует Bluetooth Network Encapsulation Protocol (позволяет использовать устройство как модем для доступа в интернет). Недостаток позволяет вызвать нарушение целостности информации в памяти, что позволяет выполнить удаленный код. Не требует взаимодействия с пользователем;

3. CVE-2017-0782 (Android уязвимость. Возможность выполнить код удаленно). Уязвимость существует в профиле персональной сети Bluetooth Network Encapsulation Protocol (отвечает за установление соединения между устройствами). При атаке происходит нарушение целостности информации в памяти, позволяет выполнить код удаленно;

4. CVE-2017-0783 (Android уязвимость. Man-in-The-Middle). Уязвимость существует в PAN-профиле стека Bluetooth. Позволяет использовать атаку «Человек посередине», создавая вредоносный сетевой интерфейс на целевом устройстве, а также перенастраивать IP маршрутизацию и принудительно передавать сообщения через этот интерфейс. Данная атака практически незаметна, т.к. не требует взаимодействия с пользователем;

5. CVE-2017-8628. (Windows уязвимость. Man-in-The-Middle). Идентична *CVE-2017-0783*, они используют одни и те же принципы в реализации некоторых протоколов Bluetooth;

6. CVE-2017-1000250 (Linux уязвимость. Утечка информации). Подобно CVE-2017-0785, уязвимость существует на сервере SDP (отвечает за автоматическое подключение устройств к службам, которые предоставляют другие устройства)

Позволяет раскрыть бит памяти, что приводит к утечке ключей шифрования;

7. CVE-2017-1000251 (Linux уязвимость. Переполнение стека в BlueZ). Уязвимость существует в стеке Bluetooth ядра Linux. Недостаток Logical link control and adaptation protocol вызывает повреждение памяти, позволяющий выполнить удаленный код;

8. Атака BlueBorne на iOS. Недостаток устранен в IOS10 и Apple TV выше 7.2.2. Уязвимость позволяет выполнить удаленный код с привилегиями;

9 Удаленное выполнение кода с помощью протокола Apple Low Energy Audio. Недостаток обнаружен в Low energy audio protocol, разработанном в Apple (Предназначен для передачи звука на периферию). Недостаток вызывает повреждение памяти, что позволяет получить контроль над устройством [14].

Заключение

В данной работе был проанализирован вектор атаки на устройства, использующие Bluetooth. Удалось продемонстрировать факт, что данная технология не является надежным каналом связи.

Существует множество решений для различных платформ для атаки по Bluetooth, и BlueBorne – только одна из них.

На практике был разобран и использован експлоит под Android CVE-2017-0785, который позволяет получить бит памяти, что в свою очередь позволяет извлечь ключи шифрования для дальнейших атак, с кражей информации и получением удаленного доступа к устройству.

Стоит заметить, что функция скрытия обнаружения устройства не обезопасит от потенциального взлома.

Единственно верное решение зашиты от несанкционированного доступа – отключение модуля Bluetooth или сокращение времени использования данной технологии до минимума, а также использование других каналов связи до появления патчей, которые устранили бы уязвимости.

СПИСОК ЛІТЕРАТУРИ

1. Инструменты Kali Linux [Электронный ресурс]. – Режим доступа: https://kali.tools/ [Время доступа: Март, 12, 2018].
2. Уязвимость Blueborne в протоколе Bluetooth затрагивает миллиарды устройств [Электронный ресурс]. – Режим доступа: https://habrahabr.ru/company/pentestit/blog/337780/ [Время доступа: Октябрь, 21, 2017].
3. Принцип работы Bluetooth [Электронный ресурс]. – Режим доступа: http://1234g.ru/blog-of-wireless-technologies/bluetooth/chto-takoe-bluetooth-i-kak-on-rabotaet [Время доступа: Апрель, 13, 2018]
4. Архитектура Bluetooth [Электронный ресурс]. – Режим доступа: http://iptcp.net/arkhitektura-bluetooth.html [Время доступа: Апрель, 18, 2018]
5. Bluetooth – Introduction|Architecture|Applications [Электронный ресурс] – Режим доступа: http://www.swiftutors.com/bluetooth-introduction.html [Время доступа: Апрель, 18, 2018]
6. Инструменты Kali Linux – Bluelog [Электронный ресурс]. – Режим доступа: https://kali.tools/?p=2470 [Время доступа: Март, 12, 2018]
7. Bluesnarfer [Электронный ресурс]. – Режим доступа: https://tools.kali.org/wireless-attacks/bluesnarfer [Время доступа: Апрель, 18, 2018]
8. BlueRanger [Электронный ресурс]. – Режим доступа: https://tools.kali.org/wireless-attacks/blueranger [Время доступа: Апрель, 18, 2018]
9. 9 Btscanner – cyborg linux [Электронный ресурс]. – Режим доступа: http://cyborg.ztrela.com/btscanner.php/ [Время доступа: Апрель, 18, 2018]
10. Crackle [Электронный ресурс] – Режим доступа: https://tools.kali.org/wireless-attacks/crackle [Время доступа: Апрель, 18, 2018]
11. Инструменты Kali Linux – Spooftooph [Электронный ресурс]. – Режим доступа: https://kali.tools/?p=2479 [Время доступа: Апрель, 18, 2018]
12. Взлом Bluetooth [Электронный ресурс]. – Режим доступа: https://codeby.net/kak-vzlomat-bluetooth-chast-1-terminy-tehnologii-i-bezopasnost/ [Время доступа: Апрель, 18, 2018]
13. Kuchuk G., Kharchenko V., Kovalenko A., Ruchkov E. Approaches to selection of combinatorial algorithm for optimization in network traffic control of safety-critical systems. East-West Design & Test Symposium (EWDTS). 2016. Pp. 1-6. doi:https://doi.org/10.1109/EWDTS.2016.7807655.
14. Хабрахабр – Уязвимость BlueBorne [Электронный ресурс]. – Режим доступа: https://habrahabr.ru/company/cloud4y/blog/337782/ [Время доступа: Октябрь, 21, 2017]

Рецензент: д-р техн. наук, проф. К. С. Козелкова,
Державний університет телекомунікацій, Київ
Received (Надійшла) 12.02.2018
Accepted for publication (Прийнята до друку) 16.05.2018

Аналіз вектора атаки технології безпровідної передачі даних Bluetooth

В. Я. Пєвнєв, К. М. Лейченко

У статті проаналізовано вектор атаки на пристрої, що використовують Bluetooth. Показано, що дана техноло-гія не забезпечує надійність каналу зв'язку. **Мета статті**. Дослідження можливості проведення атаки на технологію безпровідної передачі даних Bluetooth, аналіз отриманих даних і складання рекомендацій. **Результати**. У статті розглянуті програмні засоби, що дозволяють провести пентестінг безпровідної технології передачі даних Bluetooth, розглянуті і проаналізовані уразливості в рамках дослідження Armis - пакет експлойтів BlueBorne. Представлена проблема складності закриття уразливості і виведені рекомендації, які допоможуть знизити ймовірність несанціонованого доступу, витоку даних і інші шкідливі маніпуляції, які можливі при використанні вразливостей в Bluetooth. **Висновок**. Аналіз вектора атаки на Bluetooth відображає ненадійність даної технології, що наводить на думку про недоцільність використання даного каналу безпровідного зв'язку в системах, де важлива конфіденційність і цілісність даних.

Ключові слова: інформаційна безпека, BlueBorne, Bluetooth, безпровідні мережі.

Analysis of the vector of attacks of technology of wireless data transmission Bluetooth

V. Pevnev, K. Leychenko

The article analyzes the vector of attack on devices using Bluetooth. It is shown that this technology does not ensure the reliability of the communication channel. **Purpose of the article.** Investigation of the possibility of an attack on the technology of wireless Bluetooth data transmission, analysis of the data obtained and making recommendations. **Results.** The article considers software that allows conducting pentification of Bluetooth wireless technology, examined and analyzed vulnerabilities in the Armis research - the BlueBorne exploit package. The problem of the complexity of closing the vulnerability is presented and recommendations are made that will help reduce the probability of unauthorized access, data leaks and other malicious manipulations that are possible with the use of vulnerabilities in Bluetooth. **Conclusion**. Analysis of the attack vector on Bluetooth shows the unreliability of this technology, which suggests that it is inappropriate to use this wireless channel in systems where confidentiality and data integrity is important.

Keywords: information security, BlueBorne, Bluetooth, wireless networks.