www.volsu.ru

DOI: https://doi.org/10.15688/NBIT.jvolsu.2024.1.6

УДК 004.05
ББК 32.884.1

ИССЛЕДОВАНИЕ ТЕХНОЛОГИИ BLE 4.1 С ИСПОЛЬЗОВАНИЕМ UBERTOOTH ONE

Евгений Сергеевич Семенов

Кандидат технических наук, доцент,
заведующий кафедрой телекоммуникационных систем,
Волгоградский государственный университет
semenov.evgeniy@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Александр Игоревич Трофимов

Студент, кафедра телекоммуникационных систем,
Волгоградский государственный университет
trofimov.ai@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Владимир Генрихович Окунев

Студент, кафедра телекоммуникационных систем,
Волгоградский государственный университет
vova.okunev25@gmail.com
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. В статье предложено исследование технологии Bluetooth Low Energy (BLE) с использованием устройства Ubertooth One. Используется открытое ПО Wireshark для анализа трафика и ПО Crackle для расшифровки данных, выявляя уязвимости в процессе сопряжения BLE.

Ключевые слова: Bluetooth, Bluetooth Low Energy, BLE, Ubertooth One, анализ трафика, Wireshark, Crackle, уязвимости.

Bluetooth – это технология беспроводной связи, которая используется во многих устройствах, таких как смартфоны, наушники, колонки и т. д. Однако с широким распространением и использованием устройств, обладающих технологией Bluetooth, особую актуальность приобретают вопросы их безопасности.

В статье приведено исследование Bluetooth Low Energy (далее – BLE) – усовершенствованной версии Bluetooth 4.0, нацеленной на маломощные устройства [2]. BLE имеет меньшую мощность и потребление, как правило, во время передачи, не превышающее 15 мА. Для всех операций, связанных с шифрованием, BLE использует алгоритм AES-CCM с длиной ключа 128 бит.

BLE работает на частотах 2,400–2,4835 ГГц. Частотный диапазон BLE поделен на 40 каналов по 2 МГц, но обнаружение

происходит только на трех каналах. Максимальная скорость передачи данных (в Bluetooth 5) 2 Мбит/с.

В исследовании использовалось устройство Ubertooth One (рис. 1) – платформа разработки беспроводной сети с открытым исходным кодом на частоте 2,4 ГГц, подходящая для экспериментов с Bluetooth [3]. Данное устройство имеет следующие характеристики:

Диапазон частот: ISM 2,4 ГГц.
Bluetooth 1.x, Low Energy, 802.11 FHSS.
Микроконтроллер: ARM Cortex-M3.
Полоса пропускания: 1 МГц.
Мощность передатчика: 1 мВт.
Полудуплексный режим работы.
Разъем антенны: RP-SMA female.
Интерфейс взаимодействия с ПК: USB 2.0.
Стандартный отладочный разъем Cortex (10-контактный 50-миллиметровый JTAG).

Анализирование трафика осуществлялось с помощью открытого программное обеспечение (далее – ПО) Wireshark. Данная программа поддерживает огромное количество различных сетевых протоколов, а также обладает функцией сортировки и фильтрации трафика.

Для захвата трафика создается программный канал при помощи команды *mkfifo /tmp/pipe*. Затем в программе Wireshark открывается этот канал. Далее вводится команда *ubertooth-btle -f -c /tmp/pipe* для начала захвата BLE-трафика (см. рис. 2, 3).

После захвата трафика, для расшифровки данных, использовалось ПО Crackle под управлением операционной системы Kali Linux [4]. Оно использует уязвимость в процессе сопряжения BLE (Bluetooth Low Energy), которая позволяет злоумышленнику подобрать временный ключ (Temporary Key), передаваемый от главного устройства подчиненному. Если временный ключ будет успешно подобран, Crackle получит оставшиеся ключи – краткосрочный ключ (Short Term Key), и долгосрочный ключ (Long Term Key), используемые для шифрования остальной части соединения, и расшифрует все последующие зашифрованные пакеты.

Для расшифровки, входной PCAP файл должен содержать несколько пакетов с кодами операции управления LL_ENC_REQ и LL_ENC_RSP [1]. Для проверки наличия нужных пакетов указывается файл с захваченным трафиком в команде с ключом -i. Если они присутствуют, используется команда, указанная на рисунке 4, в которой после ключа -o указывается расположение файла для записи.

Уязвимость, которую эксплуатирует Crackle, характерна для версий BLE 4.0-4.1. С версии 4.2 в BLE был добавлен режим Secure Connection, который устраняет данную уязвимость.

В ходе проведения эксперимента удалось захватить BLE-трафик, рассмотреть структуру пакетов в программе Wireshark, также получилось расшифровать 3 пакета с помощью Crackle.

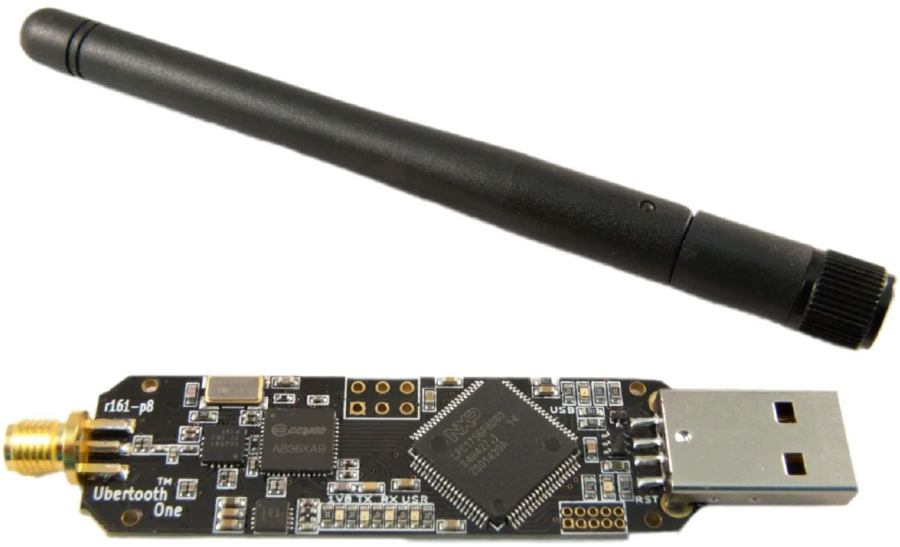

Рис. 1. Ubertooth One

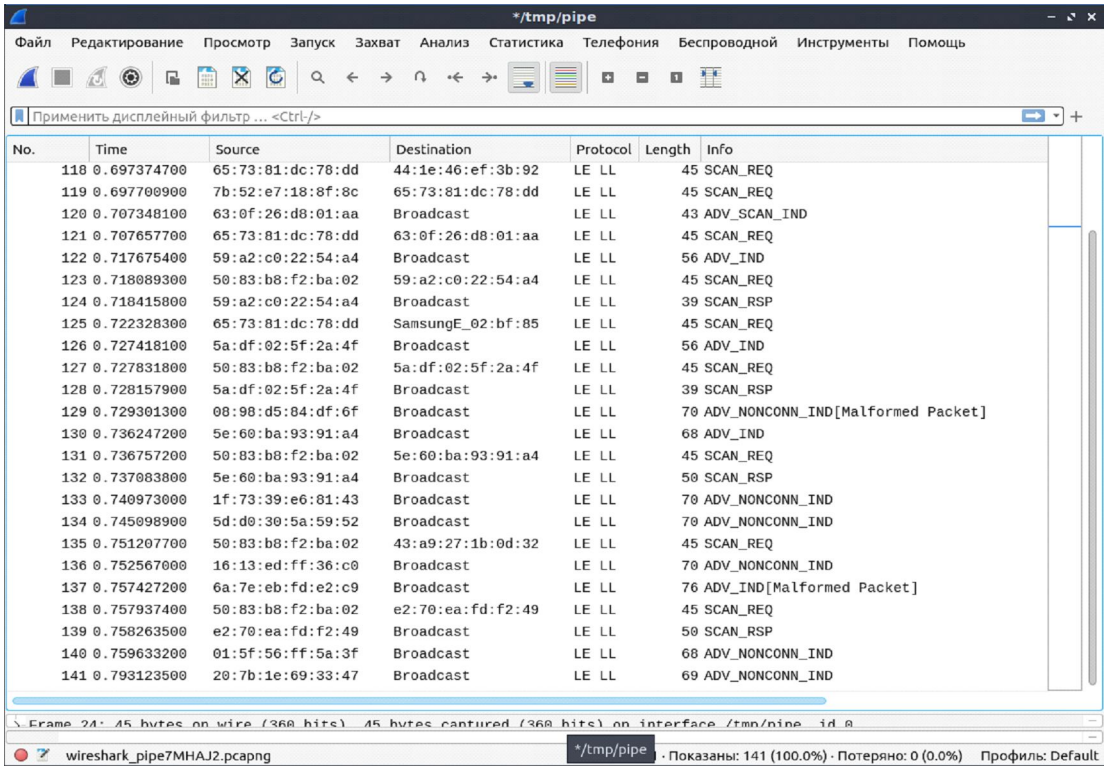

Рис. 2. Захваченный BLE-трафик в программе Wireshark

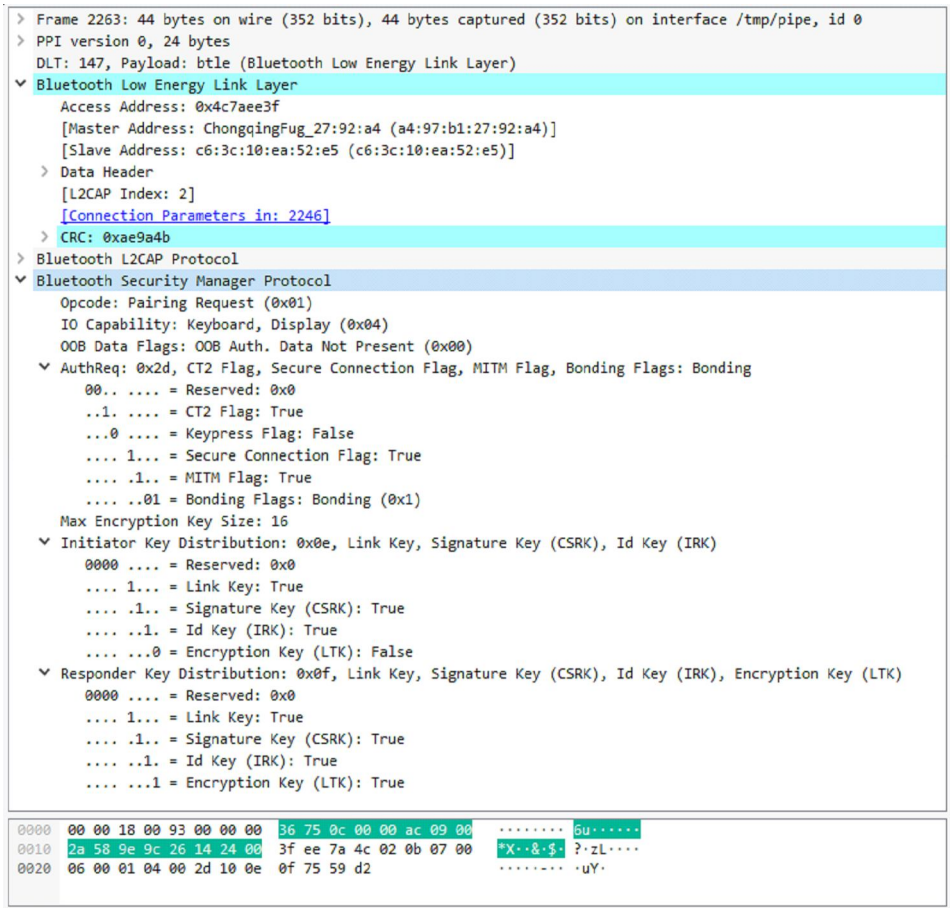

Рис. 3. Пакет Pairing Request BLE-трафика

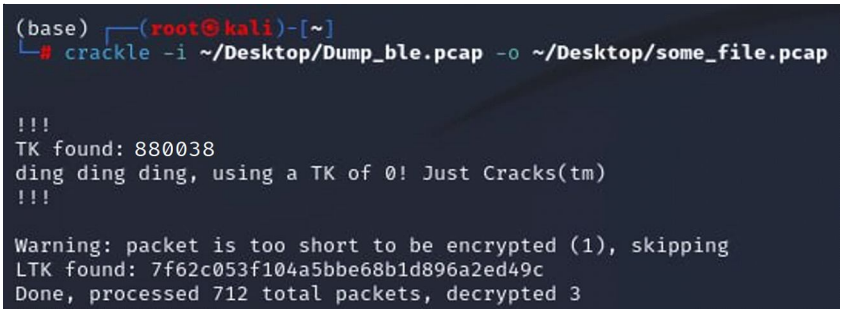

Рис. 4. Программа Crackle, расшифровавшая 3 пакета

СПИСОК ЛИТЕРАТУРЫ

1. Маркин, Ю. В. Обзор современных инструментов анализа сетевого трафика / Ю. В. Маркин, А. С. Санаров. – Электрон. текстовые дан. – Режим доступа: http://www.ispras.ru/preprints/docs/prep_27_2014.pdf. – Загл. с экрана.

2. Тонко, И. А. Преимущества и возможности технологии BLE в телекоммуникационных системах / И. А. Тонко, Е. П. Ельников, Е. А. Житковский // Новые информационные технологии в научных исследованиях : материалы XXIV Всерос. науч.-техн. конф., Рязань, 13–15 нояб. 2019 г. – Рязань : Ряз. гос. радиотехн. ун-т им. В.Ф. Уткина, 2019. – С. 371–372.

3. Kali Linux. – Electronic text data. – Mode of access: https://www.kali.org/tools/crackle/. – Title from screen.

4. Ubertooth One // GREAT SCOTT GADGETS. – Electronic text data. – Mode of access: https://greatscottgadgets.com/ubertoothone/. – Title from screen.

REFERENCES

1. Markin Yu.V., Sanarov A.S. *Obzor sovremennykh instrumentov analiza setevogo trafika* [Review of Modern Network Traffic Analysis Tools]. URL: http://www.ispras.ru/preprints/docs/prep_27_2014.pdf

2. Tonko I.A., Yelnikov E.P., Zhitkovsky E.A. Preimushhestva i vozmozhnosti tehnologii BLE v telekommunikacionnyh sistemah [Advantages and Possibilities of BLE Technology in Telecommunication Systems]. *Novye informacionnye tehnologii v nauchnyh issledovanijah: materialy XXIV Vseros. nauch.-tehn. konf., Rjazan, 13–15 nojab. 2019 g.* [New Information Technologies in Scientific Research. Proceedings of the 24th All-Russian Scientific and Technical Conference, Ryazan, Nov. 13–15, 2019]. Ryazan, Ryaz. gos. radiotekhn. un-t im. V. F. Utkina, 2019, pp. 371-372.

3. *Kali Linux*. URL: https://www.kali.org/tools/crackle/

4. Ubertooth One. *GREAT SCOTT GADGETS*. URL: https://greatscottgadgets.com/ubertoothone/

RESEARCH OF BLE 4.1 TECHNOLOGY USING UBERTOOTH ONE

Evgeny S. Semenov

Candidate of Sciences (Engineering), Associate Professor,
Head of the Department of Telecommunication Systems,
Volgograd State University
semenov.evgeniy@volsu.ru
Prosp. Universitetsky 100, 400062 Volgograd, Russian Federation

Alexander I. Trofimov

Student, Department of Telecommunication Systems,
Volgograd State University
trofimov.ai@volsu.ru
Prosp. Universitetsky 100, 400062 Volgograd, Russian Federation

Vladimir G. Okunev

Student, Department of Telecommunication Systems,
Volgograd State University
vova.okunev25@gmail.com
Prosp. Universitetsky 100, 400062 Volgograd, Russian Federation

Abstract. Bluetooth technology, widely used in devices like smartphones, headphones, and speakers, raises significant security concerns due to its prevalence. This study delves into Bluetooth Low Energy (BLE), an enhanced version of Bluetooth 4.0 designed for low-power devices. BLE operates at 2.400–2.4835 GHz, utilizing 40 channels but detecting traffic on only three. It employs AES-CCM encryption with a 128-bit key length for security. The research utilizes the Ubertooth One device, an open-source wireless development platform at 2.4 GHz suitable for Bluetooth experiments. Ubertooth One features an ARM Cortex-M3 microcontroller, 1 MHz bandwidth, and 1 mW transmitter power. The study involves traffic analysis using Wireshark, a tool supporting various network protocols and offering traffic sorting and filtering capabilities. To capture BLE traffic, a software channel is created with Wireshark using the ubertooth-btle command. Subsequently, Crackle software is employed to decrypt data by exploiting vulnerabilities in BLE pairing processes in versions 4.0–4.1. Crackle can derive temporary, short-term, and long-term keys from captured traffic to decrypt subsequent encrypted packets. The vulnerability exploited by Crackle is absent in BLE version 4.2 onwards due to the Secure Connection mode implementation. The experiment successfully captured BLE traffic, analyzed packet structures in Wireshark, and decrypted packets using Crackle, showcasing the importance of addressing security vulnerabilities in Bluetooth technologies. This study underscores the critical need for robust security measures in Bluetooth technologies to safeguard data integrity and confidentiality amidst the growing adoption of wireless communication devices.

Key words: Bluetooth, Bluetooth Low Energy, BLE, Ubertooth One, traffic analysis, Wireshark, Crackle, vulnerabilities.