Метод анализа протокола обмена данными на транспортном уровне с целью недопущения передачи защищаемой (конфиденциальной) информации

Бройко Антон Петрович

к.т.н., с.н.с., СПбГЭТУ «ЛЭТИ», Россия, Санкт-Петербург

broyko@mail.ru (*)

Кондрашов Кирилл Константинович

м.н.с., СПбГЭТУ «ЛЭТИ», Россия, Санкт-Петербург

kondrashovkk@mail.ru

The method of data exchange protocol analysis at the transport layer in order to Information Security

Broyko Anton Petrovich

Ph.D., senior researcher, St. Petersburg ETU "LETI", Russia, St. Petersburg

broyko@mail.ru

Kondrashov Kirill Konstantinovich

Junior researcher, St. Petersburg ETU "LETI", Russia, St. Petersburg

kondrashovkk@mail.ru

Аннотация. Предложен метод исследования USB-протокола для выявления проходящих по каналу конфиденциальных данных, передача которых во внешние сети нежелательна для обеспечения информационной безопасности. Физическими и программными методами исследован протокол подключения внешнего модема к персональному компьютеру с целью анализа возможностей создания устройства, предотвращающего утечку конфиденциальных данных. Предложены методы выявления и модификации передаваемых по шине USB пакетов, содержащих защищаемую информацию.

ABSTRACT. We proposed a method for studying USB-protocol to identify confidential data passing through the channel, the transfer of which to external

networks is undesirable for information security. Physical and software methods were used to study the protocol of connecting an external modem to a personal computer in order to analyze the possibility of creating a device that prevents the leakage of confidential data. Methods of detecting and modifying packets transmitted via USB bus, which contain protected information, were proposed.

Ключевые слова: информационная безопасность; защита сетей; утечка данных; USB-протокол.

Keywords: information security; information security in local networks; data breach; USB Protocol

Введение

С развитием современного мира все больше жизненно важных сервисов переводятся в режим «онлайн» и, как следствие этого, все большее значение приобретает проблема защиты конфиденциальной информации, передаваемой в открытые информационные сети общего пользования. В связи с широким распространением беспроводных сетей для передачи данных часто используется соединение персонального компьютера (ПК) с высокоскоростными сотовыми сетями стандарта LTE. Подключение к таким сетям обычно осуществляется через LTE-модем по USB интерфейсу. Для ограничения передачи защищаемой информации из ПК во внешние сети можно использовать аппаратный модификатор, осуществляющий фильтрацию данных на уровне USB-соединения.

Используемый подход

Принцип работы аппаратного модификатора USB-соединения заключается в обнаружении пакета, содержащего IP-адрес, для последующей передачи данных, и подмене этого адреса другим с пересчетом контрольной суммы. Для создания аппаратного модификатора необходимо исследовать

USB-протокол, по которому хост взаимодействует с LTE-модемом с целью выявления соответствующего пакета данных. Поскольку в открытых источниках этот протокол нигде не описан, требуется серия экспериментов со снятием сигнала с шины USB, расшифровкой и анализом передаваемых данных.

Методика эксперимента выглядит следующим образом.

1. Подключение микроконтроллера флэш-накопителя к ПК, выступающему в качестве хоста, и подключение дифференциального пробника к выводам D– и D+ разъема платы флэш-накопителя (использование данной конфигурации обусловлено простотой подключения и поставленной задачей – настроить измерительное оборудование для анализа протокола шины USB).

2. Настройка осциллографа для стабильного и надежного захвата USB-пакетов, а также отображения сигналов и формата их последующего сохранения.

3. Захват различных USB-пакетов и сохранение полученных сигналов для их последующего декодирования (необходимо исследовать до 20 различных пакетов для выявления общих закономерностей).

4. Разработка методики захвата и декодирования USB-пакетов по результатам анализа сохраненных пакетов.

5. Подключение LTE-модема к ПК с целью поиска пакета, содержащего IP-адрес.

6. Анализ большого количества пакетов данного типа для выявления их характерных признаков, возможных вариантов и разновидностей (после обнаружения искомого пакета).

7. Разработка методики однозначного определения пакетов, содержащих IP-адреса, в потоке данных USB-соединения по результатам анализа выявленных характерных признаков.

Предлагаемый аппаратный модификатор USB-соединения должен функционировать в режиме High-Speed на скорости 480 Мбит/с, в соответствии со спецификацией USB 2.0 [1]. Выявление и модификация IP-адреса при

соединении хоста с LTE-модемом по шине USB требуют предварительного установления типа и параметров соответствующего пакета. Для обнаружения искомого пакета необходимо исследовать канал передачи данных между хостом и LTE-модемом. Процесс исследования разбивается на два этапа:

1) исследование USB-протокола;
2) исследование протокола взаимодействия хоста с LTE-модемом.

На первом этапе исследовались общие характеристики USB интерфейса. Для этого контроллер флэш-накопителя фирмы Transcend был подключен к ПК через стандартный USB-порт. Из-за необходимости проведения измерений на высокой частоте, снятие сигнала с выводов разъема D– и D+ осуществлялось дифференциальным щупом Agilent 1131A, подключенным к осциллографу Agilent Infiniium 54853A DSO. Используемое измерительное оборудование позволяет детектировать сигнал с частотой до 2,5 ГГц при разрешении 20 Гигасэмплов/с, благодаря чему удается легко захватывать и раскодировать пакеты данных USB-соединения.

Раскодирование пакетов данных может производиться в «ручном» режиме в соответствии со спецификацией USB 2.0. Пример захваченного и раскодированного пакета приведен на рис. 1.

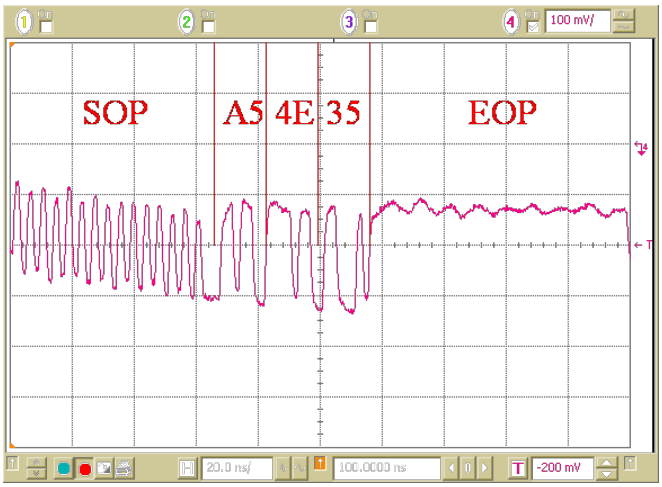

Рис. 1 Раскодированный пакет данных, захваченный на канале USB-соединения между ПК и контроллером флэш-накопителя.

По результатам раскодирования можно установить, что захваченный пакет данных представляет собой стандартный маркер начала кадра,

содержащий тип пакета, порядковый номер и контрольную сумму. Раскодируя весь поток данных, передаваемых между конечными точками USB-соединения, можно выявить требуемый пакет. Поскольку «ручной» анализ передаваемых по USB-кабелю данных при помощи осциллографа крайне затруднителен (в силу очень высокой скорости соединения и большого объема служебной информации) для существенного упрощения задачи был поставлен следующий эксперимент.

USB-соединение смартфона с внешним LTE-модемом эмулировалось посредством такого же соединения ПК с установленной ОС «Raspberry» и отладочной платы SIM8909EVB-KIT с модулем SIM8905E-TEKIT, которые представляют собой полнофункциональный макет смартфона на ОС «Android 7.0». Выбор данной конфигурации оборудования обусловлен наличием соответствующих устройств и простотой их подключения. В частности, отладочная плата поддерживает функцию USB-тетеринг, благодаря которой можно подключить ее к ПК как внешнюю сетевую карту. Плата также оснащена двумя разъемами для SIM-карт, которые позволяют организовать 4G (LTE) соединение по сетям сотовой связи, и Wi-Fi-модулем. Для проведения исследований использовалось подключение беспроводной Wi-Fi-сети. Для захвата и анализа USB-пакетов применялась программа Wireshark 2.6.7 – удобный инструмент диагностики сетевых интерфейсов.

Методика эксперимента выглядит следующим образом.

1. Подключение отладочной платы к ПК и активация функции USB-тетеринг (при этом происходит обнаружение внешней сетевой карты, которой автоматически назначаются IP-адрес в диапазоне 192.168.42.0/24 и сетевой шлюз 192.168.42.129).

2. Подключение отладочной платы к Wi-Fi-сети (при этом ей назначаются IP-адрес в диапазоне 192.168.1.0/24 и сетевой шлюз 192.168.1.1, а также появляется соединение с Интернетом).

3. Запуск программы Wireshark с правами пользователя «superuser», позволяющими захватывать пакеты USB интерфейса.

4. Захват пакетов сетевого интерфейса внешней сетевой карты, в качестве которой выступает отладочная плата, и сохранение полученных результатов.

5. Захват пакетов USB интерфейса отладочной платы и сохранение результатов.

6. Анализ полученных результатов в части местонахождения 4-байтового поля IP-адреса точки назначения внутри поля «DATA» пакета данных USB.

Вначале, после подключения оборудования, была осуществлена проверка соединения с Интернетом путем отправки ping-запроса на узел gazeta.ru. Параллельно был запущен захват пакетов сетевого интерфейса отладочной платы с помощью программы Wireshark. Всего был отправлен только один запрос, на который был получен корректный ответ (рис. 2).

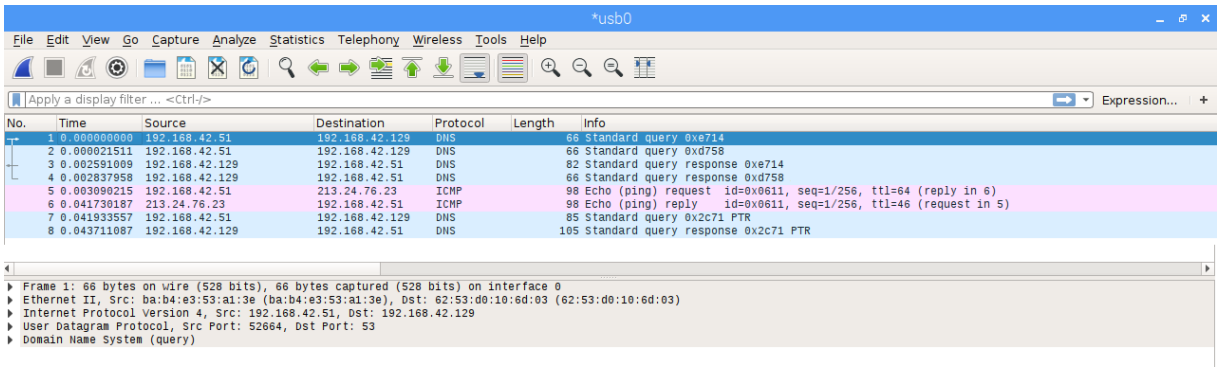

Рис. 2 Окно программы Wireshark с результатом захвата пакетов сетевого интерфейса отладочной платы при ping-запросе узла gazeta.ru.

Как видно из рис. 2, сначала был отправлен DNS-запрос к локальному серверу доменных имен, работающему на шлюзе. В ответном пакете был получен IP-адрес искомого узла gazeta.ru (81.19.72.1). Затем был отправлен собственно ping-запрос, и на него был получен ответ. Также в потоке данных сетевого интерфейса присутствуют служебные запросы, связанные с протоколами IPv6 и ARPA, поэтому всего было захвачено 8 пакетов. Для примера два захваченных пакета с содержащимися в них данными и детализированными сведениями о протоколах приведены в табл. 1.

Таблица 1 Данные захваченных пакетов сетевого интерфейса

No. Time Source Destination Protocol Length Info **1 0.000000000 192.168.42.51 192.168.42.129 DNS 66 Standard query 0x72e5 A gazeta.ru** Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0 Ethernet II, Src: ba:b4:e3:53:a1:3e (ba:b4:e3:53:a1:3e), Dst: 62:53:d0:10:6d:03 (62:53:d0:10:6d:03) Internet Protocol Version 4, Src: 192.168.42.51, Dst: 192.168.42.129 User Datagram Protocol, Src Port: 57348, Dst Port: 53 Domain Name System (query) 0000 62 53 d0 10 6d 03 ba b4 e3 53 a1 3e 08 00 45 00 bS..m....S.>..E. 0010 00 34 fc 4b 40 00 40 11 68 68 c0 a8 2a 33 c0 a8 .4.K@.@.hh..*3.. 0020 2a 81 e0 04 00 35 00 20 e7 4b 72 e5 01 00 00 01 *....5. .Kr..... 0030 00 00 00 00 00 00 03 66 73 62 02 72 75 00 00 01 ....gazeta.ru... 0040 00 01 ..
No. Time Source Destination Protocol Length Info **2 0.000021788 192.168.42.51 192.168.42.129 DNS 66 Standard query 0x06df AAAA gazeta.ru** Frame 2: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0 Ethernet II, Src: ba:b4:e3:53:a1:3e (ba:b4:e3:53:a1:3e), Dst: 62:53:d0:10:6d:03 (62:53:d0:10:6d:03) Internet Protocol Version 4, Src: 192.168.42.51, Dst: 192.168.42.129 User Datagram Protocol, Src Port: 57348, Dst Port: 53 Domain Name System (query)

```
0000  62 53 d0 10 6d 03 ba b4 e3 53 a1 3e 08 00 45 00   bS..m....S.>..E.
0010  00 34 fc 4c 40 00 40 11 68 67 c0 a8 2a 33 c0 a8   .4.L@.@.hg..*3..
0020  2a 81 e0 04 00 35 00 20 53 37 06 df 01 00 00 01   *....5. S7......
0030  00 00 00 00 00 00 03 66 73 62 02 72 75 00 00 1c   .......gazeta.ru...
0040  00 01                                            ..
```

Как видно из табл. 1, при передаче данных через сетевой интерфейс поле IP-адреса точки назначения пакета всегда расположено в одном и том же месте, а первый байт этого поля имеет смещение 0x1E. Хотя этот факт общеизвестен, так как формат заголовка пакета определен в спецификации протокола IP-соединений [2], следовало в этом убедиться перед тем, как приступать к анализу пакетов данных USB-соединения.

Ключевой задачей анализа USB-интерфейса отладочной платы является поиск IP-адреса точки назначения сетевого пакета в поле «DATA» пакета USB. Расположение этого адреса может зависеть от используемого протокола соединения хоста с внешней сетевой картой. Соответствующие спецификации весьма сложны, и зачастую сложно выяснить, каким именно из них удовлетворяет подключенное устройство. С точки зрения проектируемого аппаратного модификатора весьма важно, чтобы местонахождение поля IP-адреса было фиксированным, как в случае с сетевым пакетом, иначе реализация проекта затруднится.

Для захвата пакетов данных USB интерфейса также использовалась программа Wireshark. В целях удобства сопоставления и анализа результатов был отправлен только один ping-запрос на узел gazeta.ru. Всего было захвачено 20 пакетов, причем первые 4 пакета являются служебными, остальные 16 представляют собой те же 8 сетевых пакетов из предыдущего эксперимента, на которые были отправлены 8 ответных пакетов подтверждения успешной передачи в соответствии с протоколом USB-соединения. Результаты для двух пакетов приведены в табл. 2.

Таблица 2 Данные захваченных пакетов USB интерфейса

No. Time Source Destination Protocol Length Info **5 1.660769 host 1.4.1 USB 174 URB_BULK out** Frame 5: 174 bytes on wire (1392 bits), 174 bytes captured (1392 bits) on interface 0 USB URB Leftover Capture Data: 010000006e000000240000004200000000000000000000000... 0000 c0 e0 9d fb 2d 9f ff ff 53 03 01 04 01 00 2d 00 ....-...S.....-. 0010 97 77 1d 5e 00 00 00 00 ee 0a 00 00 8d ff ff ff .w.^..... 0020 6e 00 00 00 6e 00 00 00 00 00 00 00 00 00 00 00 n...n..... 0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 0040 01 00 00 00 6e 00 00 00 24 00 00 00 42 00 00 00 ....n...$...B... 0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 0060 00 00 00 00 00 00 00 00 00 00 00 00 62 53 d0 10 .....bS.. 0070 6d 03 ba b4 e3 53 a1 3e 08 00 45 00 00 34 e9 2f m....S.>..E..4./ 0080 40 00 40 11 7b 84 c0 a8 2a 33 c0 a8 2a 81 84 a1 @.@.{...*3..*... 0090 00 35 00 20 73 e3 41 b1 01 00 00 01 00 00 00 00 .5. s.A..... 00a0 00 00 03 66 73 62 02 72 75 00 00 01 00 01 ...gazeta.ru.....
No. Time Source Destination Protocol Length Info **6 1.660834 host 1.4.1 USB 174 URB_BULK out** Frame 6: 174 bytes on wire (1392 bits), 174 bytes captured (1392 bits) on interface 0 USB URB Leftover Capture Data: 010000006e000000240000004200000000000000000000000... 0000 80 ed 9d fb 2d 9f ff ff 53 03 01 04 01 00 2d 00 ....-...S.....-. 0010 97 77 1d 5e 00 00 00 00 2f 0b 00 00 8d ff ff ff .w.^..../..... 0020 6e 00 00 00 6e 00 00 00 00 00 00 00 00 00 00 00 n...n..... 0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 0040 01 00 00 00 6e 00 00 00 24 00 00 00 42 00 00 00 ....n...$...B... 0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 0060 00 00 00 00 00 00 00 00 00 00 00 00 62 53 d0 10 .....bS.. 0070 6d 03 ba b4 e3 53 a1 3e 08 00 45 00 00 34 e9 30 m....S.>..E..4.0 0080 40 00 40 11 7b 83 c0 a8 2a 33 c0 a8 2a 81 84 a1 @.@.{...*3..*... 0090 00 35 00 20 6b 04 4a 75 01 00 00 01 00 00 00 00 .5. k.Ju..... 00a0 00 00 03 66 73 62 02 72 75 00 00 1c 00 01 ...gazeta.ru.....

Как видно из табл. 2, при передаче пакетов данных сетевого трафика по USB интерфейсу поле IP-адреса точки назначения всегда расположено в одном и том же месте, а первый байт этого поля имеет смещение 0x8A. Дополнительные эксперименты с загрузкой различных сайтов показали, что даже в случае изохронных передач расположение поля IP-адреса внутри USB-пакета остается неизменным.

Аналогичный эксперимент был поставлен и для Wi-Fi-модема, работающего по USB интерфейсу. С помощью программы Wireshark были выявлены пакеты данных USB, содержащие внутри себя данные сетевого протокола. В частности, в захваченных пакетах присутствуют поля,

соответствующие MAC-адресам, IP-адресам и портам отправителя и получателя посылки. Далее представлены 4 захваченных пакетов сетевых данных, отправленных с хоста через внешний Wi-Fi-модем, для сравнения приведены сетевые запросы различных типов: NTP, ARP, DNS и Ping (табл. 3).

Таблица 3 Пакеты сетевых данных: NTP, ARP, DNS и Ping

01 00 00 00 86 00 00 00 24 00 00 00 5a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b6 61 54 a7 67 cc 26 54 96 0e bc b9 08 00 45 b8 00 4c 99 b7 40 00 40 11 98 55 c0 a8 2a dc 25 4f f7 08 00 7b 00 7b 00 38 23 d0 e3 00 06 ed 00 00 00 00 00 00 01 83 49 4e 49 54 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e2 ee 17 0c d8 a9 82 23 **NTP**	01 00 00 00 56 00 00 00 24 00 00 00 2a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b6 61 54 a7 67 cc 26 54 96 0e bc b9 08 06 00 01 08 00 06 04 00 02 26 54 96 0e bc b9 c0 a8 2a dc b6 61 54 a7 67 cc c0 a8 2a 81 **ARP**
01 00 00 00 7d 00 00 00 24 00 00 00 51 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b6 61 54 a7 67 cc 26 54 96 0e bc b9 08 00 45 00 00 43 0f b8 40 00 40 11 54 44 c0 a8 2a dc c0 a8 2a 81 93 5c 00 35 00 2f 46 c2 1e a0 01 00 00 01 00 00 00 00 00 00 01 30 06 64 65 62 69 61 6e 04 70 6f 6f 6c 03 6e 74 70 03 6f 72 67 00 00 1c 00 01 **DNS**	01 00 00 00 8e 00 00 00 24 00 00 00 62 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b6 61 54 a7 67 cc 26 54 96 0e bc b9 08 00 45 00 00 54 e2 57 40 00 40 01 19 e0 c0 a8 2a dc 57 fa fa f2 08 00 ff d7 06 7e 00 01 ea 9c 43 5f d3 a9 05 00 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 **Ping**

В приведенных выше пакетах (табл. 3) зеленым цветом выделены MAC-адреса, желтым – IP-адреса, а красным – порты. Как видно, все типы запросов, кроме ARP, имеют в целом схожую структуру, и все стандартные поля в них расположены на фиксированных местах. Благодаря этому можно сравнительно легко организовать распознавание и замену данных в этих пакетах, ведь позиции байтов, отвечающих, например, за IP-адрес, заранее известны и определяются счетчиком принятых байтов в модификаторе. Дополнительные трудности представляет собой пересчет контрольной суммы, который необходим при изменении содержимого пакета. Некоторую сложность вносит и метод надежного определения конца передаваемых данных и начала передачи младшего байта контрольной суммы.

В качестве идентификатора пакета для конкретного модема-отправителя из эксперимента можно использовать 10 байтов: нулевой (всегда равный 01h) и серию из 9 байтов, начиная с 50-го, которая всегда равна

2654960EBCB9080045h и состоит из MAC-адреса отправителя с параметрами сетевого пакета. Разумеется, модификатор может быть подключен к различным устройствам и MAC-адрес отправителя будет при этом разным, но такое допущение правомерно для узкоспециализированных применений.

Заключение

В результате применения предложенного метода анализа протокола обмена данными на транспортном уровне удалось доказать, что проект аппаратного модификатора данных USB-соединения на основе ПЛИС может быть с высокой вероятностью успешно реализован, поскольку изменению в пакете подлежат только 4 байта IP-адреса и 2 байта контрольной суммы. Допустимый объем буфера при этом может составлять всего 6 байт для обеспечения непрерывности передачи, а вносимая модификатором результирующая временная задержка, соответственно, будет равна 48 bt. Это обеспечивает устойчивость соединения и практически гарантирует скрытность промежуточного устройства как для хоста, так и для LTE-модема.

Благодарность

Работа выполнена в рамках государственного задания Министерства науки и высшего образования Российской Федерации №075-01024-21-02 от 29.09.2021 (проект FSEE-2021-0015)

Список литературы

1. Universal Serial Bus Specification. Режим доступа: https://www.usb.org/document-library/usb-20-specification.
2. Internet Protocol. Режим доступа: https://datatracker.ietf.org/doc/html/rfc791.