О конфиденциальности WhatsApp

Наверное каждый, кто пользовался популярным менеджером WhatsApp, обращал внимание на повторяющееся сообщение: «Сообщения защищены сквозным шифрованием. Третьи лица, включая WhatsApp, не могут прочитать или прослушать их». Если щелкнуть по ссылке в этом сообщении, вы будете направлены на сайт службы, где будет написано

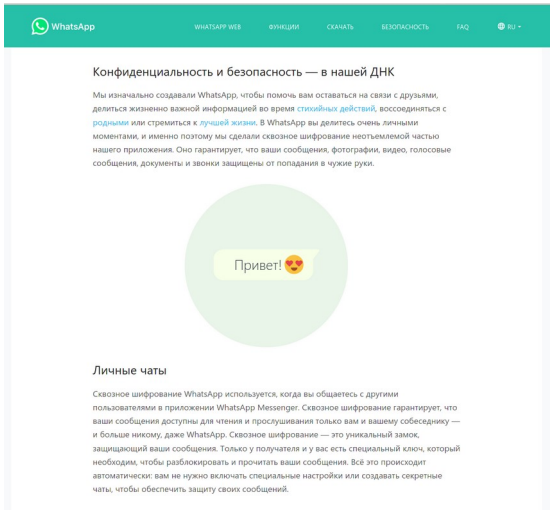

Рисунок 1. Заявление о конфиденциальности WhatsApp.

Будучи скептиком, я решил проверить это громкое заявление. Для проверки использовались два клиента WhatsApp на мобильных устройствах GSM, связанные каждый со своим компьютером. Оба компьютера располагались в одной локальной сети Ethernet и имели адреса IP из одного блока, т. е. маршрутизации между ними не было и был возможен прямой обмен пакетами.

Из приведенного заявления о конфиденциальности можно предположить, что клиенты обменяются между собой ключами TLS и смогут напрямую взаимодействовать, используя свои ключи. Но не тут-то было и никакого прямого обмена между хостами увидеть не удалось, т. е. каждый взаимодействовал с сервером WhatsApp (в моем случае это был mmx-ds.cdn.whatsapp.net (31.13.72.52) у обоих клиентов.

Для отслеживания обмена трафиком на обоих хостах была запущена программа WireShark. Ниже на рисунках представлены отфильтрованные результаты сбора пакетов, включающие лишь обмен между клиентами и упомянутым сервером WhatsApp (фильтр отображения в WireShark). Итак, запускаем на компьютере web-клиента и WireShark для отслеживания трафика. Не обязательно выполнять какие-либо действия в web-интерфейсе, он может служить лишь для просмотра и отслеживания пакетов, а писать можно непосредственно на мобильном устройстве.

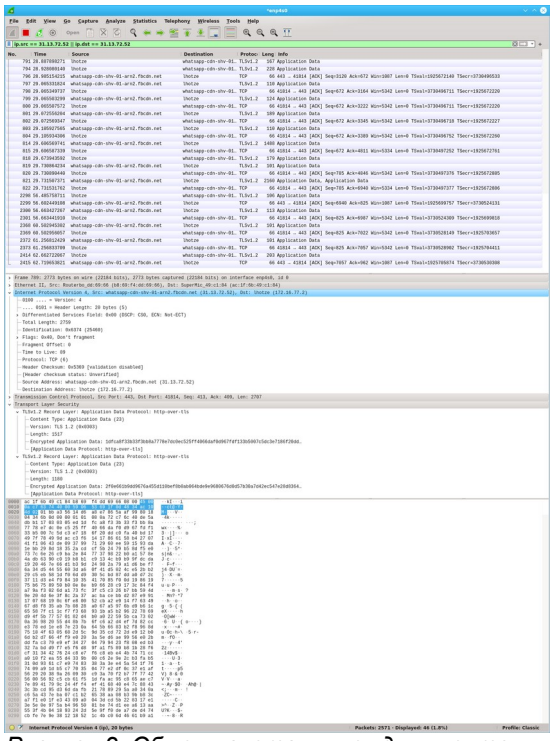

Рисунок 2. Обмен пакетами между клиентом и сервером WhatsApp.

На рисунке 2 можно видеть, что между клиентом и сервером WhatsApp действительно организован сеанс защищенного взаимодействия по протоколу TLSv1.2. Можно увидеть даже, что данные приложения шифруются, хотя пока никакого обмена между клиентами не происходило.

На другом компьютере при соединении с сервером WhatsApp наблюдалась совершенно аналогичная картина, поэтому рисунок для него не включен в текст.

Пакеты на обоих хостах были собраны WireShark и можно их посмотреть. Ниже представлены пакеты отправителя (рисунок 3) и получателя (рисунок 4), соответствующие передаче одного короткого сообщения.

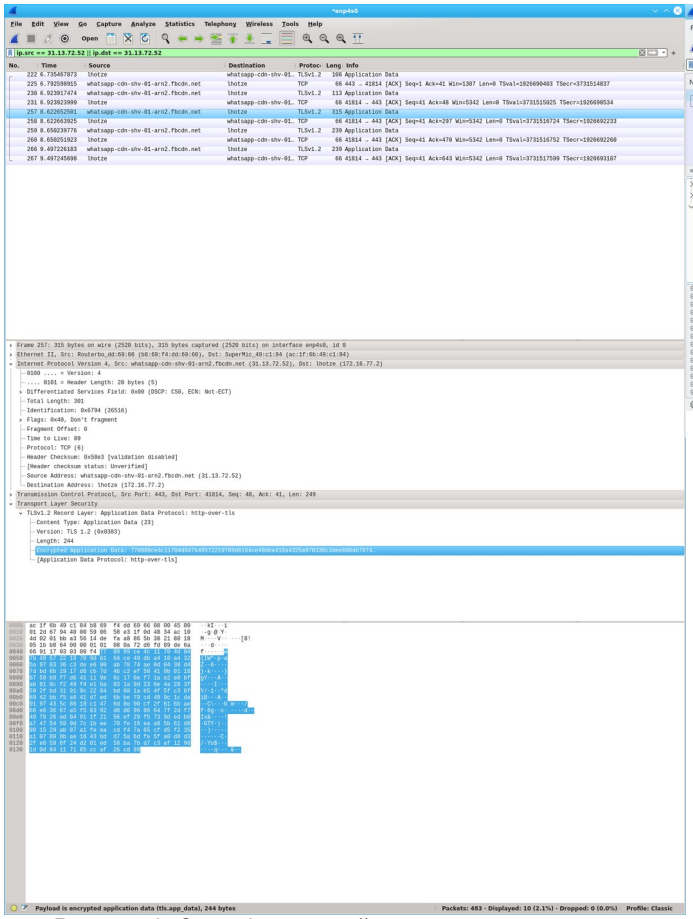

Рисунок 3. Зашифрованный пакет у отправителя.

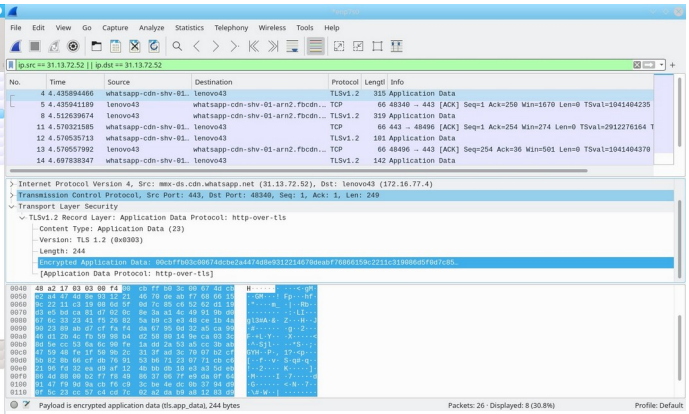

Рисунок 4. Зашифрованный пакет у получателя.

На обоих рисунках приведены данные «одного» пакета, содержащего сообщение отправленное в WhatsApp с одного мобильного устройства на другое. При сквозном шифровании (клиент-клиент), анонсированном WhatsApp данные в этих пакетах должны быть идентичными, т. е. зашифрованный отправителем текст сообщения должен совпадать с зашифрованным текстом в принятом получателем сообщении. Но не тут-то было. На приведенных рисунках очевидно, что шифрованные данные (выделены синим цветом на рисунках) не имеют между собой ничего общего, кроме размера.

Вывод очевиден - клиенты не взаимодействуют между собой напрямую, а каждый из них организует соединение TLS с сервером WhatsApp. При этом сервер расшифровывает сообщение, используя согласованный с отправителем ключ, затем снова шифрует его для получателя, используя согласованный с тем ключ. То есть говорить о конфиденциальности вашей переписки не приходится, коль скоро она подвергается расшифровке и повторному шифрованию на сервере WhatsApp. Очевидно, что никто (ничто) не препятствует перлюстрации переписки. Полагаться на приведенное выше заявление WhatsApp (принадлежит Facebook Inc.) я бы не рискнул.

Николай Малых

nmalykh@protocols.ru