Telegram представляет собой платформу для обмена мгновенными текстовыми сообщениями на базе протокола безопасности MTProto. Компания была основана в 2013 году, а сам мессенджер на данный момент имеет более 100 миллионов активных пользователей. Одна из главных целей Telegram – защита пользователей от слежки. Утверждается, что у этого мессенджера наилучшая защита на рынке и железобетонные гарантии безопасности среди приложений подобного рода.

Telegram – служба, связанная с обменом мгновенными сообщениями, которая была основана в 2013 году. Несмотря на свою молодость, на данным момент ежемесячно Telegram используют более 100 миллионов пользователей, особенно в Западной Европе. Создатели Telegram утверждают, что у этого мессенджера наилучшая защита среди аналогичных продуктов на рынке, однако в целом доверие пользователей основывается лишь на истории появления этого приложения и таланте разработчиков.

Telegram был основан в 2013 году братьями Николаем и Павлом Дуровыми, которые были основателями популярной российской социальной сети Vkontakte. После давления со стороны российских властей на предмет получения специфических возможностей (или специальных лазеек для государственных органов) Дуров покинул компанию и заявил, что VK находится под контролем политической партии, находящейся у власти. Затем Дуров покинул Россию и основал Telegram с целью предоставления средства обмена мгновенными сообщениями для простых пользователей, которое было бы защищено от слежки представителями государственных структур.

Протокол, используемый для обмена сообщениями, был разработан братом Павла Николаем, который является математиком, но малоизвестным специалистом по безопасности.

Telegram – уникальное явление среди технологических стартапов, в том числе благодаря тому, что Павел Дуров является единственным спонсором этого проекта. Кроме того, в Telegram отсутствует реклама, а сам клиент – не только бесплатный, но и с открытым исходным кодом.

Telegram имеет функцию под названием «секретный чат», которая не включена по умолчанию. Секретные чаты доступны в версии Telegrama со сквозным шифрованием. Сообщения удаляются по прошествии определенного времени, устанавливаемого пользователем, и не могут быть восстановлены. Разработчики Telegram решили не включать сквозное шифрования по умолчанию с целью удобства: секретные чаты связаны с конкретными устройствами, и невозможно продолжить разговор там, где не был начат разговор. Мы не считаем, что такое положение вещей является бесспорным. Многие обычные пользователи полагают, что никто не может получить доступ к сообщениям, хотя по факту просто доверяют безопасности сервера.

Пользователи Telegram могут создавать учетные записи и выполнять авторизацию при помощи аутентификационного кода, получаемого в виде текстового сообщения. После первоначальной авторизации пользователи могут выполнять настройки и искать друг друга. У Telegram также есть функция двухфакторной верификации, если есть желание вводить пароль во время каждого входа в учетную запись.

Как и многие аналогичные приложения Telegram следует традиционному подходу и использует облако для хранения данных. То есть, если злоумышленник сможет получить контроль над сервером, то получит (как минимум) доступ к незашифрованным сообщениям и ко всем метаданным. Обмен сообщениями между пользователями и сервером происходит на базе собственно разработанного протокола MTProto.

Пользователи обмениваются информацией по методу Диффи-Хеллмана для создания общего ключа, который затем используется при передаче сообщений. Коммуникация с сервером осуществляется при помощи публичного RSA-ключа, который прописан внутри клиента Telegram и меняется достаточно редко.

Telegram используется протокол собственной разработки MTProto, который не использует множество традиционных подходов при обмене сообщениями. Создатели Telegram утверждают, что подобный подход используется с целью улучшения производительности, однако у многих экспертов по безопасности на этот счет есть большие сомнения.

Группа исследователей в 2015 году анонсировала схему атаки на Telegram типа «челове-посередине», которая может быть осуществлена властями конкретного государства. Атака связана с генерированием общих секретов по методу Диффи-

Хеллмана для двух жертв, имеющих одинаковый 128-битный визуальный отпечаток, и пользователи, которые сравнивают отпечатки, не смогут обнаружить атаку. При реализации атаки «дней рождения» потребуется всего лишь 264 операции. С того момента количество битов, используемых в отпечатках, значительно увеличилось, однако в целом проблема остается актуальной. Чтобы проверить ключи и предотвратить MITM-атаки, пользователи должны визуально сравнить сетку квадратов с четырьмя оттенками синего. Здесь сразу же всплывает человеческий фактор. Во-первых, пользователь может не заметить едва различимых отличий между сетками. Во-вторых, у пользователя вообще может не быть желания возиться со сравнением сеток.

До 2014 года протокол MTProto использовал модифицированную версию схему обмена ключами по методу Диффи-Хеллмана . Вместо генерации ключей при помощи стандартного протокола на базе алгоритма Диффи-Хеллмана, сервер отсылал пользователю ключ, обработанный операцией XOR вместе с произвольным числом (nonce). Сей факт позволяет фальшивому серверу использовать различные nonce-переменные для двух пользователей, в результате чего будет один и тот же ключ, но который будет известен серверу. Повторимся еще раз: пользователи должны доверять серверу Telegram. Несмотря на то, что этот вопрос был решен, одно только присутствие этой проблемы вызывает массу вопросов относительно компетенций разработчиков Telegram в области безопасности, поскольку проблема чрезвычайно проста.

В некоторых частях протокола при хешировании вместо SHA-256 используется алгоритм SHA-1, который, как известно, неустойчив к коллизиям. Создатели Telegram утверждают, что SHA-1 используется в тех частях протокола, где устойчивость к коллизиям не принципиальна, однако все же более сильная хеш-функция была бы уместнее. История не раз доказывала, что бреши и неучтенные моменты – довольно распространенное явление.

Даже при использовании секретного чата, мобильная версия Telegram позволяет третьей стороне просматривать информацию о метаданных. Например, злоумышленник может узнать, когда пользователи выходят в онлайн и уходят в оффлайн вплоть до секунд. Telegram не требует соглашения от обоих сторон для установления коммуникации, и злоумышленник может подключиться и получить информацию о метаданных без ведома пользователя. Кроме того, у злоумышленника есть хороший шанс обнаружить, общаются ли два пользователя между собой посредством подключения и анализа метаданных на обоих концах

провода.

Заключение

Telegram оформился как самостоятельная компания, то приобрел популярность, благодаря заявлениям создателей, доверием и удачным временем выхода (в то же время произошли утечки с подачи Сноудена). Если верить заявлениям создателей Telegram, можно подумать, что этот мессенджер обладает высоким уровнем безопасности. Однако у Telegram были серьезные и в тоже время простые проблемы в протоколе (например, модифицированный и уязвимый алгоритм обмена ключами по методу Диффи-Хеллмана), которые может обнаружить любой знающий эксперт по безопасности.

Telegram, как и все другие продукты, имеет уязвимости, о которых пользователи должны знать. Однако, к сожалению, заявления компаний заставляют пользователей верить в то, что переписка защищена от прочтения третьей стороной.

Список литературы:

1. https://habr.com/post/412755/
2. http://dev-blogs.com/diffie-hellman-cipher/
3. https://www.securitylab.ru/analytics/490726.php