УДК 004.056.55

КАК ВЫПОЛНЯЕТСЯ ШИФРОВАНИЕ В МЕССЕНДЖЕРЕ TELEGRAM

Р.Ю. КАРАБАНОВ
(Представлено: канд. физ.-мат. наук, доц. Ю.Ф. ПАСТУХОВ)

Несмотря на то что мессенджер Telegram вышел на рынок позднее своих главных конкурентов WhatsApp и Viber, он довольно быстро приобрел репутацию одного из самых безопасных сервисов. Шифрование Telegram с помощью собственной разработки – протокола MTProto – позволило создать хорошо защищенный от взлома продукт, благодаря чему он стал популярен во всем мире.

Рейтинг безопасности

Безопасность виртуального общения определяется рейтингом Фонда электронных рубежей (EFF). В постоянно обновляемой таблице каждому сервису выставляется оценка от 1 до 7 в зависимости от уровня защиты информации от потенциального взлома (рис.).

Рисунок. – Шифрование Telegram является самым защищенным среди других месседжеров по версии Falongaze Analytics Center

Секретные чаты Telegram, шифрование которых осуществляется по принципу end-to-end (E2E), имеют в данном рейтинге максимальный бал – 7, а стандартная переписка, используемая по умолчанию, – 4. Поскольку при обычном общении ключи сохраняются на серверах компании, считается, что потенциально они могут стать доступны третьи лицам.

До недавнего времени рейтинг WhatsApp и Viber в таблице EFF был не очень высоким и равнялся всего двум баллам. Конкуренция с Telegram заставила данные компании пересмотреть свою политику безопасности. В связи с этим, был введен принцип оконечного шифрования, который с 2106 года стал использоваться по умолчанию, и позволил получить 6 баллов от EFF. Его суть заключается в хранении ключей, необходимых для расшифровки сообщений, только на устройстве пользователя. Таким образом, чтобы получить доступ к информации, необходимо обладать физическим доступом к смартфону.

Возникает вопрос: если сервис позиционирует себя как самый безопасный мессенджер, почему не использовать секретные чаты по умолчанию, что позволит безоговорочно возглавить рейтинг? Дело в том, что E2E-шифрование имеет определенный недостаток – секретная переписка привязывается к конкретному устройству, поэтому и ее история хранится только на одном устройстве.

Политика компании заключается в предоставлении пользователям права выбора, ведь стандартный режим позволяет заходить в аккаунт с любого устройства.

Шифрование Telegram на основе MTProto

Протокол MTProto использует два слоя шифрования – сервер-сервер и клиент-сервер. Он работает на основе следующих алгоритмов:

– AES – симметричный 256-битный алгоритм, принятый правительством США в качестве стандарта.

– RSA – криптографический алгоритм, в основе которого лежит вычислительная сложность задачи факторизации крупных целых чисел.

– Метод Диффи-Хеллмана – позволяет получить двум и более собеседникам секретный ключ по незащищенному от прослушивания, однако защищенному от подмены каналу связи.

– SHA-1, MD5 – хеш-алгоритмы, используемые во многих криптографических протоколах и приложениях для безопасного хеширования.В отличие от протокола Double Ratchet, который применяется WhatsApp и уже успел получить одобрение известных специалистов в области защиты информации, разработчики MTProto не спешат предоставлять свой продукт для независимого аудита. С одной стороны, это делает алгоритм потенциально уязвимым для атак, с другой – на сегодняшний день не зафиксировано ни одного успешного действия, приведшего к расшифровке сообщений. Создатели мессенджера заявляют о гарантии безопасности в отношении передачи зашифрованных данных. Для подтверждения своих слов Павел Дуров периодически организовывает конкурсы, в которых участникам предлагается расшифровать переписку двух собеседников. Призовой форд составляет 200 тыс. долларов, однако до настоящего времени ни один хакер не смог прочитать зашифрованные сообщения. Справедливости ради следует отметить, что многие эксперты довольно скептически относятся к подобным конкурсам, считая их скорее продуктами пиара, чем реальным доказательством защищенности системы.

Реален ли взлом

Даже если принять в качестве аксиомы, что MTProto действительно имеет лучшие параметры защиты среди современных мессенджеров, злоумышленники все же имеют возможность взломать аккаунт пользователя. При этом сам протокол здесь абсолютно не причем.

Уязвимость заключается в способе авторизации пользователя. Для данной процедуры используется реальный номер телефона, на который отправляется СМС-код для подтверждения входа в аккаунт. В основе подобного метода передачи данных лежит технология SS7 (Signaling System #7), которая разрабатывалась 40 лет назад и обладает слабыми параметрами безопасности по современным меркам. Теоретически злоумышленники могут перехватить СМС с кодом и взломать аккаунт. А поскольку в обычном режиме Telegram хранит все сообщения на своих серверах, хакеры могут получить доступ ко всей переписке конкретного пользователя.

Проблему решает общение в секретных чатах. В этом случае прочитать переписку можно только посредством реальной кражи телефона, так как сообщения не хранятся на сервере, а передаются исключительно между двумя устройствами.

ЛИТЕРАТУРА

1. Как осуществляется шифрование Телеграмм и в чем его отличие от других мессенджеров [Электронный источник]. – 2018. – Режим доступа: https://ru.telegram-store.com/blog/shifrovanie-telegramm/. – Дата доступа: 23.09.2018.
2. [Перевод] Почему у Telegram не включено End-to-End шифрование по умолчанию? [Электронный источник]. – 2018. – Режим доступа: https://medium.com/@tglive/telegram-end-to-end-e93554cb9e46. – Дата доступа: 23.09.2018.
3. Безопасен ли Telegram? Или как я искал закладку в MTProto / Хабр [Электронный источник]. – 2018. – Режим доступа: https://habr.com/post/206900/. – Дата доступа: 23.09.2018.
4. Анализ безопасности Telegram [Электронный источник]. – 2018. – Режим доступа: https://www.securitylab.ru/analytics/490726.php. – Дата доступа: 23.09.2018.
5. Миллиард чатов на замок: как работает шифрование WhatsApp и в чем его недостатки перед Telegram [Электронный источник]. – 2018. – Режим доступа: https://tjournal.ru/26022-milliard-chatov-na-zamok-kak-rabotaet-shifrovanie-whatsapp-i-v-chem-ego-nedostatki-pered-telegram. – Дата доступа: 23.09.2018.