

Безопасность мессенджеров



Что с безопасностью?

- Моменты, когда безопасность нужна, и когда нужно было предпринимать действия для этого, разнесены во времени
- Если (когда) вы обнаружили, что вам это нужно — уже поздно

Что с безопасностью?

- Безопасность мессенджеров — часть общей кибербезопасности гражданина
- Она является частью комплекса:
 - Доверенное железо
 - Доверенная ОС
 - Доверенное ПО

Критерии отбора мессенджеров

- наличие whiteraper'a по модели шифрования
- наличие документации по реализации
- наличие хоть какой-то пользовательской базы и пробега
- повторяемость сборок. Возможность самостоятельной сборки программистом средней квалификации под Windows/Linux, без красноглазия и пердолинга

Шифрование

- OTR: https://ru.wikipedia.org/wiki/Off-the-Record_Messaging
«Обратный храповик»
- шифрование сообщений — никто иной не сможет прочитать сообщения;
- аутентификация собеседников — уверенность в том, кто является собеседником;
- perfect forward secrecy — если потеряны секретные ключи, прошлая переписка не будет скомпрометирована;
- возможность отречения — третье лицо не сможет доказать, что сообщения написаны кем-либо другому адресату.

Шифрование групповых чатов

- Многосторонний Diffie Hellman
 - <https://crypto.stackexchange.com/questions/1025/can-one-generalize-the-diffie-hellman-key-exchange-to-three-or-more-parties>
- по multi df проблемка в объеме трафика и числе сообщений на согласование, он как минимум не меньше числа сторон. Там какие-то трюки в виде некоего pairing, нету времени сейчас разбираться, но короче задача как минимум нетривиальная. И очень сомневаюсь что это есть в условном openssl/libnssl

Шифрование групповых чатов

- Модель безопасности трудно формализуема
- Точка-точка: мы хотим взаимодействовать с собеседником, предполагаем доверие и отсутствие утечек с его стороны
- Группа:
 - То же самое, для всех участников
 - ИЛИ
 - Мы **не знаем** всех участников, **не доверяем им всем**.
Утечка от них возможна!

Атаки на клиенты

- TOX RCE

<https://www.linux.org.ru/forum/talks/17239546>

25.05.2023, 20 биткоинов (~\$530k)