SIGNAL PROTOCOL VS MTPROTO

Таборов Лев Алексеевич

Содержание

Введение

Signal Protocol является протоколом шифрования для приложения Signal Messenger, а MtProto для Telegram. В этом документе кратко описаны их отличия и почему Signal Protocol считается более безопасным.

Примитивы

	Signal	MTProto(2.0, end-to-end)
Протокол обмена ключами	X3DF на эллиптических кривых	Стандартный DH
Функция хэширования	SHA256/512	SHA256

Сравнение

Трудно сравнивать 2 протокола, потому что они задействуют разные способы защиты обмена сообщениями.

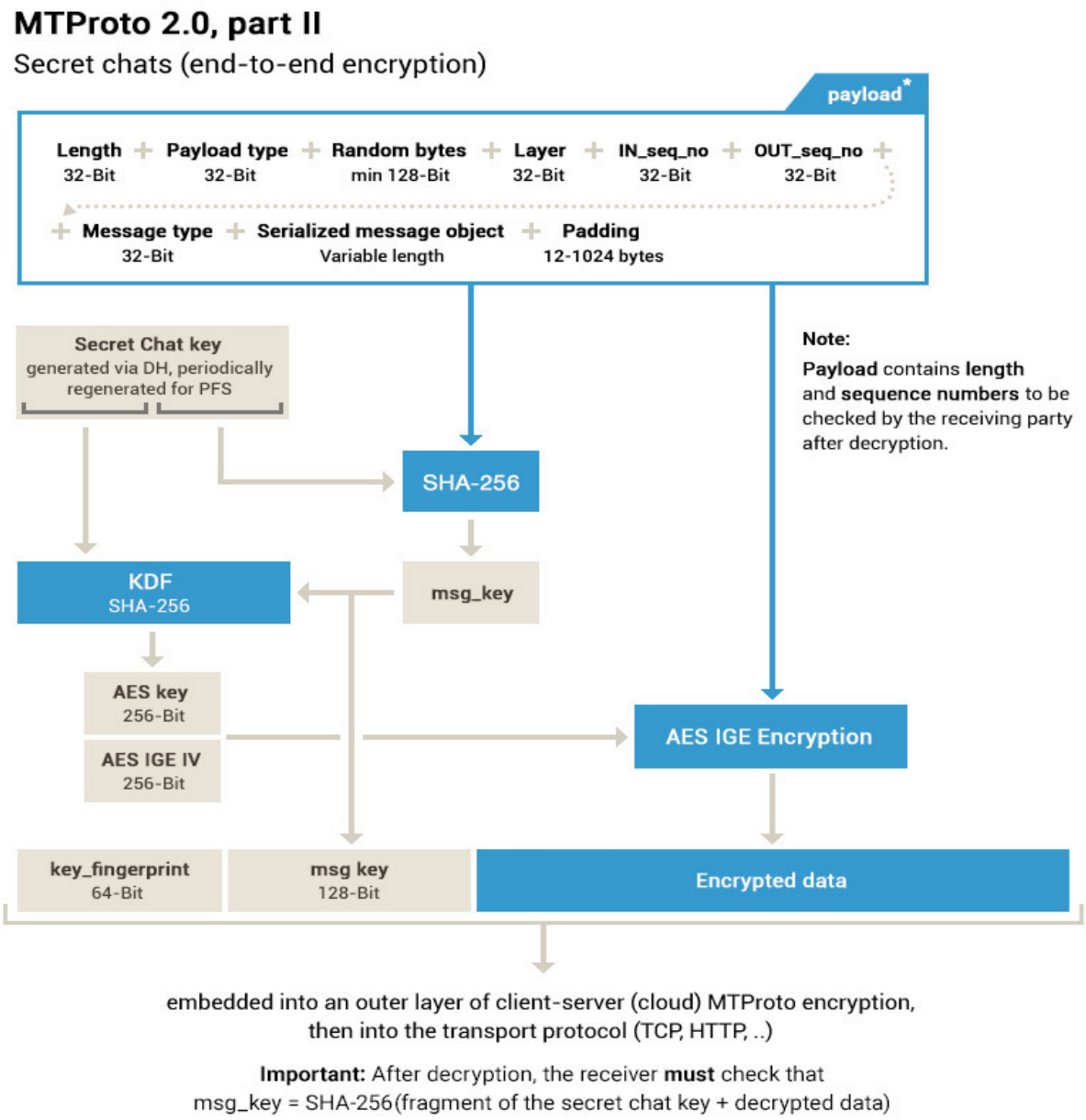
С одной стороны MTProto делает ставку на пакет сообщения, который формируется особым образом и лишь перехватив такой пакет (без ключа) прочитать его будет крайне трудно. Но из-за примитивности метода обмена ключами (простой протокол Диффи-Хеллмана, выполняющийся раз в 100 сообщений), вся система может сойти на нет, завладей 3е лицо ключами. Для сравнения простого ДиффиХеллмана и тройного можно посмотреть их описание в документе, описывающий Signal Protocol.

С другой стороны Signal использует примитивное шифрование самих сообщений (AEAD), но при этом основывается на сложном алгоритме генерации ключей, включающем в себя протокол 3го Диффи-Хеллмана на эллиптических кривых и алгоритм двойного храповика, так что ключи обновляются каждый раз при отправке/получении сообщения. Более того, из-за алгоритма двойного храповика, даже если 3е лицо перехватит какой-либо ключ, он не будет в состоянии дешифровать предыдущие и будущие сообщения.

Мнение экспертов

Экспертами был проверен протокол Signal, и его посчитали безопасным, чего не сказали про MTProto. Но была проверена лишь 1я версия протокола MTProto, 2я проверке не подвергалась.

Схема MtProto 2.0



Список литературы

https://crypto.stackexchange.com/questions/31418/signal-vs-telegram-in-terms-of-protocols
https://core.telegram.org/api/end-to-end
https://signal.org/docs/specifications/doubleratchet/
https://habr.com/ru/company/globalsign/blog/536986/
https://www.pindrop.com/blog/audit-of-signal-protocol-finds-it-secure-and-trustworthy/