The Secure Messaging App Conundrum: Signal vs. Telegram
(a comparison for non experts)

Cecilia Boschini¹,²

¹ Università della Svizzera Italiana, Lugano, Switzerland
² Facoltà Indipendente di Gandria, Gandria, Switzerland
cecilia.boschini@usi.ch

In the last few days I have been asked by many non-crypto friends “to recommend a secure messaging app alternative to WhatsApp”. This report contains my answer

The Contenders. When discussing secure messaging apps, two of them come immediately to mind: Signal [5] and Telegram [11]¹. Therefore, I decided to lay down as clearly as possible the reasons why one gives higher security guarantees than the other.

Disclaimer. Both Signal and Telegram care about security. Their teams are a collection of extremely smart people, and they do their best to protect their users. What sets them apart is their approach to security, and this is what I will analyze in this report. Neither protocol has been broken (yet), and as of the writing of this report I have never being in contact with any of the companies mentioned here.

TL;DR: Signal gives stronger security guarantees than Telegram.
If you want to prioritize security, use Signal. If you really like cool stickers, ginormous groups (100 000 of users!), and are willing to trust the guys at Telegram (they are not Facebook after all), go for Telegram.
Either choice gives you better security guarantees than WhatsApp ©
If you are looking of a summary of my points, read the Conclusions section.

Security Comparison

When discussing secure messaging apps we need to define what do we mean by “secure”. Intuitively, it is quite easy: we want that our messages can only be read by the intended recipients. This is when encryption comes into play: encryption is used to garble messages in such a way that the original message can be recovered only by someone knowing a secret information, called decryption key. As long as nobody but the intended receiver has the decryption key, someone intercepting our communication cannot read our messages².

A common misunderstanding is that, if a messaging app encrypts messages, then it is secure. This is in fact not true by itself. What if the decryption key is published somewhere for people to see?³ Then anyone could read the key, and decrypt the messages. Controlling who has access to such a key is very important.

Let us imagine now two users, Alice and Bob, that want to communicate using a messaging app by company X. When Alice sends a message, this message is sent to a server of company X, which then reroutes it to Bob. During the transmission of the message, their common (and very curious) enemy Eve is eavesdropping on the conversation⁴.
Now, if Alice wants to be completely sure that her messages are read only by Bob, she will make sure that Bob is the only one that knows the decryption key. This is called end-to-end (E2E) encryption. When E2E encryption is used, the server only sees encrypted messages and cannot read them. Hence, even if Eve was able to take control of the server, she would not gain any meaningful advantage.

Here lays the main difference between Signal and Telegram:

– In Signal, every communication (one-to-one chats, calls, group chats) is E2E encrypted.
– In Telegram, E2E encryption is not on by default in chats (it is on by default in calls), and is only available for one-to-one chats (the so-called Secret Chats) and calls (including video-calls). Groups, independently of their size, are not E2E encrypted.

¹ In Switzerland people mention Threema too. I do not consider it in this report, as it is not free; however the reader can find a brief comment about it at the end of this document.
² This is a very high-level explanation: in real-life we also want authentication, a step that makes sure that we are sending messages to the real recipient, and not to someone impersonating them. This is an extremely important step! However, we ignore it for the sake of clarity, as it is not a determinant topic in the Signal vs. Telegram security comparison.
³ I do not mean to insinuate that either Signal or Telegram publish users’ decryption keys. They don’t. They both really care about security.
⁴ In fact, Eve might actively try to hijack the conversation. We ignore this kind of attacks here for the sake of simplicity, as they are not important for my argument.
Signal has a better security infrastructure than Telegram for three reasons:

**Conclusions**

Signal has a better security infrastructure than Telegram for three reasons:
1. Signal does not ask users to trust Signal, Telegram does (and this has strong implications on security).
2. Every communication in Signal is E2E encrypted, in Telegram groups cannot be. Even assuming that encryption does not make sense for public groups with thousands of members, the lack of E2E encryption for small groups seems unnecessarily problematic.
3. E2E encryption is on by default on Signal, and in fact it cannot be turned off. This is not the case for Telegram, and it is bad practice in security. The choice of the security settings should NOT be left to users: that is what experts are for.

Still, from a security standpoint either of them is a better choice than WhatsApp, because they are open source (with some caveats in the case of Telegram, see the previous section for a more detailed explanation).

Honorable Mention: Business Plan. Until last month, both Signal and Telegram were committed to be non-profit organizations, surviving on donations. This is good, as it implies that neither of them have a reason to monetize their users. However, Telegram recently announced [3] that it will start generating revenue from advertisement in public one-to-many channels. The announcement explicitly committed to do it in a non-intrusive and ethical way, not to exploit users’ data, and to keep current features free of charge. The need for a stable income stream is perfectly understandable (Telegram has way more users than Signal9, thus needs more people to maintain the service). However, such a business model combined with the lower security guarantees of the app could more easily be turned against Telegram’s users themselves. No infrastructure is in place to prevent Telegram from exploiting its potential access to messages that are not E2E encrypted to increase its revenue through, for example, targeted advertisement.

Further Remarks and Threema

What about anonymity? In this discussion, I have focused on the confidentiality of the messages, ignoring the anonymity aspect. In fact, as Telegram already sees users messages in group chats, users’ anonymity can only be protected when a user restrict themselves to only use Secret Chats and avoids group chats; either way, both Signal and Telegram have access to users’ phone numbers and contact lists (optional in both cases). However, Signal does not have access to the content of users’ profiles [4], while Telegram does [12]. Thus considering anonymity in the analysis does not change the conclusions.

More technical comments. From a technical point of view, Signal’s protocol uses standard, well-known cryptographic techniques and has been formally analyzed by the cryptographic community (cf. for example [1,2], both available on the open archive ePrint). On the other hand, Telegram uses a cryptographic protocol developed in-house relying on techniques (in particular, the use of AES in IGE mode) that have not been as extensively studied (but they are not broken either!). Telegram claims that using a custom protocol was necessary in order to achieve reliability on weak mobile connections as well as speed when dealing with large files [13]. The fact that the security of Telegram’s encryption scheme is not supported by a broad cryptanalysis is a point in favor of Signal.

What about Threema? Threema [15] is a messaging app developed by a Swiss company, and it comes up often when discussing secure messaging in Switzerland. I did not include it in the discussion for two reasons: it is not free (requires a one-time payment of 3$10), while Signal and Telegram are, and has lower security guarantees than Signal (it does not guarantee forward secrecy when the server is corrupted, but only against external eavesdroppers). However, it guarantees higher anonymity than Signal, as Threema does not require a phone number or an email address to set it up (Signal requires a phone number).

Threema also advertises that its servers are in Switzerland, so it does not fall under the CLOUD Act, which entitles US authorities to access data from US IT service providers (even if the data is not stored in the US). Signal falls under such act (cf. [14]). However, the data that Signal servers store (users’ phone numbers and devices) or have access to (encrypted messages to be delivered) is encrypted. Thus, this is not a particularly strong point, as Signal could only hand over encrypted data to the US Government11. The claim in [14] that Signal is not GDPR compliant seems not to be true anymore [7].
In conclusion, my opinion is that from a security standpoint Threema is a better alternative than Telegram (even if Threema does not support 2-factor authentication, while Telegram does) and worse than Signal. All three are better choices than WhatsApp. But this is material for another report.

Acknowledgments

Thanks to Mark Korondi, Elena Pagnin and Nicolo Angerer for the useful discussions and comments about early drafts of this report.

References