Case Study-Is Telegram really encrypted or not?

Leonardo Oliveira Pereira
University of Coimbra, Department of Informatics Engineering, Portugal
uc2020239125@student.uc.pt

***Abstract*—This case study analyses the encryption practices of Telegram, a popular messaging platform that claims to be an *"encrypted messenger"*. By comparing Telegram to more secure messaging apps like Signal and WhatsApp, and exploring its encryption architecture, metadata handling, and additional security measures, this paper explores whether Telegram genuinely provides the privacy and security it claims. Despite offering some user-controlled security options, Telegram's default settings and encryption approach raise concerns about its overall effectiveness in protecting user data.**

Keywords—Telegram, End-to-End Encryption (E2EE), Security

I. Introduction

In the digital era, secure communication is very important, and messaging apps like Telegram have gained popularity, especially among users who value privacy and security [1], by guaranteeing that it is an *"encrypted messenger"*. However, questions have arisen regarding the actual strength of its encryption, particularly around its use of end-to-end encryption (E2EE), which is not enabled by default in all conversations. Studies show that the platform's default messaging encryption is not as robust as that of its competitors, such as Signal or WhatsApp [5], raising questions about the actual level of security it provides. While Telegram emphasizes the optional use of E2EE for some chats, concerns persist regarding the potential vulnerabilities in its encryption architecture, its reliance on proprietary encryption algorithms, and the centralized nature of its server infrastructure.

By analyzing its Security properties, comparing it with other encrypted messaging services, and evaluating potential security flaws, this paper seeks to clarify whether Telegram genuinely protects user data or if its encryption claims fall short of expectations in today's digital landscape.

II. How does telegram works?

As mentioned before, Telegram applies E2EE, which is a type of messaging where only the sender and the recipient can read the messages, excluding the messaging service. This happens because only the sender and the recipient have the decryption keys that allows to decrypt the messages exchanged between them.

The thing is that the modern private messaging services often use E2EE. So, how does Telegram differs from others messaging apps such as WhatsApp and Signal? The first main difference is that Telegram doesn't encrypt messages by default, while the other two do. To encrypt messages in Telegram it is necessary to activate optional E2EE feature called *"Secret Chats"* for every single private conversation you want to have. The feature is explicitly not turned on for the vast majority of conversations, is only available for one-on-one conversations (never for group chats with more than two people in them), activating *"Secret Chats"* in Telegram is oddly difficult for non-expert users to actually do, and even after activating this feature it only works if the conversation partner is online, and for the the last, *"Secret Chats"* are device-specific, meaning that if the feature is activated in the phone, it can't continue in a tablet or computer [4] [1].

Other difference to bear in mind is the encryption protocol used by Telegram. While WhatsApp and Signal's encryption protocol is open source, Telegram's approach to encryption is a customised protocol called MTProto, designed to protect communication between clients and servers. This means that it relies on server-client encryption for its standard chats, which reveals, by default, that Telegram is able to decrypt and read users' messages. This approach shows the difference from the more secure E2EE used by other messaging apps like Signal and WhatsApp, where even the service provider cannot read the messages [1].

One more aspect that should be taken into consideration is the way Telegram handles user data and encryption, having in mind the legal regulations in different countries. For instance, in the United States, companies are often required to comply with subpoenas that demand access to user data, including messages stored on servers, and since Telegram doesn't provide E2EE by default, the content of stored messages could be exposed to law enforcement authorities. On the other hand, companies in Europe have to comply with stricter privacy regulations, such as the General Data Protection Regulation (GDPR), but even so the metadata associated with Telegram users can be collected and stored, thereby presenting privacy risks [1].

III. Security Properties

As stated above, the *"Secret Chats"* feature is based on a costum protocol called, specifically, MTProto 2.0. This system uses a 2048-bit finite-field Diffie-Hellman key agreement and is believed to use a group of parameters chosen by the server, which introduces potential vulnerabilities if the server is compromised. The Man-in-the-middle (MITM) protection is handled by the end-users, who must compare key fingerprints. The resulting keys are then used to power non-standard authenticated encryption mode called Infinite Garble Extension (IGE) based on AES and with SHA2 handling authentication. This whole protocol raises many questions from cryptography experts, so much so that Matthew Green, cryptography expert

and renowned professor at Johns Hopkins University, quotes "Suffice it to say that Telegram's encryption is unusual." [4]. This means that the MTProto's unconventional choices and lack of clarity make it difficult to trust.

However, there is another aspect that must be taken into consideration, which is the information about who is being spoken to, when and for how long, in other words, the metadata. Typically, this kind of information is not protected with E2EE and, furthermore, metadata is very valuable and attractive to third parties, including advertisers and governments [1]. Since the data is stored on Telegram's servers and available to anyone, it is very likely that it will be collected by whoever wants to collect it [4].

IV. Security Measures

Despite Telegram's limitations when it comes to security, there are ways for users to better protect their data and therefore improve their privacy. These additional security measures include [5] [2]:

- **Enable "Secret Chats":** This feature guarantees E2EE so that conversations remain private without being compromised.
- **Enable two-factor authentication (2FA):** With 2FA a second layer of protection is added to ensure that no one gains unauthorised access to our Telegram account.
- **Adjust the privacy settings**: In Telegram's settings, there is a security section that allows users to limit who can see their personal and other information.
- **Keeping Telegram up-to-date:** Having the latest security and system vulnerability patches prevents cybercriminals from breaking into people's accounts.
- **Apply Strong Passwords:** Passwords with a minimum number of characters, combining uppercase and lowercase letters with numbers and symbols, are always a security recommendation. Also avoid using the same password for several accounts, as well as passwords that are easy to guess.
- **Use a virtual private network (VPN):** A reliable VPN offers extra security layer by covering online activities with encryption. It hides the IP address so that different entities online won't be able to track the actual location. VPN also protects against phishing scams and malicious links to malware and DDoS attacks.

In addition to all these security measures, there are many others, such as disable active sessions on other devices, delete messages for ultimate privacy, use a proxy server to hide the IP address, send self-destructing media, among others [3], all of which contribute to improving security. Naturally, all these security measures are recommended, but they only make sense if the user thinks so, in other words, whether or not he decides to implement any security measures.

V. Conclusion

In conclusion, it is confirmed that Telegram is indeed encrypted but while it presents itself as an *"encrypted messenger"*, the reality of its encryption capabilities is more nuanced. Telegram differs from other messaging apps (including Signal and WhatsApp) in that it does not provide E2EE by default, offering the ability to use only so-called *"Secret Chats"* for optional E2EE-conversation. For normal chats, Telegram defaults to server-client encryption, so the service can in fact access your messages — a far cry from the true privacy you might expect with an encrypted platform. Additionally, Telegram's MTProto encryption protocol has been criticized by cryptographers for its unusual design and with security being questionable due to the proprietary nature of the technology.

Despite all the limitations mentioned throughout the paper, Telegram offers additional security features such as 2FA, privacy settings adjustments, and optional security practices like using a VPN or strong passwords, which can improve user privacy. Nevertheless, the app's server-based, metadata-hungry design still leaves too many risks — especially around surveillance and third-party abuse of that tracking data.

Now, while Telegram can be somewhat private using its options it does not offer the same level of security as a more privacy-focused alternative such as Signal by default. Users will have to be proactive in learning and implementing Telegram's security settings for privacy — this is still not a failsafe way of maintaining the highest level of security, as the platform might potentially still be leaky.

References

[1] Is telegram really encrypted? a deeper look into its protocol. https://www.protectstar.com/en/blog/telegram-encryption, August 2024. (Accessed on 09/30/2024).

[2] Is telegram safe and should you use it? — veepn blog. https://veepn.com/blog/is-telegram-safe/, September 2024. (Accessed on 10/02/2024).

[3] Aashika Jain Anchit Sharma. Is telegram safe? how to secure your chats – forbes advisor india. https://www.forbes.com/advisor/in/business/software/is-telegram-safe/, March 2024. (Accessed on 10/02/2024).

[4] Matthew Green. Is telegram really an encrypted messaging app? – a few thoughts on cryptographic engineering. https://blog.cryptographyengineering.com/2024/08/25/telegram-is-not-really-an-encrypted-messaging-app/, August 2024. (Accessed on 09/30/2024).

[5] Monika Grigutytė. Is telegram safe? — nordvpn. https://nordvpn.com/pt/blog/is-telegram-safe/, February 2024. (Accessed on 09/30/2024).