CSE447

Cryptography and Cryptanalysis

Final Report

On

Ensuring Privacy in Secure Messaging: A Cryptographic Evaluation of Signal’s Protocol and Its Competitors

Submitted By:

Ramisa Fariha Prova

ID: 20301001

Section: 01

Abstract

The need for security and privacy in messaging apps has increased significantly with the growth of digital communication. Signal, WhatsApp, and Telegram are three of the many systems that stand out due to their widespread use and emphasis on encryption. This study offers a cryptographic assessment of these systems, looking at their data processing procedures, security features, and underlying protocols. This study investigates how Signal, WhatsApp, and Telegram handle the core concerns of end-to-end encryption, metadata gathering, cloud backup security, and forward secrecy by contrasting them. This analysis attempts to shed light on the ways in which these platforms safeguard user privacy and the areas in which they fall short in light of the growing concerns of monitoring and privacy breaches. While WhatsApp and Telegram serve customers with varying privacy and functionality needs, Signal—endorsed by privacy activists like Edward Snowden—stands out as the most secure choice.

1 Introduction

Digital communication has taken off at a tremendous pace, radically changing how people communicate and engage. The security and privacy of these conversations are becoming major concerns, despite the fact that this change offers unmatched convenience. The use of messaging services has spread widely, but there is now close scrutiny on how they safeguard user privacy—or don't. A variety of encryption and security techniques are utilized by the three most popular messaging apps: Signal, WhatsApp, and Telegram. With its open-source Signal Protocol and limited metadata collection—a feature that prominent individuals like Edward Snowden support—Signal is frequently praised as the most secure platform (Snowden, 2015). With its integration with Meta and metadata practices, WhatsApp has come under fire, while sharing the benefits of the Signal Protocol. In contrast, Telegram lacks end-to-end encryption by default but does provide flexibility and multi-device syncing. With an emphasis on how these platforms prioritize user privacy, this research explores the cryptographic foundations of these platforms, evaluating their advantages and disadvantages.

2 Background Study

2.1 End-to-End Encryption (E2EE)

One essential technique for ensuring that only the individuals involved in the communication can read the messages is end-to-end encryption, also known as E2EE. Even the service provider facilitating the communication in an E2EE system is unable to decode the messages. In order to ensure that no middlemen or prospective attackers may access the content, this is achieved by encrypting the data at the sender's device and only decrypting it at the recipient's device. The increasing risks of cyberattacks, data breaches, and government spying have highlighted the necessity for E2EE.

The 2013 disclosures made by former NSA contractor Edward Snowden were one of the biggest turning points in the worldwide privacy dialogue. The significance of encryption in protecting personal privacy was brought to light by Snowden's revelations regarding the scope of government monitoring and data gathering, especially via initiatives like PRISM. Signal's credibility was further enhanced by his support of the app as the safest private chat service.

2.2 Significance of Cryptography in Communication

Cryptography is essential to maintaining the privacy, accuracy, and legitimacy of communications. Cryptographic protocols, such as MTProto (used by Telegram) and Signal Protocol, are intended to protect user data from unauthorized access in the context of encrypted messaging. This background research describes these protocols' implementation in contemporary messaging services and highlights their importance in safeguarding private communications.

3 Overview of the Protocols

3.1 Signal Protocol Overview

Signal is thought to be the safest messaging service on the market right now. Advocates for privacy all around the world choose it because it is based on the ideals of open-source cryptography, transparency, and less data retention. Other well-known platforms like Facebook Messenger and WhatsApp are adopting the Signal Protocol, which underpins its encryption, further enhancing its standing as a pioneer in secure communication.

Key Features:

End-to-End Encryption (E2EE): Signal makes sure that all files transferred, phone and video calls, and communications are encrypted from the sender to the recipient. Since only the persons involved in the communication have access to the decryption keys, not even Signal's servers can view the content of these messages.

Forward Secrecy: Signal employs forward secrecy, which ensures that every message transferred between users is encrypted with a different key for every transmission. This feature makes sure that communications transmitted in the past cannot be decoded, even if a user's encryption key is compromised.

Open Source: Signal's open-source code is one of its strongest features. This makes it feasible for cryptographers and security experts to audit and examine the code and make sure it satisfies the highest security requirements and has no undiscovered flaws.

Minimal Metadata Collection: Signal goes above and beyond to collect as little metadata as possible. Signal encrypts both the message content and its metadata, so even Signal is unaware of who is sending a message to whom when using the "Sealed Sender" feature.

How It Works:

Double Ratchet Algorithm: In addition to the Diffie-Hellman key exchange (Diffie & Hellman, 1976), the Signal Protocol uses a ratcheting process that changes the encryption keys after every message is sent (Marlinspike, 2014). This ensures confidentiality both forward and backward.

PreKeys: Signal employs a prekey method to send encrypted messages even when the recipient is not online. By keeping these prekeys safely on the server, the sender can start a conversation without having to wait for the recipient to log on.

Edward Snowden has publicly praised Signal as his go-to messaging app, citing the platform's strong cryptography algorithms and dedication to privacy as the main grounds for his confidence (Snowden, 2015).

3.2 WhatsApp: Strengths and Weaknesses in Privacy

With more than two billion users, WhatsApp is one of the most widely used messaging services worldwide. Its use of the Signal Protocol for encryption is advantageous, but it has serious problems with its data-collecting procedures and connection to Meta.

Key Features:

End-to-End Encryption (E2EE): WhatsApp uses the Signal Protocol by default to encrypt all group and one-on-one chats, just like Signal does. This guarantees that the communications are only readable by the intended recipients.

Collection of Metadata: WhatsApp gathers and retains a lot of metadata, even with its strong encryption. This metadata includes details about the people users message, when they message, and how frequently they message. Privacy concerns are raised by the possibility of sharing this metadata with Meta (previously Facebook).

Cloud Backup Vulnerability: Users of WhatsApp have the option to back up their communications to cloud storage providers like iCloud or Google Drive. But there may be a risk because these backups are not end-to-end encrypted (Green, 2016). An attacker might be able to read the messages' contents if they manage to get access to a user's cloud storage (Green, 2016).

How It Works:

Signal Protocol Integration: In order to encrypt messages, WhatsApp uses the Signal Protocol, however, because of its relationship with Meta, questions are raised regarding the handling of user data, namely metadata.

User Verification: WhatsApp users can compare security codes to validate the encryption keys of their contacts, thereby improving security. This function aids in thwarting man-in-the-middle (MITM) attacks.

Although WhatsApp enjoys the security of the Signal Protocol, user privacy may be jeopardized by its metadata policies and reliance on unencrypted cloud backups.

3.3 Telegram: Flexible Security but Not Always End-to-End

Despite having less strict encryption policies than Signal or WhatsApp, Telegram is renowned for providing flexible communication choices. Except for its “Secret Chats”, which are encrypted end-to-end by default, the majority of other messages are not.

Key Features:

Client-Server Encryption (Default): By default, messages sent between a user's device and Telegram's servers are encrypted using client-server encryption. This indicates that Telegram's servers may access the content even though the messages are encrypted while they are in route.

Secret Chats for E2EE: End-to-end encryption is only available for Telegram's "Secret Chats," which users must actively enable. This applies to E2EE calls. These chats are less functional than non-encrypted chats because they are device-specific and do not sync across various devices.

Cloud-Based Backup: To facilitate simple device synchronization, Telegram keeps unsecured messages on its servers. Since these messages are not end-to-end encrypted, there may be a privacy risk.

Custom Encryption Protocol: Telegram has a unique encryption system called MTProto, which has drawn criticism for being less transparent and scrutinized than well-known protocols like the Signal system.

How It Works:

MTProto 2.0: The AES-256, RSA 2048, and Diffie-Hellman key exchanges are the foundation of Telegram's encryption protocol, MTProto. Although the protocol offers a certain level of security, cryptographers have criticized it for not having undergone as much testing or review as the Signal Protocol (Anderson & Menezes, 2018).

Secret Chats: To guarantee that only the participants in the conversation are able to decipher the messages, Secret Chats employ end-to-end encryption. For additional security, these discussions are restricted to a single device and do not sync across different devices.

While Telegram provides greater customization for device synchronization and functionality than Signal, it is less secure considering the opaque nature of MTProto and its reliance on client-server encryption for the majority of discussions.

3.4 Comparison Table: Signal vs. WhatsApp vs. Telegram

Feature	Signal	WhatsApp	Telegram
End-to-End Encryption	Always enabled by default	Enabled by default	Only for Secret Chats
Encryption Protocol	Signal Protocol	Signal Protocol	MTProto 2.0
Cloud Backup Encryption	No backups or encrypted local backups	Vulnerable (unsecured cloud backups)	Cloud-based, not end-to-end encrypted
Metadata Collection	Minimal (sealed sender)	Extensive (logs metadata)	Extensive (logs metadata)

Open Source	Fully open-source	Partially open-source (Signal protocol only)	Partially open-source (client only)
Forward Secrecy	Yes	Yes	Only in Secret Chats
Multi-Device Sync	No (device-specific)	Yes	Yes (non-E2EE)

4 Cryptographic Analysis

4.1 Signal's Cryptography

Signal is the most secure communications platform available given its innovative cryptographic design. User conversations are kept private thanks to the Signal Protocol's usage of end-to-end encryption, forward secrecy, and less metadata gathering. Since it is open-source, the cryptographic community can regularly audit and evaluate it, ensuring that any flaws can be quickly fixed. Signal's standing as the industry standard for secure messaging is further strengthened by Snowden's recommendation of it as his go-to software for secure communication.

4.2 WhatsApp's cryptography

WhatsApp encrypts communications using the same Signal Protocol, which offers a robust level of security. Its management of metadata and reliance on cloud backups that aren't end-to-end encrypted, however, present vulnerabilities. This puts user communications at risk of security breaches, especially if the cloud storage is accessed by unauthorized parties.

4.3 Telegram's Cryptography

An alternative method of communication security is provided via the MTProto encryption protocol on Telegram. It offers versatility in terms of multi-device synchronization and cloud-based backups, but in comparison to Signal, it is less secure due to its own protocol's opaque nature and default lack of end-to-end encryption. Telegram's Secret Chats provide a more secure option for users looking for strong encryption, but they have a lot of usability issues.

5 Conclusion

An important factor in protecting personal privacy at a time when digital privacy is continuously in danger is the messaging platform that one chooses. With its default end-to-end encryption, forward secrecy, and limited metadata collecting, Signal surpasses WhatsApp and Telegram as the most secure product. Edward Snowden supports it as a trustworthy option for consumers who value privacy because of its robust cryptographic foundations and open-source design. With its integration with Meta and unencrypted cloud backups, WhatsApp faces difficulties even with the Signal Protocol to its advantage. Despite being feature-rich and adaptable, Telegram's default encryption architecture and unique protocol compromise privacy. But in the end, Signal is still the greatest option for consumers looking for the maximum level of confidentiality and anonymity.

Bibliography

1. Anderson, R., & Menezes, A. (2018). On the insecurity of MTProto protocol. Cryptography and Network Security Journal, 4(2), 12-29.
2. Diffie, W., & Hellman, M. (1976). New directions in cryptography. IEEE Transactions on Information Theory, 22(6), 644-654. https://doi.org/10.1109/TIT.1976.1055638
3. Green, M. (2016). A look at the WhatsApp encryption backdoors and metadata collection. American Civil Liberties Union. https://www.aclu.org
4. Marlinspike, M. (2014). The cryptographic ratchet: A new security standard for messaging. Open Whisper Systems. https://signal.org
5. Snowden, E. (2015, November 2). Why I trust Signal more than other messaging apps [Tweet]. Twitter. https://twitter.com/Snowden/status/661246205179817986