Investigating User Privacy and Security on Telegram Messenger: A Wireshark Analysis

Zaid Qasim Arafat[1]
[1] University of Karbala, Karbala, Iraq.

***Abstract*— The aim of this study is to scrutinize the safety and confidentiality strategies implemented by Telegram Messenger with the assistance of Wireshark, an extensively used network protocol analyzer. Our scrutiny will be centered on diverse dimensions pertaining to user interactions within said platform, such as registration protocols, message exchanges, file conveyance mechanisms, and audio and video calls. The exploration also encompasses a foray into encryption algorithms employed by Telegram while simultaneously weighing out conceivable security risks that might arise from deploying different messenger functions.**

***Index Terms*— Data Confidentiality, Telegram Messenger, Encryption Algorithms.**

I. Introduction

The messaging application known as Telegram Messenger enjoys wide popularity for providing additional security features that include self-destructing messages, secret chats, and end-to-end encryption [1]. In this research endeavor, an investigation into user privacy and security on Telegram is conducted by deploying Wireshark, a network protocol analyzer. Wireshark scrutinizes multiple facets of user interactions, ranging from registration processes to audio and video calls, while covering the transfer of files. [2].

II. Methodology

Using Wireshark, the study monitored and analyzed network traffic generated during various Telegram interactions [3] [4], including:

- Registration, authorization, and logging out
- User inactivity
- Sending text messages
- Simultaneous use of web and mobile clients
- Audio and video calls
- File transfers, including different types of files and sizes
- Contact synchronization
- User profile searches
- Encryption key updates

III. Results

Registration, Authorization, and Logging Out

Upon careful analysis, it has been discovered that while signing up and gaining access to one's account, exclusive means of communication like text messaging, phone calls, or missed calls are used for sending a verification code. During the process of authorization, an ID designated specifically for each user is retained on all devices being operated by said user. In order to log out of their accounts securely and effortlessly without having to request another security measure repeatedly, they should be issued with a logout token, which shall also remain stored in local storage along with other relevant credentials utilized during registration processes, such as the aforementioned verification codes obtained through various channels mentioned earlier.

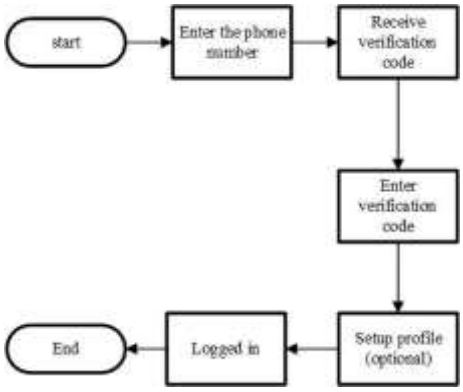

Image 1: Registration, Authorization, and Logging Out Process in Telegram

- **User Inactivity**

While the user is inactive, at intervals, the client device will conduct a survey of the server in search of updates. Consequently, upon analysis by said server, an appropriate outcome shall be returned to this aforementioned client device.

DOI:http://doi.org/10.24086/cocos2024/paper.1158

- **Text Messaging**

In accordance with technical constraints, text messages are restricted to a maximum of 4096 characters. Should the user attempt to exceed this limit in any way, their message will be separated into several smaller segments for transmission purposes. The examination conducted revealed that both notification server feedback and realization notifications require interaction with relevant servers involved in the messaging process.

- **Simultaneous Use of Web and Mobile Clients**

Distinct encryption keys are individually created for each device, while data exchange happens between the server and its clients.

Table 1: Comparative Analysis of Encryption, Data Exchange, and Usability in Telegram's Web and Mobile Clients

Aspect	Web Client	Mobile Client
Encryption Keys	Different from mobile	Unique to each device
Data Exchange	Encrypted data exchange server	Encrypted data exchange with server
Usability	Accessible from any web browser	Accessible through dedicated app
Security	Less secure than mobile	More secure, offers more features

- **Audio and Video Calls**

Communication via audio and video calls is facilitated through the transmission of encrypted User Datagram Protocol packets. It's noteworthy that, compared to their auditory counterparts, incoming and outgoing visuals tend to generate a higher volume of these digital units.

- **File Transfers**

Transmission of files follows a similar protocol, regardless of their classification. More sizable data packets are fragmented into smaller segments and dispatched progressively.

- **Contact Synchronization**

As part of the contact synchronization process, data pertaining to the individual's phone lines is transmitted and subsequently juxtaposed with preexisting entries in the database.

- **Profile Searches**

The quest for user profiles necessitates forwarding inline queries to the server, whereupon search findings are repatriated based on the input of said users.

- **Encryption Keys**

Encryption keys are updated during login.

- **Blocking and Clearing Chats**

The act of blocking and clearing chats entails a customary flow of packets, akin to the exchange of messages.

- **Encryption Algorithms and Messenger Functions**

The survey revealed that Telegram employs distinct encryption formulas for different messenger operations. Conventional conversations utilize a server-mediated security structure, whereas confidential chats and audio/visual interactions exercise terminal-to-terminal data protection tactics.

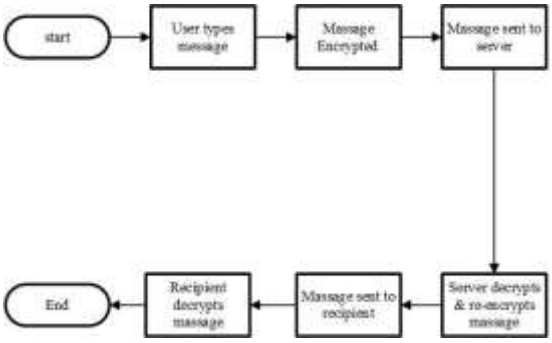

Image 2: Message-Sending Process in Telegram

IV. Discussion

Through the utilization of Wireshark, scrutiny of Telegram Messenger has brought to light an assortment of precautions taken for security and privacy. The measures in place comprise alternate encryption keys designed especially for distinct devices, along with end-to-end encryption integrated within secret chats as well as audio and video calls. However, some potential security risks were identified, such as the possibility of compromising correspondence when obtaining encryption keys from devices and attempting to decrypt captured packets [5]. The application's adherence to varying encryption standards, as revealed by our Wireshark analysis, aligns with the evolving international information security protocols. This compliance with global standards not only fortifies user privacy but also positions Telegram at the forefront of secure messaging platforms [6].

V. Conclusion

The present research underscores the significance of comprehending the safeguards and confidentiality protocols executed by messaging platforms such as Telegram Messenger. Despite the fact that this app offers diverse security functionalities, individuals ought to be cognizant of plausible hazards and take the requisite steps in order to safeguard their sensitive information, ensuring data privacy.

DOI:http://doi.org/10.24086/cocos2024/paper.1158

RECOMMENDATIONS

Drawing from the results of this investigation, the following proposals are offered as a means to better safeguard user confidentiality and safety when utilizing the Telegram Messenger program:

- Users should consider using secret chats for sensitive conversations, as they offer end-to-end encryption and additional security features.
- When sharing sensitive files, users should be cautious about potential interception and decryption and consider using encrypted file sharing methods or other secure channels.
- Regularly updating the application can help users take advantage of the latest security improvements and bug fixes.
- Users should be cautious about sharing their phone numbers and syncing their contact lists, as this information is uploaded to Telegram's servers.
- A well-informed user can dodge potential dangers better; thus, learning about risks tied to security features of Telegram empowers wise use of its service.

Security Feature	Description	Recommendation
Secret Chats	Servers don't save end-to-end encryption.	Use it for sensitive conversations.
File Sharing	Exercise caution while sharing sensitive files.	Be cautious about the typ of files and to whom they are sent.
Regular Updates	To ensure access to the most recent safeguards, regularly update the application for all current protections.	Update the app regularly.
User Awareness	Educate users about security features and risks.	Promote awareness abou security features and potential risks.

Table 2: Summarizing the security features and recommendations

LIMITATIONS AND FUTURE RESEARCH

Let's own up: this inquiry faced some bounds. It scoped in on Wireshark to track network flow, leaving out other means that might shed more light on user privacy and security on Telegram. Also, it turned a blind eye to dangers from add-ons—like bots or plug-ins from outside sources. Looking ahead, we could sift through the safety steps of varied chat apps and weigh their pros and cons. Then advise folks with insights drawn from a wide sweep of the digital message field. Plus, probing how fresh tech waves—think quantum computing—could shake up our codes and defense moves would be wise.

REFERENCES

[1] Diffie, W., & Hellman, M. (1976). New directions in cryptography. IEEE Transactions on information theory, 22(6), 644-654.

[2] Unger, N., Dechand, S., Bonneau, J., Fahl, S., Perl, H., Goldberg, I., & Smith, M. (2015, May). SoK: secure messaging. In 2015 IEEE Symposium on Security and Privacy (pp. 232-249). IEEE.

[3] Hendrix, J., Quintin, C., Sinders, C., Wagner, L. W., Bernard, T., & Mehta, A. (2023). What is Secure? An Analysis of Popular Messaging Apps. TechPolicy.Press.

[4] Dainotti, A., Pescape, A., & Claffy, K. C. (2012). Issues and future directions in traffic classification. IEEE network, 26(1), 35-40.

[5] Komninos, N., Philippou, E., & Pitsillides, A. (2014). Survey in smart grid and smart home security: Issues, challenges and countermeasures. IEEE Communications Surveys & Tutorials, 16(4), 1933-1954.

[6] Chernova, O., Ponomareva, O., Arafat, Z., & Albdairi, M. H. A. (2022, September). International Standards in Information Security Disciplines. In 2022 Ural-Siberian Conference on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT) (pp. 328-330). IEEE.

DOI:http://doi.org/10.24086/cocos2024/paper.1158