Cryptographic vulnerabilities on popular Telegram messaging platform

16 July 2021

Credit: CC0 Public Domain

Researchers from Royal Holloway, University of London are part of a team who have completed a substantial security analysis of the encryption protocol used by the popular messaging platform, Telegram, with over half a billion monthly active users.

Cryptography is the science protecting information from eavesdropping or tampering. We use it every day when we browse the web, make a bank transaction or chat on WhatsApp or Telegram. Cryptographers secure computer and information technology systems by creating and studying, for example, algorithms for encryption or for digital signatures.

As a result of their work, the researchers found several cryptographic weaknesses in the protocol that ranged from technically trivial and easy to exploit, to more advanced.

The team included Chair of Information Security and Director of the Cryptography Group, Professor Martin Albrecht and Ph.D. researcher, Lenka Mareková, from the Information Security Group (ISG) at Royal Holloway, along with Professor Kenneth G. Paterson and Dr. Igors Stepanovs, from the Applied Cryptography Group at ETH Zurich.

Talking about the findings, Professor Martin Albrecht, said: "The results from our analysis show that for most users, the immediate risk is low, but these vulnerabilities highlight that prior to our work, Telegram fell short of the cryptographic guarantees given by other deployed cryptographic protocols such as Transport Layer Security (TLS)."

TLS is a cryptographic protocol designed to provide communications security over a computer network and is widely used in applications such as web browsing, instant messaging and email.

He added: "Our work was motivated by other research we have recently done in the Information Security Group at Royal Holloway, which examined the use of technology by participants in large-scale protests such as those seen in 2019/2020 in Hong Kong. Our findings were that protesters critically relied on Telegram to coordinate their activities, but that Telegram had not received a security check from cryptographers."

Telegram uses its bespoke "MTProto' protocol to secure communication between its users and its servers as a replacement for the industry standard TLS protocol.

By default, Telegram only offers a basic level of protection by encrypting traffic between clients and servers. In contrast, end-to-end encryption, which would protect communication also from the prying eyes of Telegram employees or anyone who breaks into Telegram's servers, is only optional and not available for group chats. Since prior research indicated that many users in higher risk environments rely on these group chats, the research team focussed their efforts on the use of MTProto to secure communication between

Telegram clients and servers.

For more information on the vulnerabilities that were discovered, click here.

However, the results also show that Telegram's MTProto can provide security comparable to TLS after the changes suggested by the research team were adopted and if special care is taken when implementing the protocol. The Telegram developers have told the research team that they have adopted these changes.

This good news comes with significant caveats:

- Cryptographic protocols like MTProto are built from cryptographic building blocks such as hash functions, block ciphers and public-key encryption. In a formal security analysis, the security of the protocol is reduced to the security of its building blocks. This is no different to arguing that a car is road safe if its tires, brakes and indicator lights are fully functional. In the case of Telegram, the security requirements on the building blocks are unusual and because of this, these requirements have not been studied in previous research. Other cryptographic protocols such as TLS do not have to rely on these special assumptions.
- The researchers only studied three official Telegram clients and no third-party clients. However, some of these third-party clients have substantial user bases. Here, the brittleness of the MTProto protocol is a cause for concern if the developers of these third-party clients are likely to make mistakes in implementing the protocol in a way that avoids, e.g. the timing leaks mentioned above. Alternative design choices for MTProto would have made the task significantly easier for the developers.

UPDATE (7/17/2021): These findings helped further improve the security of the protocol: the latest versions of official Telegram apps already contain the changes that make the four observations made by the researchers no longer relevant: telegra.ph/LoU-ETH-4a-proof-07-16

More information: The analysis is available online: mtpsym.github.io/

Provided by Royal Holloway, University of London