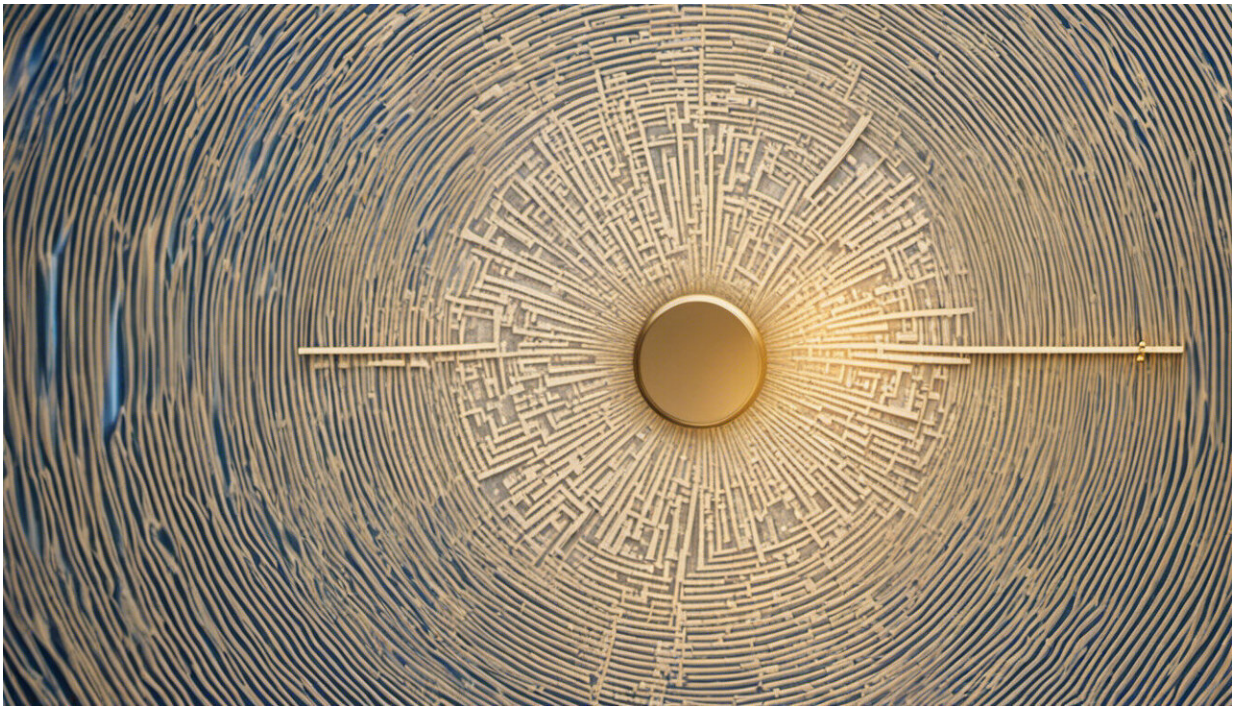
Unlocking the secret to private messaging apps

August 29 2022, by Cecilia Duong



Credit: AI-generated image (disclaimer)

Whether you're sharing confidential information or swapping movie ideas with a friend, people are turning to private messaging apps that offer end-to-end encryption to protect the contents of their conversations.

When data is shared over the internet, it often traverses a series of networks to reach its destination. Apps such as WhatsApp, owned by social media giant Meta (formerly Facebook), provide a level of privacy that even challenges Government agencies from accessing encrypted conversations.

However, with the apps constantly changing their security and privacy policies, are the messages still safe from being decrypted?

Back in May 2021, disapproval by the online community with the changes to WhatsApp's privacy policy for business entities using the platform, saw many users switch to other private messaging apps such as Signal and Telegram.

Cybersecurity expert, Dr. Arash Shaghaghi from UNSW School of Computer Science and Engineering and UNSW Institute for Cyber Security, compares encryption to the likes of having a secret conversation between you and another person.

"To keep our information away from prying eyes, we rely on cryptographic algorithms to encrypt our data. Encryption involves converting human-readable plaintext into an encoded format and the data can only be read after it's been decrypted," he says.

"Encryption involves using a key to lock a message, while decryption is using a key to unlock a message.

"In theory, if an outsider observed an encrypted conversation, they could not make sense of it, and they will need the appropriate key to decrypt it.

"Interestingly, with some end-to-end encryption protocols, such as Signal, even if someone steals the encryption keys and taps over the connection, they cannot decrypt messages already sent. In crypto

parlance, this is termed as forward secrecy."

Are our messages fully secure?

Modern encryption algorithms have been battle-tested and shown to have no known vulnerabilities. While it doesn't mean it's impossible to crack, the process requires extensive processing powers and could take a significantly long time to do. Quantum computers, if they mature enough, will be able to crack much of today's encryption.

Attackers commonly target endpoints and their vulnerabilities. This is much easier than cryptanalysis which is the process used to breach cryptographic security systems.

For instance, last year, attackers targeted a vulnerability related to WhatsApp's image filter functionality that was triggered when a user opened an attachment containing a maliciously crafted image file. There have been more serious and less complicated vulnerabilities reported targeting WhatsApp clients running on iOS and Android.

Dr. Shaghaghi says when you back up your messages on some of the messaging platforms, your messages are pushed to the cloud. This means that all your messages are now stored on someone else's computer.

"The service provider's implementation of end-to-end encryption plays a significant role in the security and privacy of a messaging app against the provider and attackers," he says.

"WhatsApp used to keep a backup of the messages in an unencrypted format over iCloud for Apple users and Google Drive for those who used WhatsApp in Android. Even though WhatsApp adopted an end-to-end encryption model in 2016, unencrypted backups were vulnerable to government requests, third-party hacking, and disclosure by Apple or

Google employees."

In 2021, WhatsApp rolled out an option for users to enable end-to-end encryption of their backups. While this was welcomed as a positive step forward, it should be the default for all users—not offered as an option, says Dr. Shaghaghi.

"Users concerned about the security and privacy of their data must make sure to enable the end-to-end encryption backup for WhatsApp and other messaging platforms."

What about Signal and Telegram?

Unlike WhatsApp and Signal, Telegram does not have end-to-end encryption enabled by default. Only when the "secure chat" function is enabled, Telegram applies the MTProto protocol, an open-source and custom-developed protocol by the messaging provider.

"As far as we know, Signal, Telegram and WhatsApp are secure in providing end-to-end encryption, if the option is enabled," says Dr. Shaghaghi.

"However, Signal is built with privacy and security as the primary motivation. Signals' endpoint source code is also available to the public—this allows anyone to inspect the code and identify vulnerabilities.

"I believe the consensus is that Signal is a more secure and privacy-friendly messaging solution when compared to WhatsApp, Telegram, or Facebook Messenger."

With so many messaging platforms available on the market, Dr. Shaghaghi says there are some simple steps to take to help safeguard a

user's privacy.

"Messaging platforms contain a lot of private information so it's worth ensuring that the platform we use has a good reputation for ensuring the security and privacy of its users," he says.

"It is also worth spending a few extra minutes to enable some of the more advanced security features these platforms offer, such as end-to-end backup encryption or multi-factor authentication.

"And whichever platform you decide to use, it's best practice to ensure we use the latest version of the apps and avoid downloading apps from third-party stores."

Moderating content exchanged over end-to-end encrypted messaging platforms

There have been strong calls by different Government organizations for these apps to include backdoors which would provide access to data when deemed required by authorities.

Recent leaks from the U.S. Federal Bureau of Investigation (FBI) demonstrated that even with a subpoena, powerful government entities have limited access to messages exchanged over apps that use end-to-end encryption.

This argument is especially worrying for many users who are concerned that it's the first step away from the strong encryption principles that they rely on to ensure the security and privacy of their data.

There have been ongoing debates in Australia and overseas regarding this topic.

"From a security engineering perspective, implementing a backdoor is never a good idea," says Dr. Shaghaghi.

"There is no guarantee that malicious hackers do not find out about these backdoors too and exploit them.

"However, those in favor of a solution allowing access for law enforcement agencies argue that they need access given the increasing usage of these platforms by criminals."

Some messaging providers and tech companies have responded by making changes to the functionality of the platform.

"To meet regulatory requirements, WhatsApp now allows users to flag a message to be reviewed by their moderators. This needs to be initiated by a user and when a message is flagged, the few messages before it is also forwarded to WhatsApp moderators," says Dr. Shaghaghi.

"Apple has promoted encrypted messaging across its ecosystem and have fought off law enforcement agencies looking for records.

"In 2021, they announced child safety features that include detecting sexually explicit pictures over iMessage, another platform using end-to-end encryption. To implement this feature, Apple plans to implement the detection on the device and not through an encryption backdoor.

"I think we can balance the need for moderating criminal content and security and privacy requirements by breaking down the problem into more specific use-cases and developing innovative solutions."

Provided by University of New South Wales