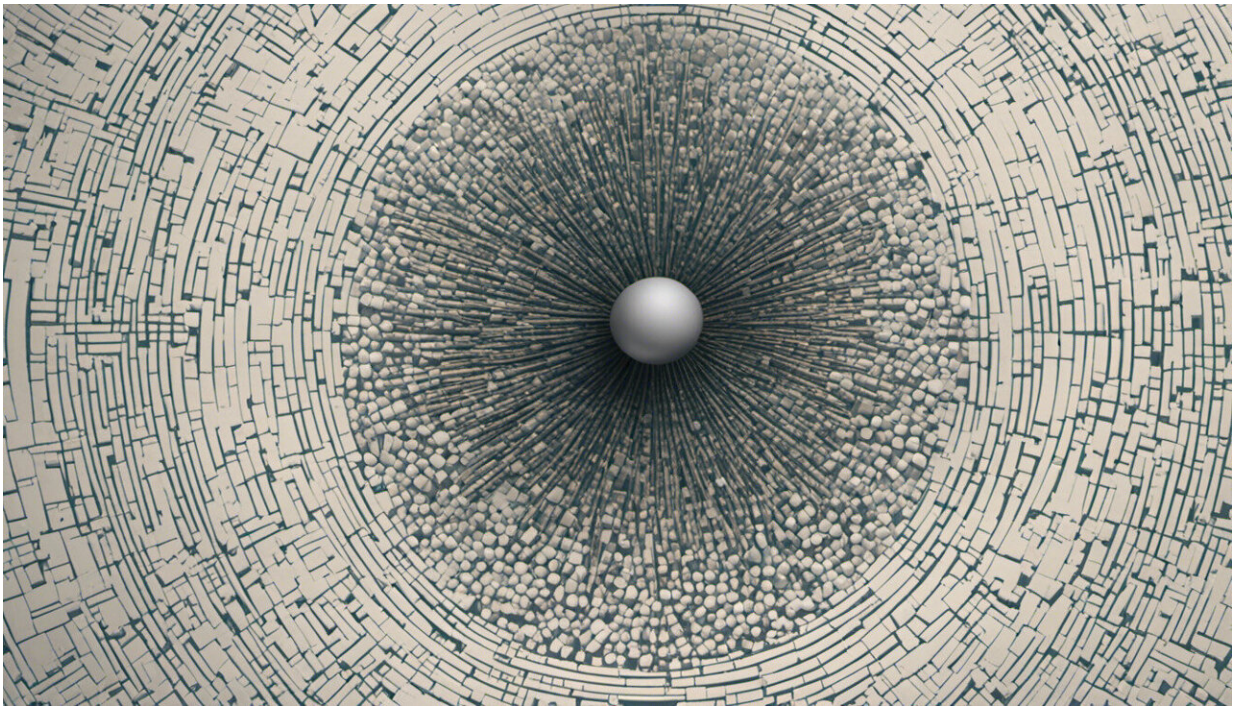
How WhatsApp encryption works – and why there shouldn't be a backdoor

March 28 2017, by Antonis Michalas



Credit: AI-generated image (disclaimer)

A battle between national security and privacy is brewing. Governments and secret services are asking encrypted messaging services such as WhatsApp to allow them access to users' data. Most recently, in the wake of the March attack at Westminster, Amber Rudd, the UK home secretary, said it was unacceptable that the government couldn't read the

encrypted messages of suspected terrorists.

The main argument behind this request is that access to messages will allow authorities to thwart future terror attacks. On the other hand, there are many ordinary people who use messaging apps for daily communication and this request would be a direct breach of their privacy. But this isn't the only problem – creating a way for the authorities to read encrypted messages would also make the system vulnerable to cyber attacks from criminals and other hackers, removing what makes it a secure way to communicate in the first place.

How does encryption work?

Encryption is simply a way for two or more users to exchange messages securely. Encryption algorithms are like a box with two locks. For example, if a user called Alice wants to send her friend Bob a secure message, she puts it in the box and locks it with her key. Then, she sends the locked box to her friend Bob, who can only open the box and read Alice's message if he has a valid key of his own.

But to be able to communicate with new users, you need a way of sharing keys that is still secure. To get over this, each user has what's called a public key that is available to anyone and proves the identity of the user, and a private key that stays with the user. Alice uses Bob's public key to lock the box, but it can only be unlocked with Bob's private key.

WhatsApp's system adds a further level of encryption, known as "perfect forward secrecy". This is like a second lock with a key that changes for every messaging session. When Alice wishes to send a message to Bob, she first generates a fresh session key, places it in the box and uses Bob's public key to lock it. She then sends it to Bob, who uses his private key to access the session key. The two of them can then start communicating

securely using that session key known only to them to encrypt their messages.

This system guarantees that there is no single key that will give access to all the data sent between Alice and Bob in the past or future. In other words, even if a key is compromised, it will only unlock a few messages before it becomes useless.

However, WhatsApp's previous system meant that the company was able to access the keys and so in theory could easily unlock the messages, breaching Alice's privacy. Last year, the company introduced what's called "end-to-end encryption", which seems to have solved this problem. Alice and Bob now use keys that WhatsApp doesn't keep specific details of, meaning only Alice and Bob can unlock their messages.

What government wants

The way WhatsApp now works makes it impossible for a third party to unlock the messages that Alice and Bob exchange. The only way a third party, such as the police or intelligence services, can access users' messages is if WhatsApp removes the end-to-end encryption and switches back to the old version of the software, or if a backdoor is installed.

A backdoor can be seen as software built into the app that allows you to circumvent or undermine security protections and surreptitiously access systems and data. In WhatsApp's case, this would be software that gives access to all keys that users are generating. Governments argue that such a mechanism would be only activated if there was a warrant to access the messages of a suspicious user. Upon activation of the backdoor, WhatsApp would recover the keys that were generated by the corresponding users in order to decrypt their messages. This would allow

WhatsApp to reveal all the information sent by a particular user.

But backdoors also create a vulnerability in the software or system that intruders can use to gain access to a system or users' private data. As a result, if WhatsApp adds a backdoor to the software then it would no longer be a secure way to communicate and so it would lose a key part of its appeal. It's also likely that installing such a mechanism would mean that intelligence agencies would be knocking on WhatApp's door every day asking them to reveal someone's messages.

Ultimately, if someone thinks that removing WhatsApp encryption would be the solution, then they don't understand the actual problem. Even if you were to remove the end-to-end encryption from WhatsApp, criminals could create their own, similar, software that would allow them to communicate securely, while ordinary users would lose the ability to send genuinely private messages.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation

Citation: How WhatsApp encryption works – and why there shouldn't be a backdoor (2017, March 28) retrieved 18 April 2024 from https://techxplore.com/news/2017-03-whatsapp-encryption-shouldnt-backdoor.html