Application of end-to-end encryption in whatsapp

Law, Security

January 2018 brought the surprisingly impossible fact that “ WhatsApp end-to-end group chats” are not secure anymore. A person who is not a group member can secretly eavesdrop on your private end-to-end encrypted group chats on WhatsApp. The main aim of having end-to-end encryption is to stop trusting the transitional servers in such a way that no one, not even the company or the server that transmits the data, can decrypt your messages or misuse its centralized position to manipulate the service. Trusting this fact many business companies, financial discussions, secret policies, private data shared through WhatsApp is no more secure now. It has been found that anyone who controls WhatsApp/Signal servers can covertly add new members to any private group. And they can spy on group conversations, even without the permission of the administrator.

WhatsApp failed to properly authenticate that who is adding a new member to the group, it is possible for an unauthorized person – not a group administrator or even a member of the group – to add someone to the group chat. In fact, the worst thing about this is even it may possible that none of the group member can have the notification about addition of the unwanted member in the group. A compromised admin or reprobate employee with access to the server could manipulate or block) the group management messages that are supposed to alert group members of a new member. Additionally it can cache sent messages to the group, read their content first and decide in which order they are delivered to the members.

One of the possible ways to fix the issue is just by adding an authentication mechanism to make sure that the “ signed” group management messages come from the group administrator only.

The general mechanism is when a new member is added to a group the phone number of each member of the group automatically shares secret keys with that person, giving them full access to all future messages.

An attacker would have to take control of WhatsApp servers which means a sophisticated hacker. So the server can simply add a new member to a group with no interaction on the part of the administrator, and the phone of every participant in the group then automatically shares secret keys with that new member, giving him or her full access to any future messages.

Once an attacker with control of the WhatsApp server had access to the conversation, he or she could also use the server to selectively block any messages in the group, including those that ask questions, or provide warnings about the new entrant. And in groups with multiple administrators, the hijacked server could spoof different messages to each administrator, making it appear that another one had invited the eavesdropper, so that none raises an alarm. It could even prevent any administrator’s attempt to remove the eavesdropper from the group if discovered.

Solution: As for WhatsApp, the researchers write that the company could fix its more egregious group chat flaw by adding an authentication mechanism for new group invitations. Using a secret key only the administrator possesses to sign those invitations could let the admin prove his or her identity and prevent the spoofed invites, locking out uninvited guests. WhatsApp has yet to take their advice.

Although WhatsApp integrates the Signal key exchange protocol for direct messaging, keys in groups are used very differently: instead of sending encrypted messages to each group member separately, each user generates a symmetric key (chain key) for encrypting only her messages to the group. The key is then once transported to every other group member using the DR algorithm for direct messaging. The dedicated group key is not refreshed by Diffie-Hellman ratcheting but only with the symmetric key derivation function in contrast to direct messaging.