More is Less: On the End-to-End Security of Group Chats in Signal, WhatsApp, and Threema

Cosmin-Ionuţ Rusu

April 2019

The paper [1] proposes a comprehensive and realistic security model for group communication protocols. The proposal is then followed by a high-level description of three well-known protocols: Signal, WhatsApp and Threema; and an analysis of their security shortcomings by designing exploits targeted for each. The authors revealed that communication integrity and group closeness are not end-to-end protected for neither of the analyzed protocols.

1 Introduction

We can imagine a group communication as a group of persons communicating in a private conference room. In such a context, we can define the following vocabulary: traceable delivery - everyone in the room hears the communication; Authenticity: everyone knows who spoke; No duplication: how often words have been said; No creation: nobody outside the room can speak; Confidentiality: nobody outside the room can hear the communication inside; Closeness: the door is only open for invited persons.

Since all the three protocols have a central server, we will assume that the protocol has a central server that receives, caches and forwards messages from senders to receivers as soon as the receivers are online (asynchronous communication).

2 Security Model

2.1 Threat Model

There are multiple threats, and each of them can use different vectors of attack. The **Malicious User** is a user that does not follow the protocol. Another assumption is that the members of the target group behave correctly. The **Network Attacker** has full control over the communication network, may access and modify all unprotected traffic (not end to end protected). The **Malicious Server** has access to the group instant messaging protocol. A **Long-term Secret Compromise** is the action of

obtaining the long-term secrets of a user and the **Session State Compromise** is the action of obtaining the full session state of a user - which contain housekeeping variables and other secrets.

2.2 Security and Reliability

According to their definition, a protocol is a Secure and Reliable Group instant messaging protocol if it fulfills End-to-End Confidentiality, Message Authentication, No Creation, No Duplication, Traceable Delivery, Additive Closeness, and Subtractive Closeness in the presence of Malicious User, Network Attacker, and Malicious Server.

3 Signal

3.1 Group protocol

In Signal, Group Messages are treated as individual messages. For every group message, the sender will send each group member that respective message, encrypting the unique group identifier in the message so the recipients will know to put it in the correct conversation. As a result, the server is not able to distinguish between individual messages and group messages (due to the end to end encryption of the messages which include the group id). Unlike messages, acknowledges are not end to end encrypted and so, they rely only on the secure transportation layer. The Group Management protocol consists of two flow: the *Update flow* where a user sends the update group information to the other members (new group members or new group information), and the *Leave flow* when a user leaves the group. All the members of the group are admins in Signal and members cannot be removed.

3.2 Security Evaluation

An attacker (A) needs to know the phone number of at least one group member (B) and the group unique identifier, to **burgle** into it. This can come from either a Malicious User that was a former member of the group and recorded the identifier or as a result of compromising the session state of a member. After that, the user will send an update group message to B adding him as a member. B will gladly update his group members information locally, and as soon as he makes another update to the group (adds more members, changes the title), he will add A. As a result, A is not an admin since all members are admins in Signal, and he has full control over the group. An attacker (A) can also make a victim believe a message was successfully delivered to all the group members, while in fact, no one saw the message. In order to achieve this, the attacker needs to either control the Signal server, or the transport layer protection. This attack exploits the fact that Acknowledgements are not end to end encrypted. The attacker needs just to intercept all the messages, to drop them and to send back to the sender ACK messages.

4 WhatsApp

4.1 Group protocol

WhatsApp key exchange and initialization protocol are the same as Signal's, but the group management is significantly different, mostly due to the fact the WhatsApp server is responsible for the distribution of group messages. The number of users in a WhatsApp group is limited to 256. As a result, group updates are not end to end encrypted since WhatsApp Sever needs to know who are the members of a group to dispatch all the messages to the correct recipients. The server gets a message with the end to end encrypted message and group id (transport layer encrypted only), attaches the timestamps and other metadata and forwards it to each group member. As in Signal, acknowledgments are only protected on the transport layer.

4.2 Security Evaluation

WhatsApp suffers from the same vulnerabilities, although the steps are different. Suppose a group of three members, B (admin), C, and D. The attacker A can send a group update message to C and D adding himself as a member to the group. Receivers will send their keys back and now A will receive all the message that the server will dispatch. Again, since ACKs are not end to end encrypted, an attacker that has control over the server can forge acknowledgments or modify the messages timestamps (since the server attaches this information). WhatsApp server breaks *Additive Closeness* and *Traceable Delivery*.

5 Threema

Threema is a close source privately owned application. The biggest difference compared to Signal and WhatsApp is that there are no key derivation, only long term secrets.

5.1 Group protocol

Threema, similar to Signal, treats group messages as multiple messages. As a result, the Threema server cannot distinguish between group messages and individual messages. In contrast to WhatsApp and Signal, Threema does not support receipt status. Threema can have a reference to other messages (the reply-to feature). The creator of the group is the only admin. The group management protocol consists of two flow: the update flow where the users send the update group information (new set of members, or new group metadata), and the leave flow when a user sends the leave message with encrypted group id to all other members. One distinguishable feature of Threema is that the members of a group can request the admin to start

a sync action. The admin then sends his view of the group members and metadata, and they all agree on that information.

5.2 Security Evaluation

In Threema, an attacker A can replay messages. The attacker just needs access to the channel between the sender and the receiver. Since only the group id and the actual content is end to end encrypted, the attacker can update the timestamp (and all other metadata) and replay the encrypted message. Not only an attacker is able to break *No Duplication*, but the attacker can rewind every group manipulation by resending previous group update messages, breaking *Additive Closeness*. By the way it's designed, the protocol does not support *Traceable Delivery*. Moreover, there is no *No Forward and Future Secrecy* due to encryption with the same long term key. An attacker can also reorder messages since timestamp is not end-to-end encrypted. Finally, the protocol suffers from *Additional Information Leakage*: if a user sends a message to a group he is not part of, the admin does sync and responds to the user with the group members and the group information.

6 Conclusion

Designing a Group Instant Communication protocol is hard, and none of the three analyzed protocol satisfies the proposed definition of a secure and reliable protocol. The results were presented to the developers and some of them fixed the errors. The exploits presented here might then be outdated (the paper was released in January 2018).

References

[1] Paul Rösler, Christian Mainka, and Jörg Schwenk. More is less: on the end-to-end security of group chats in signal, whatsapp, and threema. In *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 415–429. IEEE, 2018.