CSCI968 Advanced Network Security - Final Research Report

CCNU Wollongong Joint Institute Due: 17:00PM, 05/30/2020

Description

Online messaging service has been playing an important role in people's daily life for social activities and other related businesses. The most widely used messaging services include Wechat, Whatsapp, Facebook, Line and so on. On the other hand, the privacy issues related to the messaging services are being discussed and investigated more and more often recently. The concept of the end to end encryption (E2EE) is proposed to mainly address the security issues that the private information may be compromised at the messaging server. In other words, in the scenario that messaging servers are required, which is the case for most of the asynchronous messaging services, messages communicated between two or multiple parties need to go through the servers for various functionality purposes. As a result, precautions need to be taken on whether the messages and other related information can be learned only by the end parties or not.

Signal is one of the most popular messaging services that claims to achieve the end to end encryption security level and what's more importantly, it is an open source project applying the noise cryptographic protocol framework[1], which is also used by Whatsapp, wireguard, facebook Messenger, Skype, and Google Allo.

In this research report, you are required to first understand how Signal messaging service work by referring to the documents [2, 3, 4] along with the source code [5]. Then based on the Signal framework, provide your solutions to the following two issues.

1. Group chatting is one of the important functions in the online messaging application. Users within the group should be able to communicate with each other securely; A users should be allowed to join or leave the group; messaging server should not be able to know the sensitive information regarding the group member identities, message content and so on. You are required to define the security goals in detail that you believe to be reasonable in the group chatting scenario, and provide the solution based on the Signal framework [2, 3, 4].

2. There are many popular messaging services which do not satisfy the E2EE security level, especially for the non-open source products. This is sometimes due to the auditing or other requirements by both the government and the company itself. Please provide the solution for this scenario so that the security requirements are satisfied as in the E2EE scenario except for the case that the messaging server is able to audit the corresponding communication session (message content, and user identity and so on). Please describe

how you can limit the damage if the messaging server is compromised.

Requirement

You are required to provide a research report on the above issues containing the related background introduction and the corresponding solutions. Protocols should be concrete including all the mathematical details of the primitives you would apply. Please explain the reason behind the design to support the correctness and security properties, and show that the design can indeed achieve the goals.

One technical report (12 pages in length excluding the references) should be submitted with the following format:

1. Title
2. Authors
3. Abstract
4. Introduction(including the Signal protocol and other related background)
5. Solution related to issue 1
6. Solution related to issue 2
7. Conclusion
8. Reference (10 related references should be referred in your report)

References

[1] T. Perrin, The noise protocol framework, PowerPoint Presentation (2016).
URL http://www.noiseprotocol.org/noise.html

[2] Double ratchet.
URL https://signal.org/docs/specifications/doubleratchet/

[3] X3dh.
URL https://signal.org/docs/specifications/x3dh/

[4] The sesame algorithm: Session management for asynchronous message encryption.
URL https://signal.org/docs/specifications/sesame/

[5] Signal source code.
URL https://github.com/signalapp