Signal messaging service technical report

Wangzhihui Mei
2019124044 6603385
CCNU-UOW JI

Abstract

1 Introduction

In the modern network environment, people have increasing demands for privacy protection. Now the world is worried that people s personal privacy will be violated, as people use instant messaging apps and services, where the service provider may be the vulnerable because of attacker can crack the server or perform Man-In-The-Middle attack in the case that only transmission encryption is adopted. In other scenario, the privacy of user is transparent to server, so service providers may acquire the content of communication as they want. To solve the natural weakness of transmission encryption, End-to-end encryption is introduced.

End-to-end encryption (E2EE) is a communication system where only users participating in the communication can read the information. In general, it can prevent potential eavesdroppers-including telecommunications providers, Internet services. Such systems are designed to prevent potential surveillance or corrective attempts, because it is difficult for third parties without keys to decipher Data transmitted or stored. Generally speaking, communication providers that use end-to-end encryption will not be able to provide their customers' communication data to the specification.

Signal is an excellent End-to-end encryption protocol.[1] It is very famous in both IT and security field and applied in WhatsappFacebook MessengerSkype, etc. The core algorithm of Signal protocol is X3DH and Double Ratchet, referring to the key agreement protocol "Extended Triple Diffie-Hellman" and one secure key management algorithm respectively.

2 Solution

2.1 Issue 1

2.2 Issue 2

3 Conclusion

References

[1] **Alwen, Joël, Sandro Coretti, and Yevgeniy Dodis**, "The double ratchet: Security notions, proofs, and modularization for the signal protocol," in "Annual International Conference on the Theory and Applications of Cryptographic Techniques" Springer 2019, pp. 129–158.