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 weakness of leaking privacy in the case that only transmission encryption is adopted.

Signal is an excellent End-to-end encryption protocol.

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.

2 Solution

2.1 Issue 1

2.2 Issue 2

3 Conclusion