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.[**?**] 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. We perform the analysis of Signal by introducing the privacy preserving requirement and principle of X3DH and Double Ratchet.

1.1 Privacy protection consideration

The most significant point of privacy-preserving is the content of the communication. The leakage of communication content will expose the private content of the communication party or cause scam attack to the communicating parties, which seriously interferes with normal work and life.

The confidentiality of the communicating parties is also important, that is to say, the identification of user should be unknown to unrelated third party as far as possible. This means trying to avoid the server from knowing and storing relevant information.

Unrecognizable communication protocol is needed as well. A third party who does not have the relevant key only get the communication content feature of time and communication length, while the characteristics of the transmission content seen on the channel should be consistent with the completely random flow. The probability of occurrence of the same string of the same length on the network should be consistent with the probability of the occurrence of the same sequence of the same length of the random string. This requirement is conducive to anti-protocol identification and firewall blocking.

The identity of the correspondent should be difficult to forge and easy to verify under the protocol. This is very conducive to preventing fraud. The generally accepted method is the first-time trust model. It also supports the authenticity and signature of account information and is difficult to change.

Besides, the leakage of the temporary key should guarantee the relevant degree of forward and backward security. Unless the permanent key is leaked, it should not cause much information leakage due to the key leakage.

Finally, the security of account should be considered. Every communication account should be fully protected during the creation and usage of it, making it extremely difficult for anyone other than the account holder to gain access to the communication account. This also means that once the account is lost, it will be almost completely unable to restore. In fact, if the account can be created in batches at will, it is also a huge threat to the social network system itself. It would be better to design a security mechanism to prevent the frequency of account creation or increase the cost of account creation. Blockchain management account creation may be a good way. Correspond the block to the account, and obtain the permission to create an account by obtaining a new block or buying someone else's empty block. The update of public account metadata information (including nickname and avatar, etc.) should be synchronized and re-signed and verified on the server. The update history should be viewable by the communicating party, and non-communication parties should not be able to consult other users' metadata information.

1.2 Required attributes of the protocol

The first attribute is the openness and verifiability of the protocol. The openness ensures that the protocols and algorithms used can be publicly verified and audited. At the same time, the system is reviewed by the public and it is easier to find defects and correct them in time. It helps different third parties to make different compatible implementation solutions, avoiding defects in the unified implementation to be centrally identified and targeted attacks.

The next attribute is the decentralization and autonomy. Any centralized or maintained by a commercial company may affect the system as the center weakens or the company changes. As a basic communication service, it takes a long time to vitalize the system’s services. Company maintenance. The system can add auxiliary functions to the central server and commercial companies to provide certain support for it, but the stable operation of the system cannot rely on these centralized prerequisites

The system is best to realize that anyone can add server resources to the system on the basis of donation or for some kind of income, which can be conveniently added to the server network and can be easily disconnected from the server network without affecting the overall operation of the network. .

2 Solution

2.1 Issue 1

2.2 Issue 2

3 Conclusion

References

[] **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.