Signal Protocol

Ridho Pratama
School of Electrical Engineering and Informatics
Institut Teknologi Bandung
Bandung, Indonesia
Email: 13516032@std.stei.itb.ac.id

***Abstract*—As technology keeps developing and getting more affordable for many people, the amount of their usage keeps increasing. One of their primary use is for communication. There is now an increasing demand for safe and secure messaging platform. To fulfill that, there need to be ways to safely sending data between devices. One of the way that that could be achieved is by using cryptography. This paper will talk about The Signal Protocol, a public key cryptography protocol which is being used by The Signal messaging app, and many other messaging platform such as WhatsApp, Facebook Messenger, and Google Allo.**

Keywords— cryptography; security; signal; public key; communication

I. Introduction

The Signal Protocol is a cryptographic protocol that can be used to provice end-to-end encryption for voice calls, video calls, and text messages. The protocol is introduced in the messaging application Signal. Later, many other messaging application such as WhatsApp and Facebook Messenger claimed to have been implementing the protocol for their application.

II. Cryptographical Aspects

A. Overview

The Signal Protocol is composed of many well-known cryptography algorithm for every step of the message encryption. It composes Double Ratchet algorithm, triple Elliptic-Curve Diffie-Hellman handshake, and uses Curve25519, AES-256, and HMAC-SHA256. This subsection will futher outlines the protocol steps.

The communication starts by each party generating their own keys by the format defined for X25519 and X448 elliptic curve Diffie-Hellman functions. This is defined as the XEdDSA signature scheme. These public keys are bundled and then sent to the key distribution center.

When the sender (will be named as Alice) wants to send a message to the receiver (will be name as Alice), she will requests Bob's key bundle fron the key distribution center. Alice and Bob then will establish a master shared secret key with the Triple Elliptic-Curve Diffie-Hellman (X3DH) algorithm.

When the shared key is established, both parties then can use the Double Ratchet algorithm to send and receive encrypted messages.

B. XEdDSA Scheme

XEdDSA signature scheme is used to generate EdDSA-compatible signatures using public key and private key format defined for X25519 and X448 elliptic curve Diffie-Hellman functions.

C. X3DH Algorithm

After both parties have generated their keys, both parties need to agrees on a shared secret key. The Signal Protocol uses Triple Elliptic-Curve Diffie-Hellman (X3DH) algorithm to achieve that. X3DH establishes a shared secret key between two parties who mutually authenticate each other based on public keys.

X3DH is designed for asynchronous settings where one user (Bob) could be offline but has published some information to the server. Another user (Alice) could use that information to send encrypted data to Bob and establish a secret key for future communication.

X3DH consists of three phases:

1) Bob publishes his identity key and prekeys to a server.
2) Alice fetches a "prekey bundle" from the server, and uses it to send an initial message to Bob.
3) Bob receives and processes Alice's initial messages.

In the first phase, Bob publishes a set of elliptic curve public keys to the server, which consists of:

- Bob's identity key. Only uploaded to the server once.
- Bob's signed prekey. Uploaded to the server at some interval, the new key will replaces the previous values.
- Bob's prekey signature.
- A set of Bob's one-time prekeys. Consists of many generated prekeys which are used uniquely for each run of the protocol. Server could requests new one-time prekeys to Bob when the amount stored in the server is running low.

In the second phase, Alice fetches a "prekey bundle" containing Bob's identity key, signed prekey, prekey signature, an optionally one-time prekey when available. Alice then verifies the prekey signature and aborts when fail. Then Alice generates a ephemeral key pair which only used per protocol run. Lastly Alice generates the secret key by using Diffie-Hellman function, and HMAC-based key derivation function (HKDF) when one-time prekey isn't available. After calculating the secret key, Alice deletes her ephemeral private key. Then Alice sends Bob an initial message containing her identity

key, ephemeral public key, identifiers for which Bob's prekey is used, and an initial chipertext encrypted with associated data which encrypted by the calculated secret key.

In the last phase, Bob receives Alice's initial message, loads his private keys, and then calculates the secret key with his private keys and Alice's keys in the message. After the secret key is calculated, Bob then could try to verify the encrypted message sent by Alice, if the encryption is success then both parties could start communicating with the secret key using post-X3DH algorithm, in this case the Double Ratchet algorithm.

D. Double Ratchet Algorithm

The Double Ratchet algorithm used by two parties to exchange encrypted messages based on a shared secret keys.

For every messages, each party will generate a new key to encrypt the messages so that earlier keys could not be used to calculate the later ones. The Diffie-Hellman public values is mixed into the generated keys so that later keys could not be derived from the earlier ones. These properties give protection to earlier or later messages in case of a key compromise.

1) Key Derivation Function Chain: Key Derivation Function Chain or KDF is the core of the Double Ratchet Algorithm. KDF is defined as a cryptographic function that takes a secret and random KDF key, some input data, and returns output data. KDF chain is when the output from a KDF is used as output key and to replace the used KDF key.

In a Double Ratchet session, each party stores KDF keys for three chains: a root chain, a sending chain, and a receiving chain. As Alice and Bob exchange messages, they also exchange new Diffie-Hellman public keys, and the output from the DH become input to the root chain, this is called the Diffie-Hellman ratchet. The sending and receving chain advances as the exchange of messages goes on, this is called the symetric-key ratchet. These two ratchet are used together to construct the Double Ratchet algorithm.

2) Symetric-Key Ratchet: The exchanged messages are encrypted using the keys that derived from the symetric-key ratchet. The input to this ratchet is a constant and only used to derive unique keys used to encrypt the messages.

If only this ratchet is used in the algorithm, any attacker could compute any future keys when they are able to steal one party sending and receving chain key. To prevent this, the Diffie-Hellman ratchet is used to add additional security.

3) Diffie-Hellman Ratchet: The DH Ratchet updates its keys based on Diffie-Hellman output. To implement it, each party generates a DH key pair, which becomes the ratchet key. Every messages contains the sender's current ratchet key, which in turn in used to derive the receiver's new ratchet key. This has the security effect that even when one party's ratchet key is compromised by an attacker, it will eventually replaced with a new one.

III. Security Analysis

The Signal Protocol is designed with a lot of security considerations. This protocol provides confidentialy, integrity, authentication, and future secrecy.

The Protocol also have been formally analysed by International Association for Cryptologic Research, and have been found to be sound and have no major flaws in the design.

IV. Closing

The Signal Protocol is an advanced messaging cryptography protocol which incorporates many of modern cryptography techniques that have been proven to work. The increasing amount of the protocol's adoption over the years also proves it's realibility. It also has official implementation library in C, Java, and Javascript languages which could cover many major devices system.

References

[1] K. Cohn-Gordon, C. Cremers, B. Dowling, L. Garratt, and D. Stebila, "A formal security analysis of the signal messaging protocol," Cryptology ePrint Archive, Report 2016/1013, 2016.

[2] "Signal technical documentation." [Online]. Available: https://signal.org/docs/

[3] K. Ermoshina, F. Musiani, and H. Halpin, "End-to-end encrypted messaging protocols: An overview," in *Internet Science*, F. Bagnoli, A. Satsiou, I. Stavrakakis, P. Nesi, G. Pacini, Y. Welp, T. Tiropanis, and D. DiFranzo, Eds. Cham: Springer International Publishing, 2016, pp. 244–254.