Whatsapp End-To-End Encryption

Aashi Jain, Aastha Gupta, Sonal Soni

College of Engineering and Technology, Mody University of Science and Technology, Lakshmangarh (Rajasthan), 332311, India.

jainaashi1998.ja@gmail.com, aasthag1811@gmail.com, soni7sonal@gmail.com

+91 9457197007, +91 8168377718, +91 7726802076

Abstract: WhatsApp is a platform widely used for online communication and for exchanging text as well as audio and video messages. It is of great importance that these messages be secure. To maintain the privacy of the users WhatsApp uses end-to-end encryption technique and uses various protocols and functions like the Curve25519 function and STA-256 algorithm. WhatsApp uses the Signal Protocol which was developed by the Open Whisper System. Using end-to-end encryption, any middle man or even WhatsApp server cannot retrieve the messages and thus the privacy and security of the users is maintained.

***Keywords**: Identity Key, Signed Pre Key, One Time Pre Key, Signal Protocol, Curve 25519 function, ECDH key agreement protocol*

*****

I. INTRODUCTION

WhatsApp is a widely used social media tool to interact with people; it is widely used to chat, message, voice call or video call with our near and dear ones. It is also used to share important and private data among people. It is of great importance to ensure that all this data is secure and is available only to the sender and the receiver and no one else can access this data. To ensure this, WhatsApp uses end-to-end encryption technique to ensure that nobody can hack the data and even WhatsApp itself cannot access the data.

II. END-TO-END ENCRYPTION

End-to-end encryption [1] means that the message or data sent by a person to another person can only be understood by the two of them. No third person can understand that data even if he gets access to the same. The message (be it audio, video or text) travels in an encrypted form and only the recipient is able to decrypt it. Even the Internet Service Provider cannot get access to the message. It is of importance to ensure the security and the privacy of the end users. If any communication app is encrypted, then it does not mean that the owner company cannot view the messages. The company itself has the key to decrypt the messages and therefore it does not completely keep the privacy of the users intact. End-to-end encryption on the other hand ensures that the users are completely secured and even the owner company cannot view the messages due to lack of the keys required. The role of the company servers is to simply forward the encrypted message to the receiver.

III. METHODS

WhatsApp uses the Signal Protocol [4] (earlier known as TextSecure Protocol) to implement end-to-end encryption. This protocol works on the concept of keys. Each user has his own private key that is made at time of installation of the app on the user's phone. The corresponding recipient has the user's public key through which he can decrypt the messages encrypted by the sender. Even the WhatsApp server does not have the private key of the user so it cannot peer in the conversation of the two users. Moreover, to enhance the security, each message is encrypted by its own key and cannot be hacked even if the hacker finds the key as it changes time to time and is different for each message.

The keys used in the encryption and decryption process are-

1. Identity Key- This is the user's private key generated at the time of app installment and it remains the same. This key is not available to any other user or even the WhatsApp server.
2. Signed Pre Key- This key is also generated at the install time and the identity key is used to sign this key.
3. One Time Pre Key- This key is generated for one time use and then it is deleted from the server's memory.

The above three keys are all public and are used to encrypt the message which can only be decrypted by the receiver who has the private key. As the private key is present only at the device of the user that is why no other device/user can decrypt the message and it is completely secure.

These keys are generated with the help of the Curve25519 function of the ECDH (Elliptic Curve Diffie Helman) key agreement protocol. The One Time Pre Key is deleted once a recipient sends a message to the user.

Now, for each message, a message_secret is generated. This

key is generated using the public keys and the private key of the user. It encrypts the message and the person who has the private key can only decrypt the message and understand it. If any one hacks the message in between, then without the key he cannot decode the message and it remains of no use to him.

Further the master_secret is used to generate the root key and then the chain key with the help of HKDF (HMAC-based Extract and Expand Key Derivation) Function. The root key and the chain key are 32-byte long. Now, the chain key is used to generate the message key which is 80-bytes in size which actually encrypts the message data. It can be used to encrypt data as well as audio or video. For every message there is a new message key along with the chain key and the root key. The message key is calculated using the SHA-256 algorithm. This algorithm takes the chain key as the input and returns the message key as the hash value in the output. A part of this generated message key is used is used to encrypt the message, one part is used to authenticate the message and one part is used for initialization. The chain key is also changed each time and id calculated using the same algorithm and the input is the previous chain key. The formulas for calculating the chain key and the message key are-

Message Key = HMAC-SHA256(Chain Key, 0x01) Chain Key = HMAC-SHA256(Chain Key, 0x02)

After a message has been delivered to the recipient and received by him, a new root key and chain key are generated using the Curve25519 algorithm mentioned above and the input for it is the existing root key. The formula for this is-

Chain Key, Root Key = HKDF(Root Key, ephemeral_secret) The ephermal_secret mentioned here is calculated as-

ephemeral_secret = ECDH(Ephemeralsender, Ephemeralrecipient)

The message keys are not reused and due to regular calculation of chain keys and message keys, sometimes the messages can be received by the recipient in random order and sometimes can also disappear.

In a WhatsApp group, each user has a Sender Key and each user has an encryption scheme corresponding to the Sender Key of all the other users. Therefore, the message sent by a user on a group can only be received by all the members of the group and no one else. If any member of the group leaves the group, then the Sender Key of that particular user is deleted by the group. The message sent by a user on a group of N members is sent N times by the server, i.e. one time for each user. The following steps are followed to generate a Sender Key-

When a new user is added to the group, a Chain Key and a Signature Key is generated with the help of Curve15519 function. Then, these two keys are combined to form the Sender key and this Sender key is distributed to all the members of the group.

IV. INITIATING SESSION SETUP

To establish the communication between two users, session is established when the users communicate for the first time. This session does not expire with time; it continues until some kind of disturbance like app reinstall occurs. The client who sends the message is called the Initiator and the client receiving the message is the recipient. The initiator requests for the Identity Key, Signed Pre Key and One Time Pre Key of the recipient from the server. Then, the initiator uses the Curve 25519 function to generate the key pair which is called as Einitiator. and then loads his own identity key. Using all these keys the master_secret is generated by applying the ECDH function to all these keys. After that, this master_secret is used to generate the root key and the chain keys with the help of HKDF function. As the One Time Pre Key is used only once, and each time a new key is used, so the master_secret generated each time is different.

V. EXCHANGING MESSAGES

The initiator sends the message to the recipient with the Einitiator and his Identity key in the header of the message when the communication occurs for the first time. When the recipient receives the message, to decrypt the message he generates his message_secret using the public keys sent by the initiator and his own private key. The recipient deletes the One Time Pre Key used by the initiator. The session has been established from both sides for communication.

The messages are secured by the Message Keys which are different for each message and they cannot be reconstructed after the message has been transmitted. So, a message cannot be decrypted by anyone else.

VI. TRANSMITTING MEDIA

In addition to text, all other media like audio, video, images and all other attachments are also encrypted. These attachments are encrypted using AES256 key in CBC mode with a random IV and then a MAC of the cipher text is appended using the HMAC SHA 256 algorithm. This encrypted attachment is attached to a blob store. This attachment is sent to the recipient along with the encryption key, the HMAC key, the hash calculated by the SHA 256 algorithm and the pointer to the blob in the blob store. To understand the message the receiver has to first decrypt the encryption with the encryption key sent by the sender, then he has to verify the hash and retrieve the blob from the blob store with the help of the pointer, verify the MAC and then finally retrieve the attachment by decrypting it.

VII. WHATSAPP CALL

Along with all the messages and attachments, WhatsApp voice call and video call are also encrypted. No third party

can listen to the talks or video chats between two users. To initiate a voice or video call, first of all there has to be a session. If the session does not already exist between the initiator and the recipient, then it has to be established by following the same procedure. Then, to call the recipient, the initiator has to generate a SRTP [5] master secret. This master secret is sent to the recipient along with an encrypted message which tells the recipient about the incoming call. If the recipient accepts the call, then the SRTP encrypted call ensues.

VIII. STATUS ENCRYPTION

In addition to the communication between two or more users, WhatsApp also encrypts the status and the profile picture of the clients. This is done in a similar manner as the group messages encryption. Once the status is updated by a client, then all the other clients who are authorized to view the status receive the keys and they can decrypt the status as well as the profile picture with the help of their respective private keys and the public keys of the client whose status has to be viewed.

VULNERABILITY

Suppose one user sends a message to other user who is currently offline. WhatsApp will temporarily store the message in the unencrypted form to send it to the receiver when he comes online. In the meantime, it is possible that some third person convinces the WhatsApp server that he is the receiver by either accessing the device or by hacking the GSM network [7] so that he can get the OTP (One Time Password) that WhatsApp would use to make sure that the message belongs to the receiver. Also, the government can persuade WhatsApp to get access to the messages of the clients and therefore behave as some other user to get access to his private messages and data.

IX. PROTOCOLS USED

Signal Protocol- This protocol was developed by the Open Whisper System. It is used to provide end-to-end encryption to text, audio or video messages. It uses the Curve 25519, AES-256 and HMAC-SHA256 algorithms.

ECDH Protocol- It is a key agreement protocol. It defines how keys should be generated and exchanged between end users or two or more parties. It takes the input as two keys and gives the output in the form of a secret key.

SRTP Protocol- Secure Real-Time Transport Protocol is mainly used for enhanced security features. It is widely used to secure the VOIP (Voice Over Internet Protocol) communications.

X. DISADVANTAGES

Along with all the advantages of end-to-end encryption, there are some disadvantages also. Due to end-to-end encryption, there is no watch on the data that is being circulated. It has become difficult to keep a watch on the activities of the anti-social people who misuse the social media to spread hatred messages.

XI. CONCLUSION

The main techniques that WhatsApp uses for end-to-end encryption are-

1. ECDH- This protocol is used to establish a shared secret by two parties over an unsecure channel
2. HKDF- It is the key derivation function. It derives Root key and Chain key from the master_secret.
3. HMAC-SHA256 (Hash-based Message Authentication Code) - It gives the output as a hash value from the input provided.
4. AES256 (Advanced Encryption Standard) - It is a symmetric encryption algorithm. It gives the result as a downloadable text file

REFERENCES

[1]. end-to-end encryption (E2EE) (2015) Retrieved February 7, 2018 from http://searchsecurity.techtarget.com/definition/end-to-end-encryption-E2EE

[2]. Calvin Li, Daniel Sanchez, Sean Hua (2016) WhatsApp Security Paper Analysis Retrieved from

ISSN: 2454-4248
39 – 42

https://courses.csail.mit.edu/6.857/2016/files/36.pdf

[3]. WhatsApp Encryption Explained (2016) Retrieved February 6, 2018 from https://www.pcrisk.com/internet-threat-news/10240-WhatsApp- encryption-explained

[4]. signal protocol Retrieved February 7, 2018 from https://www.npmjs.com/package/signal-protocol

[5]. SRTP (Secure Real-Time Transport Protocol or Secure RTP) (March 2011) Retrieved February 19, 2018 from http://whatis.techtarget.com/definition/SRTP-Secure-Real-Time-Transport-Protocol-or-Secure-RTP

[6]. WhatsApp Encryption Overview. Technical white paper._ https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf

[7]. Soham Sinha, Daniel Valentine, Robin Kurosawa and Kevin Leung (March 9, 2017) Retrieved February 19, 2018 WhatsApp Public Key Vulnerability fromhttps://asamborski.github.io/cs558_s17_blog/2017/03/09/whatsapp.html