e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:02/Issue:04/April - 2020 www.irjmets.com

CASE STUDY ON WHATSAPP END TO END ENCRYPTION

Miss. Rachna Agrawal[*1], Mr. Rishabh Rathore[*2], Mr. Shashank Jain[*3], Mr.SatyamYadav[*4], Mr. Vimaljeet Singh[*5], Mr. Yash Mishra[*6], Narendra Pal Singh[*7]

[*1,2,3,4,5,6]Students, Department of Information Technology, Acropolis Institute of Technology and Research, Indore, Madhya Pradesh, India.

[*7]Professor, Department of Information Technology, Acropolis Institute of Technology and Research, Indore, Madhya Pradesh, India.

ABSTRACT

In today's world, people around the globe use messaging services for healthy communication from anywhere to everywhere. For this, WhatsApp Messenger being an exclusive cross-platform instant messaging application that allows you to exchange text, files as well as audio and video messages. WhatsApp has 1.5 billion dynamic clients in 180 nations. However, being such a popular application; taking care of privacy breach is very important to keep going along the digital ride. It is important that the messages sent across the map should be secure. Thus, to give assurance and secrecy to client, for the most part cryptography is utilized as a spine of the web based exchanges [1]. WhatsApp utilizes end to end encryption technique and uses various protocols (Signal protocol etc.) and keys (public key, private key etc.) along with algorithm like Curve25519. This paper discusses on how WhatsApp uses algorithm and makes a secured channel between the sender and recipient.

KEYWORDS: Identity key, Signed prekey, One time prekey, Signal Protocol, ECDH Protocol, Cryptography, Curve-25519 Protocol.

I. INTRODUCTION

The world is ever changing because of the progression in the domain of science and innovation, and nowadays it appears to be difficult to get away from the nearness of innovation in our everyday lives. Since Smartphones got well known, many informing messaging services as well as applications have been propelled. Whatsapp being a very popular among these messaging services is a free mobile application owned and administrated by Facebook Inc. WhatsApp helps its clients to keep in contact with companions and family members. Aside from causing its clients to get and remain associated with one another, it additionally encourages them to make groups, send pictures, recordings, document, archives and audios. As an ever increasing number of individuals use WhatsApp as a methods for communication over mobile phones, the significance of making sure about its clients' privacy and security has become progressively basic. Clients of the application anticipate a sensible measure of privacy protection for each one of their correspondences.

To meet this desire, WhatsApp in 2014 presented End-to-End Encryption (E2EE). This takes into account information between conveying messages to be secure, free from listening stealthily, and hard to split. This technology offers significant serenity to end clients in light of the fact that their information are safe in travel, and outsiders or even WhatsApp itself can't get to them; in this way messages must be unscrambled by the beneficiary. While E2EE ensures uprightness, security, and protection, also, gives hand in increasing the capacity to guard the nation by blocking terrorist's messages interchange. WhatsApp Messenger permits individuals to trade messages (counting chats, group chats, pictures, recordings, videos, voice messages and documents) and make WhatsApp calls the world over. WhatsApp messages, voice and video calls between a sender and recipient that utilize WhatsApp customer programming discharged after March 31, 2016 are end - to end encoded.

Whatsapp also ensures that no privacy breach happens at any cost. To provide security and authentication, WhatsApp is acquainted with End-with End Encryption (E2EE) innovation. This takes into consideration; information between communication parties to be secure, free from listening in, difficult to split and offers dependability to the end clients in light of the fact that their information are safe during transmission, and outsiders or even WhatsApp itself can't get to them; The Encryption and Decryption of messages are done at both sides – From Sender to Recipient side. This way messages can be secured, encrypted first and decrypted by

the recipient. WhatsApp utilizes open source Signal Protocol, created by Open Whisper Framework. The purpose of end to end encryption is to code the sender's data in a such manner that only the recipient's gadget can interpret it, making it resistant from any outside or inside capture attempt.

II. METHODOLOGY

End to End Encryption (E2EE) implies that the message or information sent by an individual to someone else must be accessed by both of them. No third individual can comprehend that information or look upon the messages regardless of whether he gains access to the equivalent. The message (be it sound, video or content) goes in an encoded form (encrypted message) and just the recipient can unscramble it. Indeed, even the Whatsapp administrator or Internet Service Provider can't gain the content of the message. It is of significance to guarantee the security and the protection of the end clients. On the other hand, the other companies itself has the way to encrypt the messages and consequently it doesn't totally keep the security of the clients flawless. E2EE encryption then again guarantees that the clients are totally made sure about and even the Messaging Service Provider Application (in our case Whatsapp) can't see the messages because of absence of the keys required. The job of the Whatsapp servers is to just advance the encrypted message to the recipient.

Initially, normal server-based messaging frameworks do exclude E2EE encryption. These frameworks can just ensure the insurance of message interchanges among clients and servers, implying that clients host to confide in the third parties who are running the servers with the original messages. E2EE encryption is viewed as more secure in light of the fact that it decreases the quantity of parties who may have the option to meddle or break the encryption. For the situation of instant texting, clients may utilize an outsider customer to execute a E2EE encryption conspire over an in any case non-E2EE convention.

(a) Keys Transmission

Whatsapp application says they don't keep a duplicate of the private keys on their servers. Whatsapp produces the private key on your phone; however they store the public keys on their server. There is no hazard in that, as parting with your public keys is the means by which encryption has consistently worked. To comprehend what that implies, envision you are talking with somebody, state, Aisha. You send Aisha your public key when you begin to talk with her. She utilizes that key to encrypt messages that no one but you can peruse with your private key.

Since WhatsApp doesn't have your private key, they couldn't peruse those. Here are the WhatsApp keys. The Public ones distinguish what your identity is and the Session keys are utilized to encode a single chat session. These keys are :

1) Public Keys : The public key encrypts the message by sharing it with the recipient user.
2) Identity Key: The identity key is generated at application install, device specific and is never changed.
3) Signed Pre Key: The Signed Prekey is generated at install and changed periodically.
4) One Time Pre keys: One time use key pair, deleted afterwards and renewed if needed.

At whatever point client pursues WhatsApp, client gives their phone number to get a confirmation code by means of text or call. At this time (registration time), each WhatsApp client produces three public-private key sets, sent to the WhatsApp server: an identity key pair (I), a signed pre-key pair (S), and a set of one-time pre-keys({O}).

WhatsApp uses these keys and the Curve25519 encryption and SHA256 hashing algorithms to create keys and encrypt messages. When you chat with someone it saves that key exchange so that it does not have to repeat that key exchange when you chat with them again. When Reinstallation of WhatsApp is done and the chats are lost, as new keys are created and those, by definition, cannot read old messages.

(b) Initiating Session Setup

For the exchange of messages between sender and recipient, a session is established when they communicate for first time. This session expires only in the case of discrepancy or error, like app reinstallation. The user who sends the message is called the Initiator or the Sender and the one receiving the message is the recipient.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:02/Issue:04/April - 2020 www.irjmets.com

Several steps for session setup are as follows:

1) Sender demands Identity Key, Signed and One Time prekey from recipient.
2) WhatsApp Server returns the mentioned values.
3) Sender saves these values as I r, S r , O r
4) Sender produces ephemeral Curve25519 key pair E
5) Sender loads its own Identity Key as i
6) Sender calculates
7) master_secret = ECDH(I i , S r) | | ECDH(E i , I r) | | ECDH(E i , S r) | | ECDH(E i , O r)
8) Sender utilizes HKDF to create root Key and chain Key from master secret.

Sender will send an encoded message to Recipient with E s and I_s attached in the header. Recipient uses these public keys, along with his own private keys, to produce the similar master secret and from that point cryptographic keys, and will erase the one-time pre-key, sender uses to begin the session.

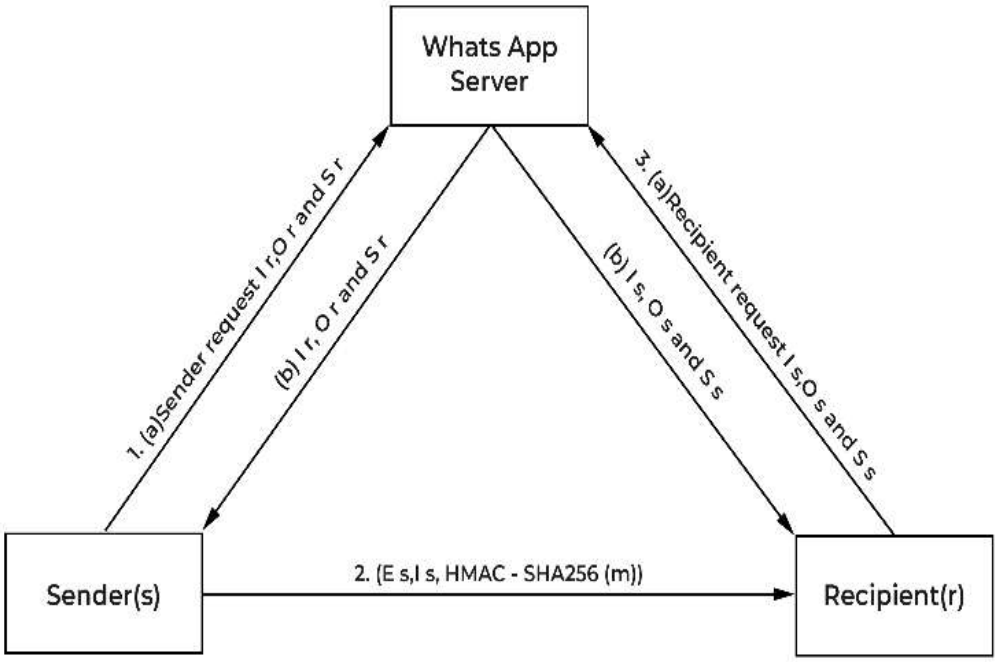

Fig-1: Key Exchange between Sender and Recipient

Figure 1 depicts the key exchange. Sender requests recipient's public keys (1a) and gets them (1b). Sender sends a message to recipient with headers for recipient to set up a session(2). Recipient requests sender's public keys (3a) and gets them (3b) and figures the master secret, building up the cryptographic session.

(c) Receiving Session

After the underlying session setup process, until the recipient reacts, all data important to assemble a session is sent within the header of all messages from the initiator i.e. Sender (E i , I i). Once a session has been established, clients exchange messages that are protected with a Message Key using AES256 in CBC mode for encryption and HMAC-SHA256 for authentication. Large attachments – video, audio, images, or files – are also encrypted.

Further strides to create a corresponding session are as follows:

1. Recipient computes the relating master key by utilizing its own keys.
2. The recipient erases the One Time Prekey utilized by the sender to start.
3. Sender uses HKDF (HKDF is a key derivation function (KDF) in view of a hash-based message confirmation code (HMAC)) to infer a relating root Key and chain Keys from master secret.

(d) Exchanging Messages

This process relies heavily on the X3DH key agreement and is what gives Signal Protocol the ability to provide forward secrecy and cryptographic deniability. This also has an additional benefit of asynchronicity and thus the ability of sending messages while being offline. As we have seen above, once the session setup is complete, sender and receiver have a common master secret, from which they both derive three keys, which are explained below:

1. a root key: (usually called root certificate) used to generate the next key, the chain key [2].
2. a chain key: It is used to generate the message key which actually encrypts the message data.
3. a message key: This Key changes for each message transmitted and is ephemeral.

These keys protect the process of exchanging messages.

Ratchet is the name of a gadget that moves only one way. Double Ratchet utilizes two cryptographic Ratchets, i.e., Diffie-Hellman ratchet and Hashing ratchet. This is used to getting new keys from current keys and moving ahead, while forgetting old keys.

WhatsApp's framework includes another made sure about degree of encryption, known as "perfect forward secrecy". This resembles a second lock with a key that changes for each messaging session. At the point when Sender wishes to send a message to receiver, sender initially creates a fresh session key, places it in the box and uses recipient's public key to lock it. Sender at that point sends it to recipient, who utilizes his private key to get to the session key. Both of them would then be able to begin communication safely utilizing that session key known uniquely to them to encrypt their messages.

III. PROTOCOLS USED

Signal Protocol: Signal protocol is a cryptographic protocol use to provide encryption for text, audio, video calls and different group messaging conversation. It is designed by Open Whisper Systems, and is the basis of Whatsapp End – to – End Encryption. This is a basic protocol which is used to provide end to end encryption. Signal Protocol's goals include end-to-end encryption as well as advanced security properties such as perfect forward secrecy and "future secrecy". The Signal cryptographic protocol has seen high take-up of encryption in close to personal communication through messaging services.

The basic algorithms used in signal protocol are :

(a) Curve-25519:

Curve25519 is a cryptographic algorithm which offer 128 bit encryption and mainly use for ECDH key arrangement. Its security depends on trouble of discrete logarithm issue in large finite groups. Curve25519 was explicitly structured with the goal that secure, quick usage is simpler to create. Specifically, no validation of public keys is required and point multiplication can be proficiently processed utilizing a constant number of tasks which avoids a number of side-channel attacks.

Curve25519(elliptic curve) implemented with Diffie hellman key arrangement which allow sender and receiver to agree on sharing a secret key over a public channel. It is based on modular arithmetic. This algorithm generally uses prime modular arithmetic which provide equal distribution of keys over a given group. This algorithm takes a prime modular e and a generator q which is use for generating keys where generator always lie between 0 to e-

This can be viewed as :

1. Sender choose a random number x between 1 and e-1, her private key.

2. Receiver selects a random number y between 1 and e-1, his private key.
3. Sender sends Receiver, x_e = g^x mod e, her public key.
4. R sends Sender y_e = g^y mod e, his public key.
5. Sender calculates ss_a = y_p^x mod p.
6. Receiver calculates ss_b = x_p^y mod p.

After accomplishment of protocol, Sender and Receiver have a shared secret ss_a = ss_b = g^(xy) mod p.

(b) ECDH Protocol:

Elliptic curve Diffie-Hellman is a key managing protocol allows different parties having elliptic key pair to share a secret key over a non-reliable medium. This shared secret may directly use as a key by receiver or can be used to derive another key. It characterizes how keys ought to be produced and exchanged between at least two parties. It accepts input as two keys and give yield in structure secret key.

Elliptic curves are used to generate points on curve. If we take a sender and receiver then sender will generate a public key(QB) and private key (db) receiver will generate it's public and private key pair(QA, da) after the generation of key pairs they exchange their public keys and generate share key equivalent to da*db*G where G is generator point on curve.

Sender will produce a public key and a private key by taking a point on the curve. The private key is a random number (dB) and the Sender's public key (QB) will be generated by Handshaking of keys, that is depicted below:

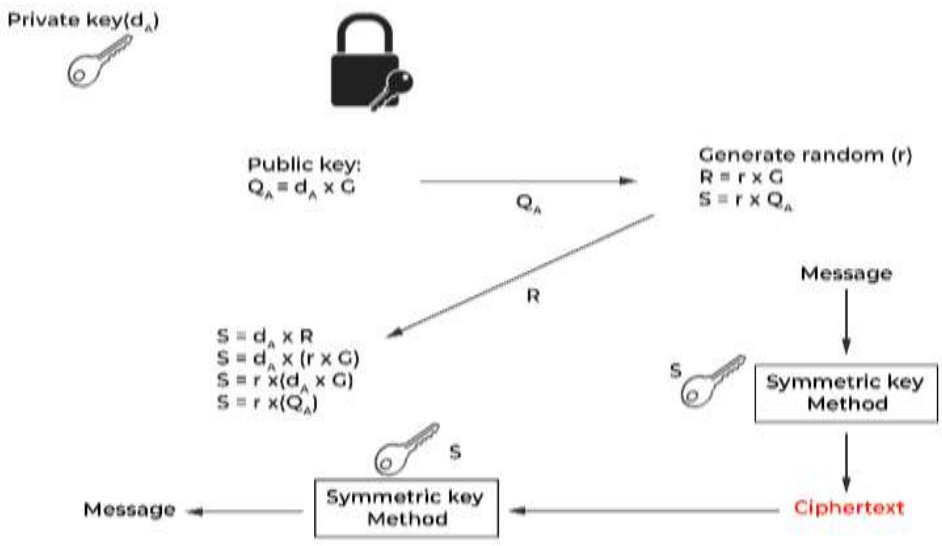

Fig-2: Handshaking of keys with ECDH Protocol

1. QB = dB×G
2. Receiver will do likewise and produce her public key (QA) from her private key (d A): QA= dA×G
3. They at that point exchange their public keys. Receiver will at that point utilize Sender's public key and her private key to determine:

   Share key Receiver = dA×QB = dA×QB

   This will be the same as:

   Share key Receiver= dA×dB×G = dA×dB×G
4. Sender will at that point utilize Receiver's public key and his private key to determine:

   Share key Sender = dB1×QA= dB×QA

This will be the same as :

Share key Sender= dB×dA×G = dB×dA×G

5. The final share key generated will be same for both sender and receiver.

IV. CONCLUSION

The need of texting and messaging services on cell phones and their utilization of end to end encryption in shielding the privacy of their clients have become a worry for certain legislatures. WhatsApp has risen as the most famous messaging application in market today. It puts forth government and secret authorities attempts to battle sorted out crimes, criminals, and pornographers in fact incomprehensible.

Privacy protection is a key component of human rights in this digital and social era, and improvements influencing it should be accounted for. While a major share of nations' population would support a limitation on access to unrecoverable encryption, there is no worldwide agreement, and the probable result is a mess of national strategies. In recent times, several companies data were hacked or compromised due to not using proper encryption technique. This paper provides a proper understanding and lists the role of encryption in WhatsApp messaging service.

Whatsapp exhibits that messages send by sender is decrypted only at the recipient's side, neither could it be read by WhatsApp nor any intruder can intercept the message as these messages are secured by end to end encryption. The enormous factor in giving this security layer originates from WhatsApp's tremendous utilization of ephemeral and dynamic keys.

V. REFERENCES

[1] K. Berlin, S.S. Dhenakaran "Adoption of Crypto Encryption Techniques in Different Scenario " in International Journal of Advance Research in Computer Science and Management Studies, Volume 5, Issue 8, August 2017.

https://www.researchgate.net/publication/327982333_Adoption_of_Crypto_Encryption_Techniques_in_Different_Scenario/link/5bb2026ca6fdccd3cb80b486/download

[2] pcrisk.com "Whatsapp Encryption Explained".

https://www.pcrisk.com/internet-threat-news/10240-whatsapp-encryption-explained

[3] Amit Panghal "WhatsApp's End to End Encryption" .

https://medium.com/@panghalamit/whatsapp-s-end-to-end-encryption-how-does-it-work-80020977caa0

[4] Vamsi Krapa, S.Prayla Shyry, M.Rahul Sai Krishna "WhatsApp Encryption- A Research " International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8, Issue-2S3, July 2019.

https://www.ijrte.org/wpcontent/uploads/papers/v8i2S3/B10930782S319.pdf

[5] "WhatsApp Encryption Overview: Technical White Paper",WhatsApp.

https://www.whatsapp.com/security/WhatsAppSecurityWhitepaper.pdf

[6] Aashi Jain, Aastha Gupta, Sonal Soni," Whatsapp End-To-End Encryption" 3rd International Conference on Computing: Communication, Networks and Security (IC3NS-2018) ISSN: 2454-4248 Volume:4 Issue:3.

http://www.ijfrcsce.org/download/conferences/IC3NS_2018/IC3NS_Track/1522230027_28-03-_2018.pdf

[7] Whittaker, Z. (2017) US Says It Doesn't Need Secret Court's Approval to Ask for Encryption Backdoors.

https://www.zdnet.com/article/us-says-it-does-not-need-courts-to-approve-encryption-backdoors/