WhatsApp Encryption- A Research

Vamsi Krapa, S.Prayla Shyry, M.Rahul Sai Krishna

ABSTRACT--- In the recent years, battle between national security and a person's privacy has become prime conflict. Governments and secret services are asking encrypted messaging services such as WhatsApp to allow them access to user's data. After the March attack at Westminster(2017), UK home secretary, stated that accessibility of WhatsApp's data is mandatory to authorize the legitimate user since the government couldn't smell the encrypted messages of suspected terrorists. But in turn such access to messages will allow authorities to thwart future terror attacks. In this paper, novel enhanced End to end encryption technique is proposed to identify the breaches and mitigate the terror attacks. Also different encryption techniques are compared with respect to their performance and the best encryption technique is revealed.

Keywords — End to end encryption technique, Breaches.

I. INTRODUCTION

WhatsApp Messenger allows people to exchange messages (including chats, group chats, images, videos, voice messages and files) and make WhatsApp calls around the world. WhatsApp messages, voice and video calls between a sender and receiver that use WhatsApp client software released after March 31, 2016 are end-to-end encrypted[5].

The Signal Protocol, designed by Open Whisper Systems, is the basis for WhatsApp's end-to-end encryption. This end-to-end encryption protocol is designed to prevent third parties and WhatsApp from having plaintext access to messages or calls. What's more, even if encryption keys from a user's device are ever physically compromised, they cannot be used to go back in time to decrypt previously transmitted messages[6].

II. RELATED WORK

Nidhi et al.(2019) stated that whatsapp is most popular mobile application found on every smartphone. They analyze the whatsapp messaging platform and critique it security arch and also privacy preservation techniques they reported that end to end encryption does offer protection against forward secrecy. Their final argument is that the end to end encryption channel can't preserve privacy because of the meta data . They said that it is able to reveal information to show connections between people and their personal information.

They have also elaborated security architecture of WhatsApp and performed analysis on various protocols used.They have also stated that whatsapp encryption is vulnerable and had gone through many attacks for example in 2011 problems found in a verification and proved that the authentication mechanism was unsecure. WhatsApp failed in session hacking which allowed unauthorised access where an attacker can get sender information. They also explain about security architecture by explaining how key management works. They concluded that this app has attracted many users because of high usage of end to end encryption.

Robert E.Endely (2018) stated that the instant message services on mobile devices which are end to end encrypted and safeguarding the users privacy have become a worry for government as it uses end to end encryption which trouble government to find organised crime, terrorist attacks, and child pornographers and almost technically impossible. He have also said that the government has requested for a backdoor which will only be used for national security purpose but the end users defended that by explaining the hackers may take it as an advantage and break the privacy of the user.

He stated that interest and need towards request for security and privacy of their messages has also increased. WhatsApp solve their issue by introducing end-to-end encryption in 2016, which is impossible for hacking so there will be no third party to read messages and even the WhatsApp couldn't access a message except the receiver. Government surveillance is also eliminated. He found that the WhatsApp didn't agree for giving a backdoor to the government which would create an opportunity for the hackers to get into the use information. In 2004 Skype give access to government as a backdoor which led the users of Skype protest against it and had stopped using Skype.

Sonal soni et al. (2018) stated that WhatsApp user's apply end to end encryption technique various protocol and functions like curve 25519 function and STA 256 algorithm. They stated even the internet provider will have no access of the messages and the difference between encryption and end to end encryption. If any communication app is encrypted then it doesn't mean the messages are totally private those apps will have their own key to decrypt the messages whereas end to end encryption communication app the messages are totally secured even the app server will have no access to decrypt the message and the only work the app server need to do is transfer the encrypted message from sender to receiver.

They said it uses signal protocol and to implement end to end encryption. This works on concept of keys and also explains about the keys named as identity key, signed pre key onetime pre key. They also explained about the session key which acts as a bridge at the first time of communication and does not expire till the app gets re-installed or the device is changed. They also explained how

Revised Manuscript Received on July 10, 2019.

Vamsi Krapa, Third Year CSE, Sathyabama, Chennai, T.N, India. (E-mail: vamsi.krapa@gmail.com)

Dr S.Prayla Shyry, Assoc.Prof,dept of CSE, Sathyabama, Chennai, T.N, India. (E-mail: suja200165@gmail.com)

M.Rahul Sai Krishna, Third Year CSE, Sathyabama, Chennai, T.N, India. (E-mail: mithintirahul8006@gmail.com)

the message get exchanged using their identity key and onetime pre key. They mentioned in their paper that the protocols used are Signal protocol, ECDLT protocol, SRTP protocol.

Soham Sinha et al. (2017) stated that Tobias Boelter In April 2016 discovered a flaw in WhatsApp implementation, Facebook defended the implementation as a design choice. They stated that "The Company can read end to end messages" and this vulnerability cracks huge threat to freedom to speech. They mentioned three methods of vulnerabilities.1.The users will have both public and private key if the public key is shared the connection was established and the private key stays with themselves in this process the hacking can never be done. the vulnerability occurs during the generation of new public key which takes place when the app is reinstalled or WhatsApp using device is changed. 2. They said as the texts sent gets encrypted only by the time it move out of the device so if the sender send message when the receiver is offline then message stays in the senders device unencrypted so the hacker can hack the device and get the message this leads to the Vulnerability.

If The hacker hacks the GSM network the OTP can be generated and the WhatsApp can be recreated on the name of sender so that at that stage all the unsend messages sent by the sender can be accessed by the hacker this is also a vulnerability. 3. if the hacker can buy a SS7 hub which is illegal in most of the countries but if the attacker can manage to get that and register in it and get the number of any person (user) which is usually open for all. Through that he can contact the GSM network operator so they can easily get all the details of the user like IMSI and USIM number so can recreate the whatsapp and get all the mesasages of the user which leads to vulnerability.

III. PROPOSED METHODOLOGY & RESULTS

Existing Methodologies use end to end encryption and the security in the encryption is remarkable. But still, in general the security in the communication channel can be compromised and in turn the server user database is compromised. To overcome such situations, a novel single secret key can be generated from both the sender and the reciever side. The keys from both the sides are not communicated through the channel. But the integrity of the key is validated in periodical intervals. Also existing RSA and DES can be compared and the best method is revealed.

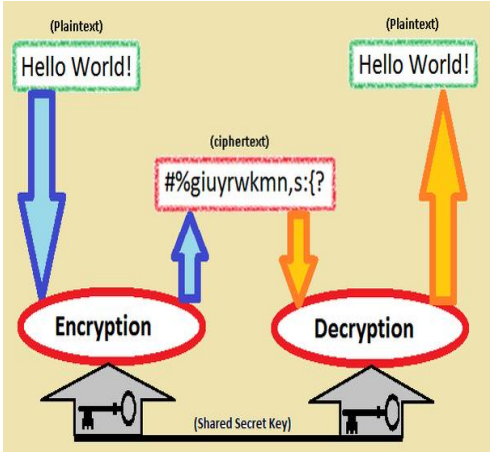

Fig 1: Shared Secret key Encryption

IV. CONCLUSION

Recipients can only decrypt the mesaage and it could never be read by watsapp. Also it is secured by an authentic end to-end protocol. the messages can only be decrypted by the recipient. Enitre Whatsapp contents are secured and intruder cannot intercept the messages and crack any confidential information calls are protected by end-to-end encryption. The private key of watsapp users cannot be accessed by WhatsApp servers. The integrity of the communication is ensured by verifying the keys of whatsapp users.

REFERENCES

1. https://www.researchgate.net/publication/312778290_WhatsApp_security_and_role_of_meta data_in_preserving_privacy
2. https://file.scirp.org/pdf/JIS_2018012214154978.pdf
3. http://www.ijfrcsce.org/download/conferences/IC3NS_2018/IC3NS_Track/1522230027_28- 03-2018.pdf
4. https://asamborski.github.io/cs558_s17_blog/2017/03/09/whatsapp.html
5. Rama Krishna, V., Subhashini, R., Botnet algorithms adaptability for mimicking attacks and inducing mimicking attack, Journal of Advanced Research in Dynamical and Control Systems, 2018.
6. Y. Bevish Jinila , K. Komathy (2013)," A privacy preserving authentication framework for safety messages in vanet", 4th International Conference on Sustainable Energy and Intelligent System (SEISCON 2013), December 12-14, 2013, pp. 456-461, IET