WhatsApp Securum –Gratifying or Malus

Prof. Mayuri Dendge[1] **Prof.Sandip Gadilkar**[2]
[1] Bharti Vidyapeeth' Institute of Management and Information Technology, Navi Mumbai
[2] Indian Maritime University,Mumbai Port Campus

Abstract -
WhatsApp recently enabled End-to-End security with 256-bit encryption. Using this encryption method a single word can take hours and days to decrypt; envision for trying to decode a sentence or entire message. But though the messaging platforms are highly secure, they can still be bypassed by a hacker to intercept your messages.
Neither the flaw exists in the messaging app nor its services but may it do exist in telecom operator's technology. Signaling System 7, or SS7, is the main culprit and it is the technology used by telecom operators, on which the highly secure messaging system and telephone calls rely.

Keywords -
Vulnerability,End-to-Endsecurity,eavesdropping,Vulnerability,DRA,
Spoofing,IME,MAC,Encryption,Decryption,DiffieHellman

I. INTRODUCTION

World's most popular messaging app WhatsApp recently added many features and updates for its robustness.WhatsApp messages, picture and images can be easily read and manipulated; WhatsApp has a built-in secure method to store all messages and conversations in encrypted files. One simply cannot read the messages or edit them with regular software and applications. WhatsApp stores all the data in multiple files named msgstore.db, msgstore.db.crypt8 respectively. Previously, it was storing it in an older format (msgstore.db.crypt7), which was easily decrypted by various backup apps and third-party apps, which allow a user to read the messages in it. Now that WhatsApp uses the new encryption for higher security, it seems that hackers and developers are one step ahead of the tech giant and have managed to get a breakthrough.

A third-party application is available online (exempted Google Play), which can easily open the encrypted database and edit the contents inside it. The app free to download, is available on third-party app stores and pirated servers, is very simple to use and anyone can download and use it. The only requirement for the app to work is a rooted Android smart phone.

II. LITERATURE SURVEY

As far as encrypted services and the work of law enforcement concern the founder quoted - "While we recognize the important work of law enforcement in keeping people safe, efforts to weaken encryption risk exposing people's information to abuse from cybercriminals, hackers, and rogue states. Basically, performing a MITM attack seems not possible in WhatsApp end-2-end encryption.

However, there still have ways to breaking into as placing malware like RAT or logger in phone or computer directly. If one wants to use only the phone number, one can use vulnerability to spoof the WhatsApp system as the owner of the account, which can't be fixed and require more technique.

There are many methods one can use to hack WhatsApp which can't be listed out because every hacker (expect script-kiddie) have a "Super Smart Brain" that can think out of the box. It would be difficult to hack, but not impossible. if man can make something, man can also break it. Most likely one is not hacked remotely. It was done at terminal.

III. ALGORITHM

The Research on is on WhatsApp partnered with Open Whisper Systems for the cryptographic portions of messaging. The process involves a variation of Off the Record (OTR), Perfect Forward Secrecy (PFS), and the Double Ratchet Algorithm (DRA). Open Whisper Systems has blog posts on cryptographic ratcheting, and their Signal Protocol Integration for WhatsApp. WhatsApp used text secure algorithm to provide an end to end encryption to the user. In text, secure algorithm a random key is generated for each pair of communications. So, text secure is a mix of both advanced cryptographic protocol.

DoubleRatchet Algorithm

The Double Ratchet Algorithm obtain its name from its "ratcheting" mechanism on the Chain key to get new Chain Keys, occurring when a user sends a message and when a user receives a message afterwards. To offer end-to-end encryption for instant messaging Double Ratchet Algorithm can be used.

*Step1.*When a user sends a message, it hashes the Chain Key to get the next Chain Key. Afterwards, when the user receives a message, it will also receive an ephemeralCurve25519 key used for "ratcheting" the Chain Key and Root Key forward.

*Step2.*The first ratchet phase is referred to as the Hash Ratchet, since the Chain Keys hashed withHMACSHA256 to get the new Chain Key.

*Step3.*In this phase, the Chain Key is used to derive the onetime use Message Key by the following:

3.1 Message Key = HMACSHA256(Chain Key, 0x01)

Subsequently, the Chain Key is ratcheted forward

3.2 Chain Key = HMACSHA256(Chain Key, 0x02)

Step4. The second phase, referred to as the DH Ratchet (Diffie Hellman), occurs when a user receives the message. In addition to receiving the encrypted message, it also sends a public ephemeral.

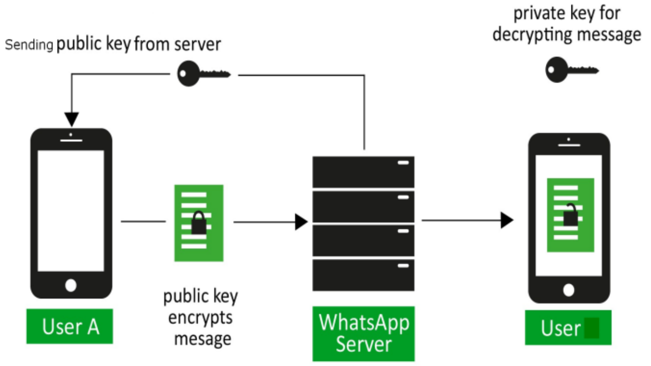
Sending public key from server
private key for decrypting message
User A
public key encrypts mesage
WhatsApp Server
User

Fig1.1. ***DoubleRatchet Algorithm working mechanism***

IV. RESULTS AND FINDINGS

The Research demonstrates that there are several techniques through which one can be victim. They are as following.

1. A using device X. Mobile Number as M.

1.1. B using device Y. X has WhatsApp installed for M.
1.2. B installs WhatsApp in device Y, tries to activate it using the M.
1.3. B is somehow able to get access to verification code for A's mobile number M.
1.4. B starts using WhatsApp on Y using A's number (M), which was already working on X. Then the moment for mobile number M, WhatsApp starts working on Y, it will stop working on X (showing a message one can't associate a single mobile number to multiple accounts)and that's how one will get to know, if someone else in this world got a hold on your WhatsApp account.

2.Get another WhatsApp and send a text to a phone number which one wants to be checked. Don't read the message. Keep it unread in phone. Wait for few hours or a day and watch if the message sent to that number read or not by checking the double tick blue color ticks followed by the message. If yes, then surely someone has got access to WhatsApp account in any way if it's not then account seems to be secure.

V. PROVIDENCE AND WARINESS

The Research depicts, if one is suspicious about WhatsApp conversations or account then trance the Double Ratchet Algorithm and go through all the installed apps running on the cell. If found some apps unknowingly installed, uninstall it and never lend the mobile to someone. The hacker tends to install a spy app on the mobile phone without one even noticing. Check out and uninstall it.

VI. FUTURE SCOPE

The Research demonstrates the Double Ratchet Algorithm is designed to provide security against an attacker who records encrypted messages and then compromises a sender or receiver later. This Security could be defeated if deleted plaintext or keys could be recovered by an attacker with low level access to the compromised device. Recovering deleted data from storage media is a complicated topic which is outside the scope of the research. In the age of open source software, encryption tools are freely available. Most importantly, WhatsApp should invest more in technology and building simple features that helps to protect the privacy and security of messages and calls through WhatsApp. The Double Ratchet Algorithm (DRA), Open Whisper Systems has blog posts on cryptographic ratcheting, and their Signal Protocol Integration for WhatsApp. WhatsAppused text secure algorithm to provide an end to end encryption to the user. In text secure algorithm a arbitrary key is generated for each pair of communications. So text secure is a mix of both advanced cryptographic protocol.

VII. CONCLUSION

The Research demonstrates the algorithm's sanctuary could be defeated in case of deletion the plaintext or keys from attacker side and when the accessibility of device is not much secured (Low level secured) that would be compromise with device access. End-to-end encryption is useless unless the device itself is secure and that is exactly what hackers and cyber-criminals will target. Pointing out that the encryption feature does not matter if the end devices—phones, tablets, and computers—are not encrypted. "Even perfectly encrypted platform's communications are as secure as the user's devices, and with the rise of new malware every single day, nobody is safe". A KDF chain is a nucleus notion in Double Ratchet Algorithm, it accept a secret and random KDF key and some input data and returns output data. If the key is already known and random, the KDF should still offer a secure cryptographic hash of its key and input data.

References

[1] Stott, Nick. "WhatsApp has grown to 1 billion users". The Verge. http://www.theverge.com/2016/2/1/10889534/whatsapp1billionusersfacebookmarkzuckerberg

[2] Koum, Jan. "end to end encryption" WhatsApp Blog. https://blog.whatsapp.com/10000618/endtoendencryption

[3] "WhatsApp Encryption Overview: Technical White Paper". WhatsApp. https://www.whatsapp.com/security/WhatsAppSecurityWhitepaper.pdf

[4] Anderson, T. & Garrison, D. R. (1998). Learning in a networked world: New roles and responsibilities.

[5] Gibson, C. (Ed.), Distance Learners in Higher Education.

[6] Boyd, D.M. & Ellison, N.B. (2008). "Social Network Sites: Definition, History, and Scholarship,"

[7] Stake R. E. (1995) The Art of Case Study Research. Sage, Thousand Oaks, CA.WhatsApp.(2010,November). Retrieved April 11, 2012, from BlackBerry App World: WhatsApp. (2010).

[8] BlackBerry App World http://appworld.blackberry.com/webstore/content/2360