



# WHATSAPP HACKABILITY

MANJUSHREE C.V<sup>#1</sup>, S M Y ALTAMASH<sup>\*2</sup>

<sup>1</sup>Assistant professor & Research Scholar, <sup>2</sup>UG Student

<sup>12</sup>Department of Computer Science and Engineering

<sup>12</sup>Vemana Institute of Technology, Bangalore, India.

**Abstract:** With the increase in usability of whatsapp by more than 1.2 billion users world-wide[8], there is a great issue on its security and hence it provided end to end encryption[1] through which the texts, status updates, calls, images, documents etc. Which are sent to the users are secured, third parties and not even whatsapp can know the messages which are sent this is achieved by the 256 bit encryption technique which encrypts the messages using signalling protocol[9], the main drawback of whatsapp is it uses a text message or a voice call to get registered for whatsapp service. The calls and text messages for registration can be redirected to a second number and thus the whatsapp can be hacked using the SS7 protocol vulnerability [3][4][5][7].

**Keywords:** End to end encryption, signalling protocol, SS7 protocol.

## I. INTRODUCTION

Whatsapp a cross platform messaging app by which a user of one platform can send messages to other platform devices, the messages sent by whatsapp mainly use XMPP protocol[2], exchanging messages with privacy is the major concern so as to ensure its security it came up with an end to end encryption feature which use signalling protocol[9]. End to end encryption [1] was developed by the open whisper systems they mainly use 256 bit encryption technique to provide security, by encrypting the messages sent from one device to another. Using this feature the messages sent between the devices are having a lock and key[1] which is specific for a connection and whatsapp provides the feature to cross verify its security feature by scanning the QR code. Even if encryption keys from a user's device are ever physically guessed right, they cannot be used to go back in time to decrypt previously sent messages. But due to the flaw of SS7[3][4][5][7] the account can be hacked completely by redirecting the messages and calls of the registered phone number to the hacker's phone number and the hacker can access the account by entering the received OTP. The hacker can't retrieve the previous messages which are sent prior to the registration of whatsapp on his device. Eavesdropping can be done by using an app named whatscan which is available for android, iOS.

## II. LITERATURE SURVEY

- **WhatsApp Encryption Overview Technical Whitepaper:**-This paper gives an overall technical details of the security features implemented in the design of the whatsapp end to end encryption with signal protocol and lock and key feature which is unique for particular user and the lock and key keeps changing after a certain time. It describes the usage of public key, session key, root key, message key in the transmission and receiving of encrypted messages. The messages sent are secured by access of any third party and even whatsapp.
- **An Overview On The Architecture Of Whatsapp:** -This paper gives the details of how the XMPP (eXtensible Messaging Presence Protocol) is used by whatsapp to communicate with different platform applications. Which makes it much faster and reliable application.
- **Hacking mobile network via SS7: interception, shadowing and more:** -This paper gives the details of using SS7 protocol and its usage of hacking the text messages, phone calls and eavesdropping on the victims Phone. Hacking is possible as the 2G/3G Networks use SS7 protocol to communicate with other telecom operators, even though it is hackable most of the telecom operators use this technology.
- **User Location Tracking Attacks for LTE Networks Using the Interworking Functionality:**-This paper gives the detailed information of how the 2G/3G Networks use SS7 protocol and its hackability and overcoming of hacking by using LTE ( Long Term Evolution ) via Diameter protocol. Diameter uses IPsec/TLS and certificate based authentication. It also gives the overview of how the signal form SS7 interact with Diameter Protocol.

### III. HACKING CAN BE DONE AS FOLLOWS

- HACKING USING SS7 PROTOCOL.
- HACKING USING WHATSCAN APP.

### IV. HACKING USING SS7 PROTOCOL

Even though whatsapp is fully secured with lock and key or End to end encryption[1] but for registering to whatsapp it follows a traditional method, it sends an OTP to verify the user's identity to the phone number on which the whatsapp is being used on failure of receiving OTP, it sends a voice call to the number and upon valid OTP entry it creates a whatsapp account, the hacker redirects the calls and messages and gains access over the whatsapp account by entering the right security key as in the (fig 1.1). This type of hack can be done without having to access the hacked device manually by using the SS7 protocol [3][4][5][7], which is been used by many of the telecom operators. by using SS7 protocol the hacker can trace the calls, texts, location[4].

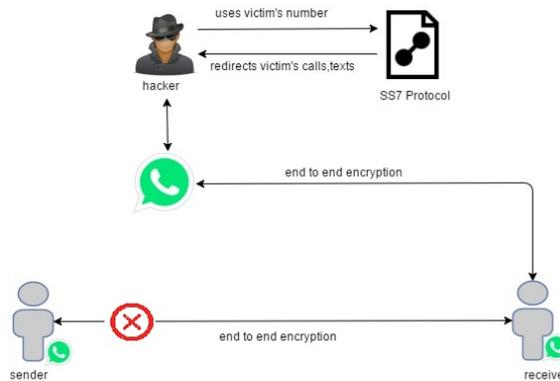


fig 1.1

Fig1.1 Hacking WhatsApp using SS7 Protocol

By using this hardware vulnerability the hacker can gain full access over the account and can text, call and perform various other operations available in whatsapp by using the identity of the hacked user.

### V. HACKING USING WHATSCAN APP

This type of hacking is possible only when the whatsapp code (QR code)[10][11] is scanned by the victim's phone and this requires the use of the victim's device for scanning the code, this type of hacking is mainly done by our friends or family members for eavesdropping on the conversations we are having, the process is explained as in the (fig 1.2). By using this app the hacker can hack or hijack our account and can text others by using the identity of original user.

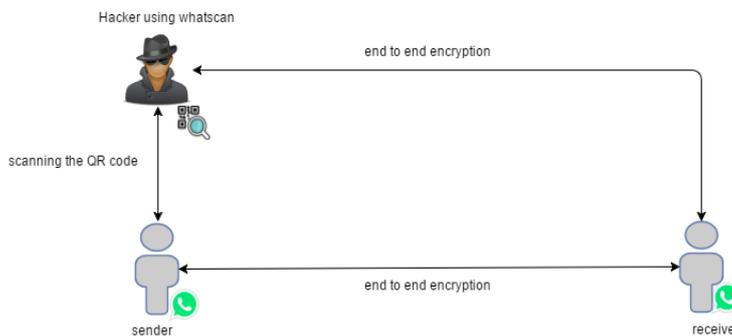


fig 1.2

Fig 1.2 Hacking WhatsApp using whatscan App.

The drawback of using this app for hacking is that the hacker can't access the whatsapp when the original user is offline, only the texts, videos, images can be read by the hacker and not the audio. If the original user gets the doubt of getting eavesdropped by someone on the chats he is having, he may manually check and log out by this the hacker can't access the account and needs to scan the code again to gain access.

## VI. CONCLUSION

Even though whatsapp provides greater security features such as end to end encryption compared with other messaging apps, it can be hacked using the hardware vulnerability of SS7 protocol[3][4][5][7] or by using whatscan app[10][11]. We can monitor the device status if it is hacked or not by using an app SnoopSnitch[6].

## REFERENCES

- [1]. (2016 Nov), “Whatsapp Encryption Overview Technical white paper”.
- [2]. Umesh Gupta “An Overview On The Architecture Of Whatsapp”, International Journal of Computer Science & Engineering Technology (IJCSSET).
- [3]. Dmitry Kurbatov, “Hacking mobile network via SS7: interception, shadowing and more”, Security specialist Positive Research.
- [4]. Siddharth Prakash Rao, Silke Holtmanns, Ian Oliver, “User location tracking Attacks for Long Term Evolution networks using the interworking functionality”.
- [5]. Bob Kamwendo, “Vulnerabilities of SS7 attacks and how to mitigate against these vulnerabilities”.
- [6]. Karsten Nohl, “Mobile self defense”, Security Research Labs.
- [7]. Signalling system 7 (ss7) security report.” [Online]. Available: <http://tinyurl.com/SS7-Security-report>.
- [8]. Whatsapp Wikipedia” [Online]. Available: <https://en.wikipedia.org/wiki/WhatsApp>
- [9]. Signal Protocol Wikipedia” [Online]. Available: [https://en.wikipedia.org/wiki/Signal\\_Protocol](https://en.wikipedia.org/wiki/Signal_Protocol)
- [10]. Whatscan for Whatsapp – Android Apps n Google Play”[Online]. Available: <https://play.google.com/store/apps/details?id=com.whatscan&hl=en>
- [11]. Whatscan for Whatsapp Web on the App Store – iTunes - Apple” [Online]. Available: <https://itunes.apple.com/in/app/whatscan-for-whatsapp-web/id1147804589?mt=8>