iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 2 **Issue:** IX **Month of publication:** September 2014

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

Whatsapp : The messenger that bought a revolution

Akshit Chauhan[1], Deepak Chandel[2], Deepak Kumar[3]

[1,2,3]*CSE Department*
DCE Gurgaon

Abstract: All people were exchanging SMS(short message service) till the time whatsapp was launched for android market, ios , blackberry and windows phone. It was an invention that none one of us had think of, but it happened, and it was made possible by us citizens "BRIAN ACTON" and "JAN KOUM"(former employees of yahoo!) in 2009 as they founded "WHATSAPP INC." , a company with 55 employees. Whatsapp Messenger is basically a proprietary, cross platform instant messaging subscription service for smartphones that uses internet for communication in addition to text messaging , users can send each other images, video and audio media messages as well as their location using integrated mapping features. There are many online messaging applications available like "LINE","VIBER","HIKE","WeChat","KAKAO TALK","TELEGRAM","SKYPE","TANGO", but no other application has crossed the number of users , whatsapp messenger has crossed(it handles 27 billion messages per day).But this fantastic applications had some security breaches and loopholes which made the founders of the application to work on it and make it secure. They succeeded to a much extent but it's still not secure.

Keywords: nWhatsapp, messenger , breaches , loopholes , proprietary.

I. INTRODUCTION

WhatsApp Messenger is a cross-platform mobile messaging app which allows you to exchange messages without having to pay for SMS.

WhatsApp Messenger is available for iPhone, BlackBerry, Android, Windows Phone and Nokia and yes, those phones can all message each other! Because WhatsApp Messenger uses the sameinternet data plan that you use for email and web browsing, there is no cost to message and stay in touch with your friends.

In addition to basic messaging WhatsApp users can create groups, send each other unlimited images, video and audio media messages.

WhatsApp was switched from a free to paid service to avoid growing too fast, mainly because the primary cost was sending verification texts to users. In December 2009 WhatsApp for the iPhone was updated to send photos. By early 2011, WhatsApp was in the top 20 of all apps in the U.S. App Store[1].

II. BRIEF HISTORY OF WHATSAPP MESSENGER

In June 2009, Apple launched push notifications, letting developers ping users when they were not using an app. Koum updated WhatsApp so that each time you changed your status it would ping everyone in the user's network. WhatsApp 2.0 was released with a messaging component and the active users suddenly swelled to 250,000. Koum visited Brian Acton, who was still unemployed while managing the unsuccessful start up, and decided to join the company. In October Acton persuaded five ex-Yahoo friends to invest $250,000 in seed funding, and as a result was granted co-founder status and a stake. He officially joined on November 1.[7] After months at beta stage, the application eventually launched in November

2009 exclusively on the App Store for the iPhone. Koum then hired an old friend who lived in Los Angeles, Chris Peiffer, to make the BlackBerry version, which arrived two months later[2].

III. PLATFORM USED AND TECHNICAL SUPPORT

The application eventually launched in november 2009 exclusively on the App Store for the iPhone. In August 2011 a beta for some Nokia series 40 was added, being the first smartphone OS with whatsapp support. A month later support for windows phone was added and then blackberry 10 in march 2013.In June 2014, a Whatsapp employee also confirmed that the company is working on a tablet version of the App and the oldest device currently capable of running Whatsapp officially is the Symbian-based Nokia N95 in March 2007.

Whatsapp uses a customized version of the open standard "Extensible Messaging and presence Protocol(XMPP)" which is a communications protocol for message-oriented middleware based on XML (Extensible Markup Language).This protocol was developed by Jabber open source community in 1999 for the near real time , instant messaging (IM),contact list maintenance and presence information, it is designed to be extensible , the protocol has also been used for publish-subscribe systems, signalling for VoIP, video, file transfer , gaming and for some social networking services. Whatsapp uses a fantastic technique , a software that compares al the phone numbers form the device's address book with it's central database to add contacts to the user's whatsapp contact list. Previously it was a different scenario. Earlier the Android and Nokia S40 version used an MD5- hashed(The **MD5** message-digest algorithm is a widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed in text format as a 32 digit hexadecimal number. MD5 has been utilized in a wide variety of cryptographic applications, and is also commonly used to verify data integrity). Almost all smartphones(Android, Blackberry ,iPhone , Nokia) support Whatsapp Android phones running on above Android 2.1 and above , all Blackberry devices having OS 4.7 or later and iPhones running on iOS 4.3 and later support whatsapp. Multimedia messages are sent by uploading the image, audio or video to be sent to an HTTP server and then sending a link to the content along with its Base64 encoded(**It** is a group of similar binary-to-text encoding schemes that represent binary data in an ASCII string format by translating it into a radix-64 representation. The term *Base64* originates from a specific MIME content transfer encoding.)

IV. SECURITY ISSUES

- If an application is made, it's not possible at the beginning/at the development time that it may possess all the security factors needed. This also happened with Whatsapp Messenger, in which, May 2011, a security hole was reported which left whatsapp user accounts open for session hijacking(it is sometimes also known as "cookie hijacking" , it is the exploitation of a valid computer/whatsapp session—sometimes also called a session key—to gain unauthorized access to information or services in a computer system/whatsapp) and packet analysis(a computer program or a piece of computer hardware that can intercept and log traffic passing over a digital network or part of a network). Earlier, the messages that were exchanged between the people were sent in a non-encrypted format , which allows anybody to intrude/see messages between two people, if the packets were available for that session an obtaining packets was not a big deal at that time.

- Another security issue was there in WhatApp when an unkown hacker hosted a website called whatsappstatus.net that made it possible to change the status of an whatsapp user, as long as the phone number was known. It was one of the vulnerabilities in whatsapp . To resolve the problem ,in form of security measure the website's IP-Address was blocked and in return a window tool was made which was providing the same functionality.

- Due to several reasons , whatsapp was removed from the iOS App store and no disclosure was being made.

- Around 2012, the security researchers noticed that when whatsapp was again available on App store , the messages that were exchanged between people were not in a plain text, they were encrypted . The cryptographic method used was described as "broken".
- Another problem that arised a security concern in the whatsapp messenger was that as soon as somebody installs whatsapp on their phones , it used to read the list of all contacts and provide the user with a list of filtered contacts that were already registered on

ISSN: 2321-9653

Whatsapp. The issue was that whatsapp require the user to upload their entire address book to the whatsapp server which were mirrored on the Whatsapp Servers , including the contact information for the contacts who are not using whatspp. Though this information was stored in a hashed form , still it was not secured

V. ENCRYPTION AND DECRYPTION

Earlier the messages that were exchanged between people were not encrypted but these days messages are encrypted in a format "msgstore.db.crypt7". Some people don't know about whatsapp chat database mechanism. The WhatsApp chat database is saved on the SD card/Internal memory which can be read by any Android application if the user allows it to access the SD card, as we know people use many apps, games so its very easy steal whatsapp chats database file from SD card using any android malware app/stealer app. now lets directly make a simple stealer to steal database, you can find whatsapp database in your SD card>Whatsapp>Database folder named as "msgstore.db.crypt7".

It can be decrypted using a simple method , one need to follow just simple steps:

- Apply some Social Engineering(refers to psychological manipulation of people into performing actions or divulging confidential information) techniques to get access to the whatsapp database of your friend / victim whose chats you want to read.
- After getting all the Database files with extension "msgstore.db.crypt7", save it into your computer.
- Open the Browser and go to www.recovermessages.com or http://www.desencriptawhatsapp.com.ar/.
- After opening one of these websites , upload all those database files that you have saved in your system by clicking the upload option.

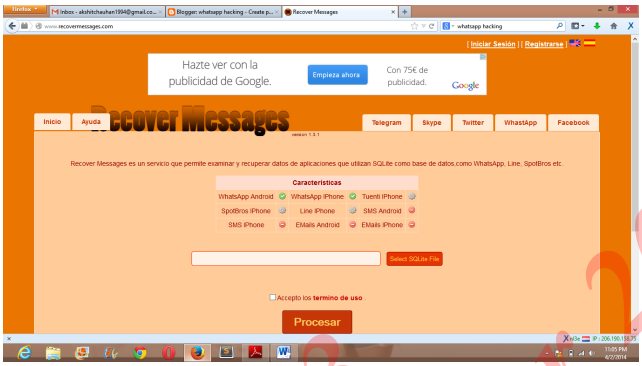


Fig 1. Screenshot of the first website www.recovermessages.com

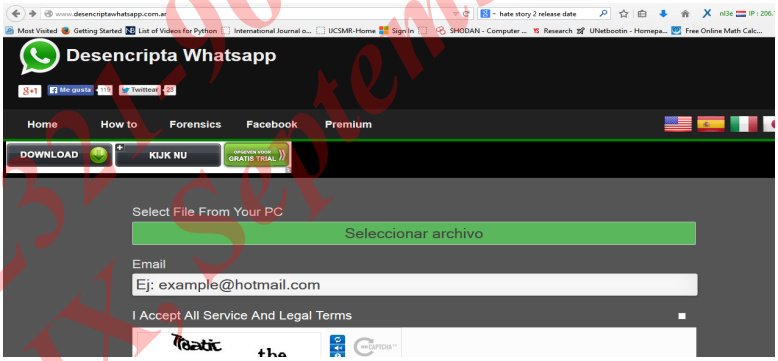


Fig2. Screenshot of second website that helps in decrypting whatsapp messages http://www.desencriptawhatsapp.com.ar/

VI. FUTURE SUGGESTIONS

The future of WhatsApp is now in Facebook Inc. hands because Facebook Inc. has bought whatsapp from it's founders and developers at a huge amount of 19billion dollars(1900 crores approx).After Facebook acquired Whatsapp some updates were to be seen in its functioning i.e users were able to hide their last seen , profile picture , status from their contacts as well as from the unknown persons.
There are three options available when we go to whatsapp->settings->account->privacy .One is to show all the three parameters to everybody , to all contacts , not to show any of the parameters to anybody.
This update to whatsapp came as soon as Facebook took over WhatsApp Inc.
In future we would expect more of such updates from Facebook Developers.

VII. CONCLUSION

There is a still need to apply a more complex algorithm to build such a encryption technique that no one could decrypt by uploading messages on any website or by using any programming language script especially python scripts are more useful in these types of decryption techniques using Linux operating system.

REFERENCES

[1] Whatsapp (Internet Sources: Wikipedia)

[2] Whatsapp (Internet Sources: Wikipedia)

[3] http://akshitchauhan01.blogspot.com/

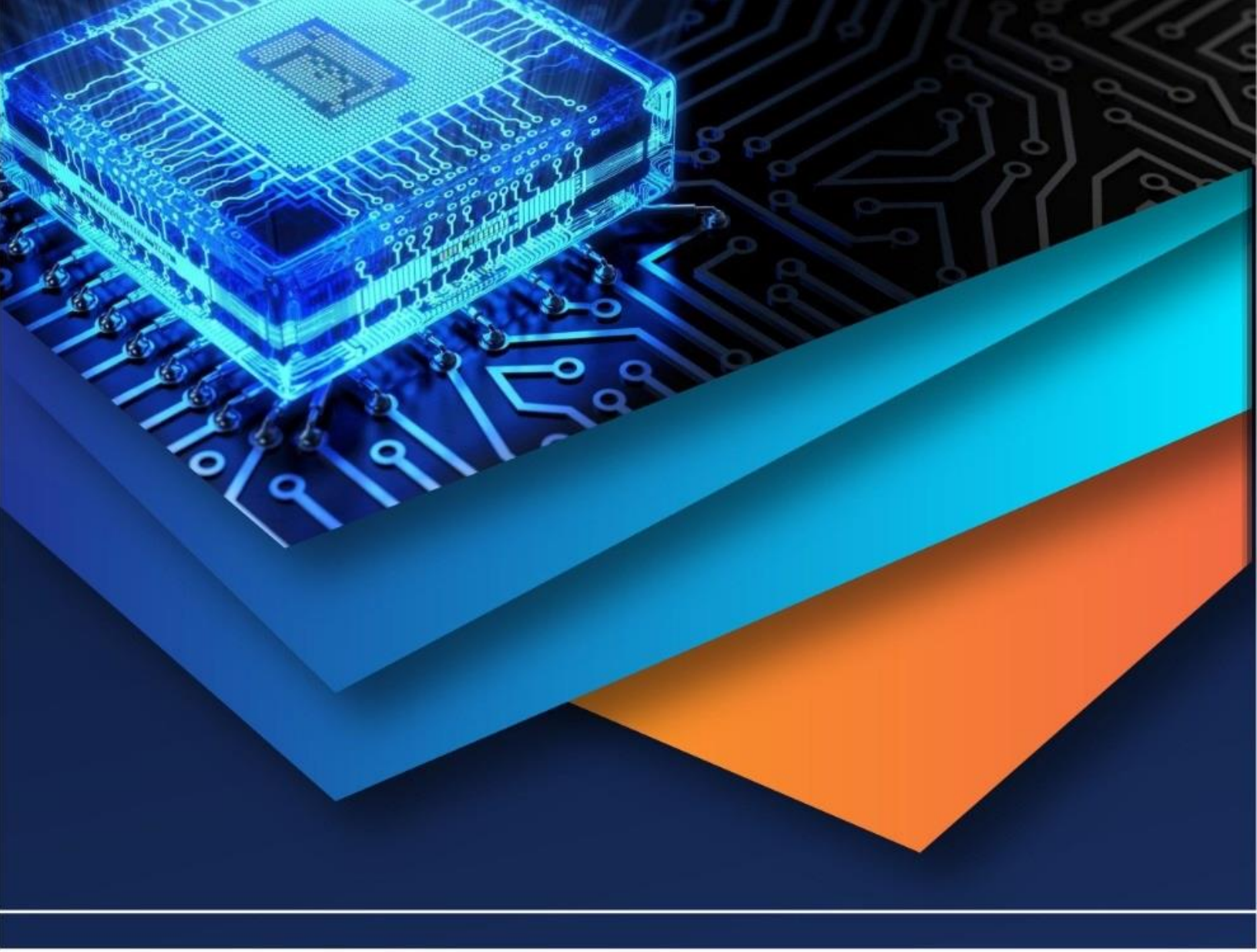
[4] http://www.googlescholar.com

[5] www.Wikipedia.com

[6] http://www.whatsapp.com/

[7] http://www.desencriptawhatsapp.com.ar/

[8] www.recovermessages.com



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY