Security Aspect in Instant Mobile Messaging Applications

Puneet Kumar Aggarwal
Amity University,
Noida, India
puneetaggarwal7@gmail.com

P.S. Grover
KIIT Group of Institutions
Gurgaon, India
drpsgrover@gmail.com

Laxmi Ahuja
Amity University,
Noida, India
lahuja@amity.edu

***Abstract* - Instant mobile messaging applications are one of the most popular applications for communication between the users. The applications initiates' message sending via internet, making it cost free for the users. Sending of messages can be in any form either a text message or it can initiate voice call. Almost all of these applications offer different built in features which makes the apps appealing to the user but in majority of cases, the app developer's neglect security feature of their usage. Security as one of the important factor plays a vital role for measuring quality of mobile applications. So, it's important to identify level of security services provided by these apps. This research paper presents a study on current security features of popular instant mobile messaging applications and also discusses the reason to focus more on security aspects for improving the overall quality of these applications.**

Keywords: mobile; applications; instant messaging; chat; security; quality

I. INTRODUCTION

Chatting applications have already spread their roots all over the world. They are ubiquitous. Almost every Smartphone user uses these applications on a daily basis. Their tempting offers and attractive features make it even more difficult for Smartphone users to escape them. There are millions of Smartphone available in the market with different operating systems [21]. They have the capability of installing different applications on them in order to be able to perform many tasks, such as messaging. Wi-Fi networks showed a tremendous increase in the last few years. According to a study, by the end of year 2020, there will be thrice the number of broadband subscribers then they are today [25].

The increasing internet facilities give a great opportunity for instant messaging applications and have made them capable of creating a brand new era in the field of communication. Instant messaging applications are particularly the most popular category of applications among the users [7,10].

They have the capability of sending text as well as voice messages or initiating voice or video calls, sharing media files [12], also includes dwelling with friends [13], group chats [16] via internet, which makes it cheaper for users to communicate with each other all over the globe.

978-1-5386-1686-4/18/$31.00 ©2018 IEEE

There are many applications available to users. Many of them claim to be providing high security and confidentiality to user's information proving the app as quality app, yet news papers are usually flooded with security issues of such applications. According to a report provided by Electronic Frontier Foundation (EFF) majority of these chat applications do not provide enough security for their users [22]. Unfortunately, instant messaging applications are no exception. Some malicious users, hack into the servers and get access to the information of other users that can be used against them. It proves that many developers do not consider security as the primary goal of their applications. This is the major reason for quality degradation of mobile applications. Developers are required to focus more on security to provide quality app's to users.

Securing mobile messaging applications is important because of many reasons. Various studies showed that most of the popular messaging apps failed to the security standards. This refers that while these applications are popularly known and used by many people, the companies might misuse the information of their users. While many messaging applications are free to use, developers equip the applications with built-in processes which track every single movement of their users and then sell their private information to the 3rd party advertisers in order to earn money. This is done without the knowledge of the users and ultimately the privacy of user is compromised and in some cases, causing personal loss to the user. This also has wider legal and security implication to the users.

The main purpose of this research paper is to highlight the security aspects provided by application developers. Some instant mobile messaging applications have been selected and investigated from security perspective for improving the overall quality of these applications.

The rest of the paper is organized as follows. Section II presents the background with the brief study of security aspects of such applications for the user. Section III discusses some of the popular instant messaging applications, reviewing the general features provided by them and also presents the summary of selected messaging applications from the security point of view. Section IV presents the conclusions drawn from the study and future work to improve the overall quality of these applications

while making them more secure for communication purpose. Finally references at last.

II. BACKGROUND

Smartphone business across the world has seen rapid growth over the years. According to a report, by the end of 2020, 90% of world population will have access to Smartphone [25]. One of the many reasons behind this fast growth is decreasing cost due to a number of competing manufacturers of Smartphone. The powerful hardware and popular applications have caught the imagination of the young generation. Therefore, there is a demand and supply in abundance.

More Smartphone means more operating systems. Two of the main operating systems are android and iOS. As of August 2017, there are approximately 3197242 applications available for android in Google play store and around 2200000 applications are available for iOS Apple store [23].

A. Smartphone Ecosystem

Smartphone attracts users mostly with their operating systems. Application stores are itself an ecosystem which provides everyone including freelance developers as well as companies, a chance to publish their applications. Anyone who has access to internet can discover the applications which get approved by the store.

Every industry can benefit from such ecosystem. Many industries including insurance, teaching and even government agencies are getting benefits of Smartphone ecosystem and internet access to better serve their customers. Instant messaging is one of the application used word wide for communication using internet. Many companies are providing instant messaging services to their users. All these IM applications compete with each other to get more users and to defeat other players in the market. They are always trying to attract more users by creating better user interface and offer more features to the users [24].

B. Security services for mobile instant messaging

There are 3 key aspects to evaluate any Chat application from security point of view. They are: Confidentiality, Integrity and Availability. Confidentiality ensures that certain type of information can be accessed only by the authorized parties. Integrity means information can be modified only by intended and authorized parties. Availability means that information is accessible to authorized parties at authorized times [17,26].

1) Confidentiality:

Confidentiality is privacy which is achieved when messages are exchanged by two parties through a communication channel, is readable only to the parties linked with that channel. It can be achieved by encryption. It is a process in which a message is encrypted by a cryptographic technique and this message can only be read by the intended party by decrypting the same message as described in Fig.1.

Cryptography is the practice which is used to secure a communication between two entities in the presence of any third party [1]. It supports confidentiality, integrity, authentication of user by creating a suitable medium channel. Cryptography uses two major types of algorithms: symmetric key cryptography and public key cryptography.

Symmetric key cryptography provides both the intended parties a shared key to encrypt and decrypt the messages. Even if the third party somehow manages to intercept the communication channel, he will not be able to decrypt the encrypted message as he does not have the shared key [5].

Public key cryptography uses the algorithm which needs two keys. Those keys are: the private key and the public key. Public key cryptography is sometimes also known as asymmetric cryptography [2].

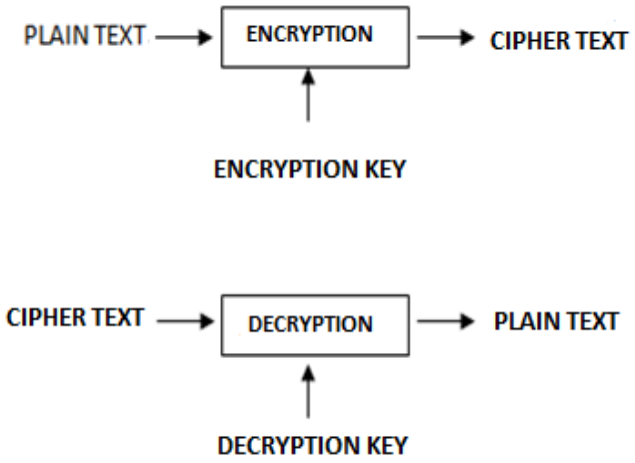

Fig. 1. Message sending using cryptography

2) Integrity:

Integrity is used to make sure that only the original message is transferred between the entities. Without that, any malicious user could try to modify or even delete the message. Integrity is achieved by hashing. Hashing uses a hash function which maps an encrypted message to a fixed size length integer. It is a one way function, which implies, even if someone has an output of the hash, it cannot be reversed.

3) Availabiity:

Availability keeps the data and resources available for authorized use, especially during emergencies or disasters. Information security professionals usually address 3 common challenges to availability:

1. Denial of Service (DoS) due to intentional attacks or because of undiscovered flaws in implementation.

2. Loss of information system capabilities because of natural disasters or human actions (bombs or strikes etc)
3. Equipment failure during normal use.

III. Mobile Chat Applications

As it was mentioned in previous sections, there are many chat applications in the mobile market. Recently some chat applications have started to distinguish themselves in the market by calling themselves as "secure chat application". Normally in these types of chat applications, they are self-claimed by their providers that they have prioritized security and privacy of their users at the first place. Although majority of chat applications use various types of encryption, unfortunately in most of the cases, the IM owners' servers issue the keys or have access to message keys to decrypt them.

In order to investigate IM apps' security features, several IM applications have been selected based on their popularity. In the following sections, a brief study of different mobile instant messaging applications is presented. Five different chat applications have been selected based on their popularity, business orientation, and self-claimed security providing services.

A. WeChat

It was first released in 2011 and by 2017 it was one of the largest standalone messaging application used for social messaging by ample of users. Number of tasks can be done by using this single application, hailing a taxi, splitting the bill in a restaurant, purchasing a cinema ticket, investing in financial products, transfer money to their friends, shopping online.

This is a messaging application used by the platform of both Android and iOS [18]. It does not provide end to end encryption but it uses public key for encryption. WeChat encrypts the message transferred between the server and the device, in order to secure it from any third party which might be waiting for unencrypted message to be transferred over internet.

B. Facebook Messenger

Facebook Messenger is an instant messaging service and software application. It was originally developed as Facebook Chat**.** There can be transfer of text messages, pictures, audio or video, document files, stickers between the users. Users are also provided with the facility of voice as well as video calling through the messenger [4]. Multiple accounts can be maintained with the same application. It uses end-to-end encryption technique to provide security to users. As on April 2017, messenger has active 1.2billion users worldwide.

C. WhatsApp

WhatsApp is one of the most commonly used messaging applications all over the world. Users are allowed to make voice calls, video calls, send text messages, images, GIFs, contacts and many more through internet. It also provide users with a special feature known as status, which allows users to upload photos, small videos for a time span of 24 hours.

In spite of all these facilities, WhatsApp uses end-to-end encryption and has more than 1.3 billion active users [3].

D. Wickr

The primary objective of the Wickr Secure Messaging Application is to provide secure communication between two or more correspondents. Wickr has some unique features which make it very appealing for users [19]. One of such features is that they offer self-destruct messages, which means that as soon as user reads the message, the message will be wiped of the recipients Smartphone. They claim that the application removes all the metadata and they do not upload users' contact book to the server. It uses end-to-end encryption for data security.

E. Viber

Viber is one of the most popular free chat applications with millions of users all over the world. A research revealed that, Viber is not secure for many reasons. One of the major reasons research for this, media files such as pictures, videos which are transferred between users, have no encryption at all and the data is stored on Viber server unencrypted which can be accesses without any authentication mechanism [20]. This gives malicious users the ability to simply launch Man-in-the-Middle attack. It is a kind of attack in which a malicious user intercepts the communication channel and listens to the conversation of two parties. Viber does not support end-to-end encryption.

Use of mobile applications is among the top activities on Smartphone users. People use them to communicate with others by sending text messages, photos, videos, emoji's, text files and other type of contents either individually or as a group. Table I provides brief overview of different features that are provided by these five selected chat applications.

IV. Security Aspects

As it has been mentioned previously that, majority of Instant message chat applications are closed source and not having proper documentation, restricting external auditors and security experts to investigate the security of these applications. Number of parameters exists based on which security of applications can be measured. Some of the parameters that are important are identified and explained below.

A. Encryption for message transfer

In cryptography, encryption of a message refers to the encoding a message that can only be accessed by authorized parties. It denies the interference of interceptor; it does not prevent interference by itself. While doing encryption, the intended message, referred to as plain text and the encrypted message is referred as a cipher text which is further decrypted to again convert it into plain text.

TABLE I. GENERAL FEATURES OF INSTANT MESSAGING CHAT APPLICATIONS

	We Chat	Voxer	Wickr	Viber	WhatsApp	Messenger
E2EE	No		Yes	No	Yes	Not by default but can be done
Open Source	No	No	No	No	No	Yes
Secure Channel	Yes	Yes	Yes	Yes	Yes	Yes
Mobile Platform	Android iOS Windows	Android iOS Windows	Android iOS	Android iOS Windows	Android iOS Windows	Android iOS Windows
Group Chat	Yes	Yes	Yes	Yes	Yes	Yes
User Friendly	Yes	Yes	Yes	Yes	Yes	Yes
Liked to Phone Number	Yes	Yes	Yes	Yes	Yes	Optional
Block Unknown User	Yes	Yes	Yes	Yes	Yes	Yes
Mute Notification	Yes	Yes	Yes	Yes	Yes	Yes
Voice Call	No	Yes	Yes	Yes	Yes	Yes
Video Call	Yes	No	Yes	No	Yes	Yes
Free SMS	No	No	No	Yes	No	No

B. *Encryption for file transfer*

For encryption file data while transferring it from one node to other, three options are available which are: file transfer protocol (FTP), secure file transfer protocol (SFTP) and hyper text transfer protocol (HTTP). The most widely implemented and fastest option is FTP. It has a wide range of data ports. SFTP and FTP are more for use within the server whereas HTTP is more interactive to users. In spite of all these, all three of them will however encrypt the data and protect it from attackers over internet.

C. *Encryption by default*

Security of data transferred is also provided by the channels used to transfer the data. Secure Sockets Layer (SSL) is a security protocol used to establish an encrypted connection between server and client. It transmits sensitive information such as credit card numbers etc, securely using some channel secure algorithms. Every browser interacts with secured servers using SSL protocol establishing the secured connection. SSL secures large number of information every single day especially during online transactions and while transmitting confidential information.

D. *Encryption Cipher*

Cipher is an algorithm which is used to encrypt or decrypt the information. Mostly, ciphers substitute same number of odd characters as inputs but sometimes it can be more and sometime less. Encryption Cipher can be categorized as follows:

i) Encryption using symbols: message can be encrypted using either blocks of symbols or continues stream of symbols.

ii) Encryption using keys: It can use same key for both the purpose that is, for encryption and decryption which is referred as symmetric key encryption algorithm or it can use different keys for encryption and decryption, which is called asymmetric key algorithm (example; RSA, ECC, DSA etc).

E. *Key Size for encryption*

Key size can be defined as the number of bits in a key used by any cryptographic algorithm. There can be different key size for different algorithm. For securing data against any forge activities, the key size must be large so that interceptors could not be able to crack it within the specified period of time. The key used to encrypt the data is one of the confidential concept which provides security in all aspects.

F. *Self destructing messages*

Self-destructing message paramount's personal security while sharing people personal messages through various messaging applications. in general, popular messaging apps offer security in the form of end-to-end encryption, but they don't offer any security of the chats, when the apps are on your device. Also, some people don't want to save messages while chatting, this is where self-destructing messaging applications come into play. Using this service provides applications to destruct messages automatically when they are read or after a certain period of time, which can be decided by the user itself.

By identifying the above security parameters, based on which one can define the security provided by different instant messaging applications and can predict about the quality of messaging applications. Table II below provides the summary of the above selected popular messaging applications in respect of security based on different criteria's'.

V. CONCLUSION

With the continuous improvement of use of mobile applications in each and every field there is a need of quality applications. Many different characteristics usually represent the quality of an application. The application developers must refer to quality standards while developing software applications for mobile. It helps in maintaining and improving the quality of their applications for mobile. In different quality models, security referred as one of the quality characteristic for mobile applications. Developers are required to develop quality applications with the defined standards for security as per the quality models. In majority of cases, the app developer's neglect security feature which results in app quality degradation. So, it's important to identify level of security services provided by these apps. The research paper presents a study on current security features of popular instant mobile messaging applications and also discusses the reason to focus more on security aspects for improving the overall quality of these applications.

Future work includes consideration of other quality characteristics important for mobile applications and issues that must be taken care off while developing applications so that, developers are able to develop good quality applications

providing ever-improving quality of software in a quantifiable manner.

TABLE II. SECURITY FEATURES OF INSTANT MESSAGING CHAT APPLICATIONS

	Viber	We Chat	WhatsApp	Facebook Messenger	Wickr
Operating System Support	Windows Phone, Android iOS, BlackBerry OS, Symbian	Windows Phone, Android iOS, BlackBerry OS, Symbian	Windows Phone, Android iOS,	Windows Phone, Android iOS,	Android iOS,
Encryption	Concepts of "Double Ratchet", 128-bit Symmetric	Client-to-server and server-to-client	Signal Protocol, Calls-SRTP	Encrypted with AES CBC and authenticated using	Elliptic Curve Deffie Hellman key Exchange
Encrypted by Default	YES	-	Yes	No	Yes
Encryption Cipher	Asymmetric ECC	-	Symmetric, Asymmetric ECC	Symmetric, Asymmetric ECC	Symmetric, Asymmetric ECC,RSA, DSA
Key Size	256	-	256	256	256
Encrypted Ground Chat	Yes	-	Yes	No	Yes
Encrypted File Transfer	Yes	-	Yes	-	-
Self Destructing Messages	No	No	No	No	Yes

References

[1] R. L. Rivest et al.,"A Method for Obtaining Digital Signatures and Public-key Cryptosystems", Vol. 21 (2), pp. 120–126, ACM, 1978.

[2] C. Kaufman et al., "Network Security: Private Communication in a Public World", Prentice Hall PTR, 2002.

[3] K. Church and R. deOliveira, "What'sup with whatsapp? :Comparing mobile instant messaging behaviors with traditional sms", In Proceedings of the International Conference on Human-computer Interaction with Mobile Devices and Services, pp. 352-361, ACM, 2013.

[4] "Facebook Messenger" [Online] Available: https://www.messenger.com/

[5] "Introduction to Cryptography: Principles and Applications - Second Edition. Hans Delfs, Helmut Knebl," pp. 12, 2007.

[6] R. Ling, "New Tech, New Ties: How Mobile Communication Is Reshaping Social Cohesion", The MIT Press, 2008.

[7] M. Bohmer et al., "Falling a sleep with angry birds, facebook And kindle: A large scale study on mobile application Usage", In Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services, MobileHCI'11, pp. 47 56, ACM, 2011.

[8] A. Shabtai et al., "Google Android: A Comprehensive Security Assessment", IEEE Security and Privacy, Vol. 8 (2), pp. 35-44, 2010.

[9] M. Landman, "Managing Smart Phone Security Risks", in Proceedings of Information Security Curriculum Development, pp. 145-155, ACM, 2010.

[10] A. Hang et al., "Too much information!: User attitudes towards smartphone sharing" In Proceedings of the 7th Nordic Conference on Human-Computer Interaction: Making Sense Through Design, pp. 284–287, ACM, 2012.

[11] A. P. Felt et al., "Android Permissions: User Attention, Comprehension, and Behavior", In Proceedings of the Eighth Symposium on Usable Privacy and Security, 2012.

[12] Y.-Y. Chen et al., "Sharing (and discussing) the moment: The conversations that occur around shared mobile media", In Proceedings of the International Conference on Human-Computer Interaction with Mobile Devices and Services, pp. 264–273, ACM, 2015.

[13] K. P. O'Hara et al., "Everyday dwelling with whatsapp", In Proceedings of the International Conference on Computer Supported Cooperative Work & Social Computing, pp. 1131–1143, ACM, 2014.

[14] [14] A. Mylonas et al., "Delegate the smartphone-user? Security awareness in smartphone platforms", Computers & Security, Vol. 34, pp, 47-66, 2013.

[15] M. La Polla et al., "A Survey on Security for Mobile Devices", Communications Surveys & Tutorials, pp. 446-471, IEEE, 2013.

[16] M. E. Smith and J. C. Tang, "they're blowing up my phone": Group messaging practices among adolescents", 2015.

[17] C. P. Pfleeger and S. L. Pfleeger, "1.3 the Meaning of Computer Security - Security in Computing, 4th Edition."

[18] "WeChat Developers," WeChat API Documentation. [Online]Available: http://dev.wechat.com/wechatapi/documentation.

[19] "Wickr | Top Secret Messenger"[Online] Available: https://wickr.com/.

[20] "Viber Security Vulnerabilities: Do not use Viber until these issues are resolved."[Online]. Available: http://www.unhcfreg.com/#!Viber Security-Vulnerabilities-Do-not-use-Viber-until-theseissues-are resolved/c5rt/BB4208CF-7F0A-4DE1-92A4 529425549683.

[21] "Most popular global mobile messenger apps 2017 Statistic," Statista. [Online].Available:https://www.statista.com/statistics/258749/ most-popular-global-mobile-messenger-apps/

[22] "Secure Messaging Scorecard," Electronic Frontier Foundation.[Online]. Available: https://www.eff.org/secure-messaging-scorecard.

[23] "Number of apps available in leading app stores 2017 | Statistic."[Online]. Available: https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/

[24] "Number of mobile messaging users worldwide 2017 | Statistic."[Online]. Available: http://www.statista.com/statistics/369260/mobile-messenger-users/.

[25] "Ericsson Mobility report," Ericsson, June. 2017.

[26] "NIST SP 800-12: Chapter 1 Introduction." [Online].Available: http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf