Common Vulnerabilities and Risk Analysis in Messaging Applications in Social Media with special reference to Whatsapp

Rakhi Gupta
Computer Engineering Department, PHd Research Scholar
Bharati Vidyapeeth Deemed University College of Engineering, Pune. India

Dr. Suhas Patil
Professor , Computer Engineering department
BVDUCOE , Pune

Dr. S.D. Joshi
Professor ., Computer Engineering department,
BVDUCOE , Pune

Abstract- Social Messaging apps are latest buzzword. The aim of this paper is to highlight the risks and vulnerabilities common to all the social messaging application which are adding data to this streaming model. The ease of social interaction added by these applications like Whatsapp , Viber, Snapchat, Wechat etc. is not without hazards. The most dangerous of this is Authentication and Account Hijacking, which allows an attacker to become the master of victim's account. Next is Sender ID Spoofing/Message Manipulation where an attacker can manipulate or forge messages and sender information but not hijack the entire account. In risk of Enumeration, all applications allow the users to upload their phone book to identify registered users. The server replies with the list of contacts registered with the service. Thus it can be found out whether the targeted person uses this service and status messages of that user can be used for profiling. It can also lead to impersonation and spoofing attacks. If we take case study of Whatsapp, it allows user profiling without user knowledge also the users still cannot tell the difference between end-to-end encrypted messages and regular messages. There are seven basic requirements for a secure and privacy preserving chat service. Taking these, we have provided a comparison between our risk analysis for these commercially available products. The aim of the paper is to analyze the risk for Social media services and explore any potential complexities involved in such a service providing privacy, protection to its customers.

Keywords: Social media , Risk Analysis , Security, Social Messaging Applications

I. INTRODUCTION

Social Media streaming contributes to a large amount of data component of Big data. Social Messaging applications like Whatsapp go a long way in adding to this streaming. When we talk of online communications , WhatsApp is the most popular name. The application has over 1 billion active users as on February 2016. [6]. This facility and ease of use comes with its own vulnerabilities and risks. The aim of this paper is to highlight some of these risks with the aim of mitigation of selected ones.

II. RISKS IN WHAT'SAPP

WhatsApp is considered to be one of the biggest mobile chat services available on different platforms (e.g. iOS, and Android). [11] [13]. The primary aim of these apps is on messaging and privacy concerns are secondary. WhatsApp stores the chat history on the client's device and does not store any messages on the server. The client application uses SSL[14] to connect to the server; however, a recent blog posting [12] discussed the deployment of SSL version 2. This deployment might open up WhatsApp to attacks on SSL 2.0. To provide security in chat messages between sender and receiver there is no E2E encryption. However the message server can read the exchanged messages.

2.1 Security Risks,Flaws and Vulnerability :

Its fairly easy for any attacker to hijack a user's account , and this account cannot be recovered by the user. It is being warned that WhatsApp is easily hackable .[1] According to H Security reports , using WhatsApp on a public Wi-Fi network is risky as data can be sniffed and account can be misutilized to send and receive messages. It is not possible then to restore account security.

According to H Security , the app uses an password which is internally generated, to log onto the server , which is generated on Android devices from the device's IMEI number , on iOS devices from the devices MAC address. " The problem is that this information is not secret as IMEI can be found on stickers inside Android phones (under the battery) and it is easy to obtain it using a shortcut key combination or by any third party app," Sniffing(gathering) this data on devices on iOS is much simpler as the MAC address is easily seen by anyone within range of the Wi-Fi network being used. With this data , it's very easy to hijack the account. "The attacker enters the MAC or the IMEI into a script . This allows him to send messages using the hijacked account." It is not possible to block the attacker as the password cannot be changed .

2.2 Crash Messages

Some time back , it was discovered that it was possible to crash someone's instance of WhatsApp by sending a message over 7 MB. . After the message is received, WhatsApp crashes every time user tries to open the thread. And control can only be gained by deleting the thread. The same effect can be achieved by sending a much smaller message – only 2 KB in size containing a set of special characters.

2.3 The first one is modification of user's status message by a probable attacker.

We analyzed the protocol for setting the status message and find out vulnerabilities that could cause unauthorized modification of status messages.

2.4 *Privacy-related design error.*

It is possible to figure out whether the owner of a given phone number has installed the messenger application. The status message of the user is also visible to the people who have stored this user in their address book. To store any user's number , no user confirmation is required , so an attacker can get status messages of all subscribers to this service. This approach can be combined with other approaches for an enumeration attack. It was confirmed that the protocol has been implemented for Android messages and that WhatsApp messages from /to iPhones running iOS are still not end-to-end encrypted. The WhatsApp users still cannot tell the difference between regular messages and end-to-end encrypted messages.

Figure 1. Results for circumvention tools [2]

Functions	Tool	Security	Resilience	Usability	Overall
Text(Android)	Whatsapp	* Figure 3.	* Figure 4.	**** Figure 5. ***	Good
Text(iOS)	Whatsapp	*	*	****	Good
Text(Symbian)	Whatsapp	*	*	****	Insufficient
Text(Blackberry	Whatsapp	*	*	****	Adequate

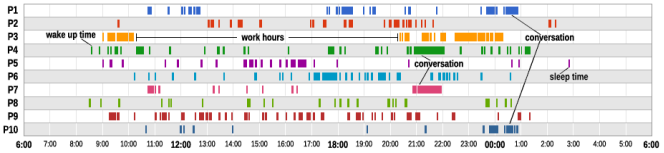
2.5 Poor implementation of SSL encryption could be a boon to eavesdroppers. [3]

WhatsApp follows Version 2 of SSL encryption., The version is susceptible to several well-known attacks that allows people to peep into a connection between the two end points and also to decrypt and manipulate the traffic as it passes through. WhatsApp has not completely implemented certificate pinning , that blocks attacks using forged certificates to bypass Web encryption.

Praetorian also notes two WhatsApp SSL deficiencies: the use of SSL null ciphers and the SSL export ciphers being enabled . Both weaknesses make it easier for attackers to bypass encryption. It allows a Man –in –the –middle attack for downgrading the encryption , so sniffing can be carried out. [7]

2.6 Presence information is inferred from interaction with the messaging app [4]

WhatsApp sets the presence status to \online , automatically when the app is in foreground, and to off line when it is in the background. The \last seen feature reports when the user was last online. Any Whatsapp user can see user's presence information as long as the phone number is known and was added to the phone's address book. The automatic transmission of the presence status (online or offline cannot be deactivated. This subscribes to a kind of presence information which allows for continuous monitoring of the presence status.



Presence information showing the WhatsApp activity of a group during one day. A bar on the timeline shows the amount of time WhatsApp was actively used. [4] This information could be collected by management and the user will not even be aware of this form of surveillance or how it would be used [8]

	VoIP	Text Messages	Number Verification	Uploads Address Book
WhatsApp 2.6.4	no	yes	SMS, active SMS	yes
Viber 2.0.3	yes	yes	SMS and passive phone call	yes
eBuddy XMS 1.15.2	no	yes	SMS	yes
Tango 1.6.9568	yes	no	SMS	yes
Voypi 1.2	yes	yes	SMS	yes
Forfone 1.5.6	yes	yes	SMS	yes
HeyTell 2.3.0	yes	no	no	no
EasyTalk 2.0.1	yes	yes	SMS	yes
Wowtalk 1.0.3	yes	yes	SMS	yes
	Status Messages	Platforms	Estimated User Base	
WhatsApp 2.6.4	yes	Android, iOS, BlackBerry, Symbian	23-63M	
Viber 2.0.3	no	Android, iOS	10-15M	
eBuddy XMS 1.15.2	no	Android, iOS	1-1.5M	
Tango 1.6.9568	no	Android, iOS	10-15M	
Voypi 1.2	no	Android, iOS	0.1-0.15M	
Forfone 1.5.6	no	Android, iOS	0.2-0.25M	
HeyTell 2.3.0	no	Android, iOS	5-9M	
EasyTalk 2.0.1	no	iOS	0.25-0.3M	
Wowtalk 1.0.3	yes	iOS	0.06M	

Table 1. Overview of selected smartphone messaging applications, their features, supported platforms, and estimated user base.

III. SALIENT FEATURES

3.1 WhatsApp uses a customized version of XMPP [8], an open XML-based communication protocol for message-oriented middleware, near real-time instant messaging, sharing of presence information, and maintenance of contact list. Whats-App gives the same features plus the ability to upload multimedia data such as images, audio or video content.

Three basic steps can be performed to automatically collect a WhatsApp user's presence information: Registration(One time), user login, and subscription to presence information. [4]

3.1.1 One-time WhatsApp Registration

Identification of WhatsApp accounts is done by a unique username based on users' international phone numbers (e.g., 491511000110@s.whatsapp.net). The following steps are compulsory to create a new user account:

1. The phone number and a SHA1-hashed device identity have to be POSTed to an HTTPS URL to request for a six digit authentication code.

2. The authentication code is received via SMS or automated voice call.

3. The Device identity , authentication code, and phone number have to be combined into a HTTPS URL to obtain a server-generated password.

3.1.2 User login

The authentication handshake of Whatsapp uses a mechanism called WAUTH-1[16]. After the hello message , it is the XMPP protocol which uses a challenge response authentication mechanism using the user login initiated by the client. The server gives response with the CHALLENGE DATA which is used by the client and generates a PBKDF2 key with the private password which is obtained during one-time registration and SHAI is used as the hash function.

After handshake, when the server authenticates the client, then each message is encrypted. The RC4 key is made up of the first 20 bytes of the PBKDF2 result combined with a hash over the concatenated CHALLENGE DATA, RESPONSE DATA, and the current timestamp.[4]

IV. COMMON VULNERABILITIES IN ALL MESSAGING APPS [10]

4.1 Authentication and Account Hijacking:

Of all the vulnerabilities, most dangerous is the one which allows the attacker to become the master of victim's account. Some applications prompt the user for their phone number and then send a SMS to that number which has an authentication code which the user has to enter . One related vulnerability is of de-registration or deactivation of existing accounts.

4.2 Sender ID Spoofing/Message Manipulation

This vulnerability is about an attacker manipulating or forging messages and sender information but not hijacking the entire account. In this messages are created and sent with a fake (spoofed) sender ID and bypasses user-identification mechanisms inside the application.

4.3 Unrequested SMS/Phone Calls

Most applications use passive SMS-based verification or passive phone calls during sign-up, it is possible to generate unwanted messages or even phone calls to arbitrary phone numbers. Thus combining multiple applications leads to too much of spam. Although , the contents of these messages cannot be modified which makes it difficult for spammers.

4.4 Enumeration

Nearly all applications allow the users to upload their phone book to identify registered users. The server replies with a list of contacts which are registered with the service. In this , if the attacker knows a specific phone number , it can be found out whether the targeted person uses the service. This can be used for attacks such as impersonation or spoofing. Imagine a scenario, where the attacker can upload large amounts of different phone numbers of any particular area and gets an overview of all users in that area.

4.5 Modifying Status Messages

Some applications have functionality to set a status or mood message. This creates a vulnerability which allows the attacker to modify these messages without accessing the affected account.[10]

V. ANALYSIS OF THE PROPOSED ARCHITECTURE

5.1 We list seven basic requirements for a secure and privacy preserving chat service. Taking into account these seven requirements, we have done a comparison between our proposal and commercially available products . The comparison based on the listed requirements is shown in table 1.

Comparison with Existing Chat Applications

Table 1. Comparison with Existing Chat Applications

Criteria	WhatsApp	BlackBerry Messenger	Wickr	Silent Text	Proposed Chat
Req1	-	*	*	*	*
Req2	-	-	(*)	(*)	*
Req3	*	*	*	*	*
Req4	-	-	-	-	*
Req5	-	-	-	-	*
Req6	*	*	*	*	*
Req7	-	*	*	*	*

Note: "*" means that it meets the requirement. "-" stands for either does not support the requirement or information is not publicly available. "(*)" means that the requirement is partially supported.

It can be seen that our proposal meets all the requirements, and that one of the most widely-used mobile chat services, WhatsApp does not support many requirements. However, in support of WhatsApp we can profess that they do not claim to provide a secure , privacy-preserving chat service. Therefore, it does not meet the majority of the requirements.

5.2 Implementation Analysis

The main purpose of the implementation was to provide a risk analysis concept for constructing a privacy-preserving and secure mobile chat application with specifications in open source. Therefore, this endeavor was a study of the technical difficulties which a chat service provider might face in course of development of such a service.

This can be considered as a basic list of requirements. No major technical issues were faced during our development process. In majority of cases, the important components are already present, and there are only reservations about handling a large number of simultaneous connections.

VI. CONCLUSIONS

WhatsApp is one of the most popular messaging applications on smartphones. It is primarily used to exchange Short messages, images or videos. However these messaging apps pose new privacy risks for users.

In this paper we have primarily investigated WhatsApp's feature of sharing presence information . this information can be requested by anybody for any known number. While it is possible to deactivate the \last seen" feature by users, sharing the current online status cannot be deactivated and thus allows continuous monitoring. [4]

There are several privacy risks from presence information. A detailed usage statistics can be created , daily routine can be derived , and even communication partners can be figured out. Socially and economically , this information can be misused.

At present , the one mitigation to this risk is the use of third party apps to prevent WhatsApp from constantly updating the online status . The design architecture needs to implement a better control mechanism to the user to enable fine grained control of presence sharing feature which is implemented in the protocol, There could also be privacy by default setting.[4]

In future research, we would like to experiment with the scalability and reliability of the chat server, to uncover some bottlenecks in building conducting a risk analysis on privacy-based chat server. [11]

REFERENCES

[1] COMP 5135 Individual Literature Review Mobile Security: Risk and Privacy of Using WhatsApp 14123059G Edward, Sze Kin Wah
[2] Empirical assessment of data protection and circumvention tools availability in mobile networks , Cormac Callanan, Borka Jerman-Blažič and Hein Dries-Ziekenheiner. ISBN: 978-0-9853483-7-3 ©2013 SDIWC
[3] http://arstechnica.com/security/2014/02/crypto-weaknesses-in-whatsapp-the-kind-of-stuff-the-nsa-would-love/
[4] Privacy Implications of Presence Sharing in Mobile Messaging Applications, Andreas Buchenscheit,1;3 Bastian Könings,2 Andreas Neubert,3
[5] Social Inference Risk Modeling in Mobile and Social Applications Sara Motahari, Sotirios Ziavras, Mor Naaman, Mohamed Ismail, Quentin Jones. Electrical and Engineering Department, 2Department of Library and Information Science, Information Systems Department2009 International Conference on Computational Science and Engineering978-0-7695-3823-5/09 © 2009 IEEE DOI 10.1109/CSE.2009.237
[6] http://tech.blorge.com/2015/09/18/whatsapp-web-risks-privacy-of-over-200-million-users-know-the-details/15726/
[7] https://www.praetorian.com/
[8] XMPP Foundation. Extensible messaging and presence protocol (xmpp) standard, 2011. http://xmpp.org/, accessed on 22.02.2014.1,3 New Jersey Institute of Technology, 2Rutgers University
[9] What's new with WhatsApp & Co.? Revisiting the Security of Smartphone Messaging Applications , Robin Mueller , , Sebastian Schrittwieser ,Peter Fruehwirt , Peter Kieseberg , Edgar Weippl
[10] End-to-End Secure and Privacy Preserving Mobile Chat Application , Raja Naeem Akram and Ryan K. L. Ko Cyber Security Lab, Department of Computer Science, University of Waikato,
[11] D. Goodin. (2014, February) Crypto Weaknesses in WhatsApp "The Kind of Student the NSA would Love'. Online. ARS Technica. [Online]. Available: http://arstechnica.com/security/2014/02/crypto-weaknesses-in-whatsapp-the-kind-of-stu_-the-nsa-would-love/
[12] (2014, February) The WhatsApp Architecture Facebook Bought for $19 Billion. Online. High Scalability. [Online]. Available: http://highscalability.com/blog/ 2014/2/26/the-whatsapp-architecture-facebook-bought-for-19-billion.html
[13] A. Freier, P. Karlton, and P. Kocher. (2011, August) RFC:6101 - The Secure Sockets Layer (SSL) Protocol Version 3.0. Online. IETF