Analyzing Instant Messaging Applications for Threats : WhatsApp Case Study

Priti Jagwani*

Internet has revolutionized the way we communicate. Email, social media, instant messengers and now mobile messaging are milestones in this trail. This paper has presented details about instant messengers covering their important features, working methodology and safety threats of using them. However, the use of WhatsApp and similar mobile instant messaging apps also poses new privacy risks for users. Further we investigated in detail, security issues of WhatsApp: the most popular instant messaging application available now days. Privacy implications of using WhatsApp and potential keypoints to remain safe while using it are also discussed.

Keywords: WhatsApp, Instant Messaging, Threats.

Introduction

Along with the advancement of social media instant messaging applications are gaining popularity. Now days these messaging services have become integral part of our communication networks. Instant messaging is an online chat application which offers transfer of text on internet in real time. Instant messaging facilitates transmition of messages between two parties bi directionally. After typing the text when a user on either side wants to transmit, he/she selects “send”. Almost all instant messaging in their fancy versions provides voice chat, file transfers, voice over IP and clickable hyperlinks. Depending on the protocol used in instant messaging, the technical architecture can be peer-to-peer (direct point-to-point transmission) or client-server.

Starting from early 1990s with Unix “talk”, instant messaging (IM) applications traveled a glorious path till present scenario of height of popularity. Each and every IM service provides its own client either in the form of a browser based piece of application or in the form of a separately installed piece of software. In recent times third party client software applications exist that will connect with most of the major IM services. Adium, Empathy, Miranda IM, Pidgin, Qnext, Trillian and Facebook Messenger are a few of the common ones. With smart phones becoming an integral part of lives of masses today, many versions of IM for mobiles are in market. These apps allow consumers to send messages from their mobile devices to other mobile devices. Some popular examples of desktop IM are black berry messenger (BBM), skype, pidgin, trillion, facebook messenger, windows live messenger, yahoo messenger etc. Almost all IM which are available for desktop have launched their versions for mobiles. Most used IM for mobiles are watsapp, facebook

*Asstt. Prof., Department of Computer Science, Aryabhatta College, University of Delhi, Delhi (India).

messenger, qqmobile, wechat, skype, viber, line etc. Facebook has discontinued support for its messenger for Windows Desktop client for Facebook Chat. This implies that Facebook no longer offers a desktop instant messaging client of its own. Users can, however, still use third-party applications to connect to Facebook chat from their desktops.

Features

With the beginning of IM in 1980s, these applications have undergone a lot of changes till date. Early instant messaging programs were primarily real-time text, where characters appeared as they were typed. This includes the Unix ”talk” command line program, which was popular in the 1980s and early 1990s. IM capabilities have greatly expended in recent decade. IM chats take place in absolute real time. This real time flavor is differentiating IM communications from emails. Some systems permit messages to be sent to users not then ‘logged on’ (offline messages), thus removing some differences between IM and email (often done by sending the message to the associated email account). One line of difference between email and IM is immediate receipt of acknowledgement. Emails are lacking in this feature. Instant messaging applications are adding more and more features which make them even more popular like users may see each other via webcams, or talk directly for free over the Internet using a microphone and headphones or loudspeakers, chat in a group, share multimedia files, voice calls over internet etc. A persistent quality of emails is also provided in some IM applications where a user can store chats for later references.

Working Methodology

When a client of IM service (IM application) is installed on a machine and user open the client, it tries to establish a connection to the server using a proprietary protocol fixed for communication. After getting connection to the server login credentials are being asked for. Post verification of login credentials, user is logged in. Information about connection like IP address and port number etc are sent to the server. The server creates a temporary file that has the connection information for user and list of contacts. It then checks to see if any of the users in the contact list are currently logged in. If anyone among the contact list is logged in, a message is sent back to the client and the people online in the contact list also get an indication about user’s logged in (online) status. Also user’s contact list shows the person as online. Now user can communicate with the person online. Now onwards all communication takes place between the two clients; here onwards server is not involved in communication. The other person gets user’s instant message and responds. The window that each of the communicating persons sees on their respective computers/mobiles expands to include a scrolling dialog of the conversation. Each person’s instant messages appear in this window on both devices. When the conversation is complete, the message window has been closed which eventually means, user is going offline and exits. When this happens, the client sends a message to the server to terminate the session. The server sends a message to the client of each person on user’s contact list who is currently online to indicate that user has logged off. Finally, the server deletes the temporary file that contained the connection information. In the client application of user’s contacts that are online, user moves to the offline status section.

The major IM utilities use a proprietary protocol that is not understood by other instant messaging services, so users of one service are usually blocked from contacting members of another. But recently some sophisticated IMs are also introduced in market like Trillian and Pidgin, which allow users to IM on several services at once.

Safety Threats of Instant Messaging Apps - Case Study : WatsApp

All of the lucrative features provided by the IM are only one side of the coin. On the other side there are vulnerabilities associated with IM technology. These vulnerabilities have created several security issues. Instant messaging is not considered a secure way to communicate. All of the messages and connection information are maintained on servers. This whole lot of information is controlled by the provider of IM utility. IM connections and messaging usually occur in plain text, making them vulnerable to eavesdropping. Also, IM client software often requires the user to expose open UDP ports. This gives rise to the threat posed by potential security vulnerabilities. There are also some "obvious" features of IMs that are threats to security like presence and status broadcasting, interoperability with others, maintaining a lists of all desired contacts, use of third party servers to provide chat functionality to messenger clients and keeping a log of messages and other events/ activities.

Now days most utilities do provide a certain level of encryption, but even though they are not secure enough to send any confidential information through the system. There have been reported cases of IM user logs being captured and used by nefarious sorts, and hackers have been known to instant-message virus-infected files. Voice over Internet (VoIP) is thought to be more vulnerable to infiltration than text-based instant-messaging.

WatsApp Inc. was founded in 2009 by Brian Acton and Jan Koum. WatsApp Messenger is a proprietary cross platform instant messaging client for smart phones that operates under a subscription business model. WatsApp has acquired instant messaging market by serving itself as a free alternative to SMS text messaging. It uses internet to send text messages, images, video, user location and audio media messages to other users using standard mobiles. It is becoming the most popular IM service for cell phones. According to a study WatsApp had a user base of 900 million in September 2015. WatsApp Inc., based in Mountain View, California, was acquired by Facebook Inc. on February 19, 2014, for approximately 16 billion USD.

Initially WatsApp communications were not encrypted. All the messages are sent and received in plain text. Also accounts are open for session hijacking and packet analysis. Communication in plain text makes the logs vulnerable if packet traces are available. This was reported in May 2011 and fixed in September 2011 with a new version release of messenger application for cellphones in which message encryption was facilitated but in May 2015 researchers have noticed that although the messages sent on WatsApp are in encrypted form but the encryption itself is breakable. But for an end user it is difficult to tell the difference between plain text messages and encrypted messages.

2012 was actually a year of WatsApp being in the news for all the bad reasons (security breaches). In January 2012 a website was published which made it possible to change the status of an arbitrary

WatsApp user, as long as the phone number was known. Later in September hijacking of any WatsApp account was demonstrated.

In November 2014, WatsApp had a partenership with Open Whisper Systems. The idea behind this partenership was to have an end to end encryption by incorporating the encryption protocol which was used in the TextSecure application of Open Whisper Systems. It was make sure by Open Whisper Systems that they have incorporated the protocol into the latest WhatsApp client for Android and that support for other clients, group/media messages, and key verification would be coming soon. But there was no announcement or documentation about the encryption feature on the official website, and further requests for comment were declined.

In December 2014, a critical vulnerability was disclosed which allows anyone to remotely crash WhatsApp just by sending a specially crafted message of 2kb in size. To escape the problem, the user who receives the specially crafted message has to delete his/her whole conversation and start a fresh chat.

WhatsApp has a built-in (un)secure method to store all messages and conversations in encrypted files. WhatsApp stores all the data in multiple files named msgstore.db, and msgstore.db.crypt8 respectively. A third-party application is available online, which can easily open the encrypted database and edit the contents inside it. The only requirement for the app to work is a rooted Android smartphone.

To target an individual, all an attacker needs is the phone number associated with their account. By sending a seemingly innocent 'vCard' contact card containing malicious code, and persuading the victim to open it, they can launch an executable file and begin downloading malware onto their PC. WhatsApp has verified and acknowledged the security issue and has developed a fix for web clients worldwide, which started rolling out on August 27. All versions of WhatsApp Web after v0.1.4481 contain the fix for the vulnerability.

Every now and then various commissions of different countries advised their people against use of WatsApp. In 2013 the Saudi Arabian Communications and Information Technology Commission (CITC), in February 2014, the public authority for data privacy of the German state of **Schleswig-Holstein** and on December 17, 2015, mobile providers in Brazil were ordered to block WhatsApp for 48 hours.

In January, 2015, WhatsApp launched a web client which can be used from the browser. This desktop version of WatsApp is known as WatsApp Web. Initially it has become a hub of security flaws. It had two major security issues that compromised user privacy: the WhatsApp Photo Privacy Bug and the WhatsApp Web Photo Sync Bug. User can get attacked by Web malware which are malicious links looking like the original link of WatsApp which is available for download.

WatsApp Spy Public is an App available online which can bypass privacy settings of any WatsApp account. Using this one can monitor status messages, status changes, and user photos, as well as adjust security settings, even if the app's owner has set the privacy options to "nobody".

There are certain features in WatsApp which are proving to be security holes like any stranger can retrieve events of a users last seen and online/offline status in WhatsApp and secondly, there are certain privacy options in WatsApp which are misleading and provide no option to disable online/ offline status.

As of December 1, 2015, WhatsApp has a score of 2 out of 7 points on the Electronic Frontier Foundation's secure messaging scorecard. It has received points for having communications encrypted in transit and having completed an independent security audit. It is missing points because communications are not encrypted with a key the provider doesn't have access to, users can't verify contacts' identities, past messages are not secure if the encryption keys are stolen, the code is not open to independent review, and the security design is not properly documented [8].

What can be done

One of the best WhatsApp security tips is to protect the app with a password or PIN. This can be done with the help of third-party apps as WatsApp doesnot provide such a feature. Others are blocking WhatsApp photos from appearing in photoroll, hiding 'last seen' timestamp, restricting access to profile picture, deactivate WhatsApp if user losses the phone and last but not the least being careful what a user is talking about. Users should always remember to log out of WhatsApp Web. Most users are unware that they should ideally log out of WhatsApp Web for security reasons. WatsApp Inc. should replace the "last seen" privacy option with an "online/offline status" only and set all privacy options by default to "nobody" and notify users about the consequence of setting these options to "contacts" or "everyone".

Conclusion

The future of instant messaging is very bright. IM has completely changed the world of communication. IM are becoming richer in their services and capabilities. But along with providing technology and convenience on finger tips of users, IM also open security vulnerabilities. In this paper case study of WatsApp has been presented considering all of its security aspects and weaknesses. Finally a brief description of possible solutions is also submitted which can lead to a safer user experience.

References

1. Buchenscheit, Andreas, et al. "Privacy implications of presence sharing in mobile messaging applications." *Proceedings of the 13th International Conference on Mobile and Ubiquitous Multimedia*. ACM, 2014.
2. https://en.wikipedia.org/wiki/Instant_messaging
3. https://www.whatsapp.com/
4. https://en.wikipedia.org/wiki/WhatsApp
5. http://indianexpress.com/article/technology/social/whatsapp-tips-8-ways-to-secure-your-personal-chats/

6. http://www.express.co.uk/life-style/science-technology/603846/WhatsApp-Security-Flaw-Web-Users-Risk-Malware-Hack

7. www.makeuseof.com/tag/4-security-threats-whatsapp-users-need-know

8. https://www.eff.org/secure-messaging-scorecard