Is our privacy being compromised as we speak? Eavesdropper's heaven or a nightmare? A study of Mobile Voice over Internet Protocol (mVoIP) and Instant Messaging (IM) Applications.

Farhan Ahmed Siddiqui
Department of Computer Science, University of Karachi
Karachi, Pakistan

Muhammad Ahsan Najam
Department of Computer Science, University of Karachi
Karachi, Pakistan

Muhammad Saeed
Department of Computer Science, University of Karachi
Karachi, Pakistan

Nasir Touheed
Department of Computer Science, IBA Karachi
Pakistan

Abstract
In the recent times, mobile voice over internet protocol (mVoIP) applications have been greatly adopted by the masses and have really captured much of the attention in the application market place. These applications not only provide voice communication with little to no cost but also offer instant messaging service. People across the world use applications like this and some even communicate daily with others just by using these applications rather than the conventional way of text messages and GSM calls. With applications consolidating millions and millions of users, security and privacy is a topic which many prefer not to discuss. In this paper we delve into the details of this sensitive issue and discuss whether or not these applications are even safe to use. Whether our communications are secure and kept private from eavesdroppers and in more technical terms, whether these applications have any sort of an encryption mechanism in place and if that mechanism is even strong enough.

Key words:
mVoip, internet protocol, instant messaging

1. Introduction

Within the last few years, mVoIP and IM applications have taken the world by storm. People have for the longest time wanted the whole world at their fingertips. Now what once was a dream and a fantasy is a reality. With the advent of applications like WhatsApp, OoVoo, Viber, Mo+ etc. people can communicate with anyone across the globe. People can not only instant message anyone else irrespective of their location but can now call them. All and all doing so with no charges at all. The applications use your internet service whether it is your Wi-Fi, 3G or 4G service and makes the communication possible. Although all of this would seem to be perfect, there is a topic of great interest which is not examined properly in this realm and which would be of great interest. As they say, with great powers, comes great responsibility, these applications and the companies which own them have a lot to be answerable for. Security and privacy are two main issues which revolve around these applications, these two key areas are not at all explored and there are only a handful of studies if at all which examine aspect of these so called "perfect applications". Majority of the people who use these applications aren't even aware of the fact that anyone can basically intercept their communication and if the communication is not encrypted, can easily read and misuse their information. Other than this, is the communication encrypted at the servers or is the privacy of the user in the hands of the developers of these applications? Some of the people do not even care about this fact but to some this is of great concern. This paper aims to solve this problem and provide somewhat of a statement as to which applications in this day and age are the most secure, which applications provide the best form of privacy, which applications encrypted your communications the strongest and how do they go by doing this, which applications you should use and should not. We selected various applications and labeled them "famous" based on the "millions of users" who have downloaded the application and make up the user base of that particular application. In the next section we describe the experiment which we used to analyze these applications, what we did, what we hoped to achieve and what we got in the end. After which the subsequent sections would deal with the applications on an individual basis, one application after the other, what we found out about the instant messaging bit of the application, what we found out about the voice call bit and just an overall assessment of how well the application is secured. After we have presented all of the relevant information about these applications and have given a concrete comparison of the applications both region wise and generally, we would go on to conclude it with what we think is the best application in terms of security and privacy, finally would end the paper by providing a future work recommendation portion and explain what more can be done in this realm.

Manuscript received October 5, 2017
Manuscript revised October 20, 2017

2. The Experiment:

The experiment which we conducted was simple enough, we simply intercepted all of the communication which were going on via the applications one by one. The data in the form of packets of each corresponding application was captured in this way and then those packets were further analyzed and dissected. An Apple device was used in this experiment which was used to send and receive both messages and calls. The intercepting device which was a laptop was used to intercept and capture all of the packet data and was used in the whole analysis phase.

3. The Findings:

3.1 OoVoo:

The first and probably the most interesting application to discuss is ooVoo. Developed by ooVoo LLC and released in the year 2007, ooVoo is available across all major platforms such as Android, Windows Phone, iOS etc. Their official website boats about consolidating about 150 million users with thousands registering each and every day. With such a broad spectrum, this application was a prime target to further dig in and analyze.

3.1.1 Text Analysis:

The application was installed and opened up two different devices, the one under the microscope as mentioned was an iPhone 6S, a few messages were sent to and fro across the devices after which the packet data went into analysis phase in WireShark. When we sifted through the packets, we found out that there was no encryption in place whatsoever. The communication was basically in plaintext, one could not only read the user's ID but could also read the messages and the entire communication was open. The following figure i.e. Figure 1 of a packet solidifies this declaration.
In Figure 1, one could clearly see that nothing is encrypted, the <body> tags contain the body of the message which you just sent, and tags like <message from> and <item to> identify the user's ID. All of this sensitive information is in plaintext for anyone to read and misuse if he/she so pleases. This was probably the most shocking finding of the study.

Figure 1 - ooVoo IM Packet

3.2 WhatsApp:

By far the most popular messaging application there is WhatsApp, formerly made by two employees of Yahoo! Brian Acton and Jan Koum and now owned by Facebook incorporates about 1 billion users and counting, with new users registering each and every day. As with any application these days, WhatsApp is available across all major platforms which include Android, iOS and Windows Phone to name a few. This is an interesting application to evaluate because it recently added end-to-end encryption to its arsenal which is the cornerstone of security and privacy in the realm of any application which involves communication amongst varies parties. It claims to be extremely secure and that not even WhatsApp itself can read our messages and listen to our calls. With a user base of over a billion that should have been the case. We put this theory to the test.

3.2.1 Text Analysis:

WhatsApp delivers what it promises, it encrypts all of the text messages by using end-to-end encryption. Which in lay man terms mean that the messages go under an encryption involving 256 bits, thereby even if someone who is not authorized is snooping around and is intercepting messages, would not be able to retrieve any of the sensitive information and it would take him/her months or even years to decrypt a single sentence. WhatsApp uses an encryption method called the Elliptic curve Diffie-Hellman (ECDH) by which even WhatsApp cannot even access the information as only the two parties who are communicating with each other consolidate to the public key with their respective private keys and only they can read each other's messages. No "plaintext" was found in the packets of WhatsApp both sent and received, confirming the fact that it is indeed encrypted. The handshaking packet revealed the fact that it uses ECDH method to incorporate the encryption.

3.3 Free Calls & Text by Mo+:

Probably the more un-familiar application of the lot but still a viable application to dig into is the application by MoPlus Inc. Although the application is not as famous as WhatsApp and Viber, it is present in both the Google Play Store and Apple's AppStore. With over 5 million downloads on the Play Store and about the same figure on the AppStore, this application is no slouch when it comes to gaining attention from the users. The application was last updated in January so one has to imagine it contains the basic encryption mechanism even if it does not incorporate end-to-end encryption. The application promises to deliver crystal clear voice call, fast and reliable text messages amongst the communicating parties as well. The application seemed somewhat of a "dark" horse and so was selected to undergo the experiment.

3.3.1 Text Analysis:

As the application was updated in the same year i.e. 2016, one would think that it has all the basics covered of what an mVoIP and IM application should be like in terms of security and privacy. The following screenshot is a real eye-opener to say the least. Basically, anything and everything could be seen in "plaintext", from the sender's number to the receiver's number and of course the most crucial part, the message body too.
Everything is in "plaintext" just like ooVoo, the only difference lies in the fact that ooVoo transfers information by using the user's ID rather than their phone numbers whereas Mo+ uses the phone numbers so a sensitive information like a phone number is even up for grabs to anyone who can intercept the communication going on via this application. All of this can be clearly seen from Figure 2, i.e. a packet which was analyzed in WireShark.

3.4 Viber:

Viber is also one of the most famous mVoIP and instant messaging application on the market as of now. Other than WhatsApp which is the most famous and widely used, Viber can be thought of as a close second to that of WhatsApp in terms of fame and user acceptance.

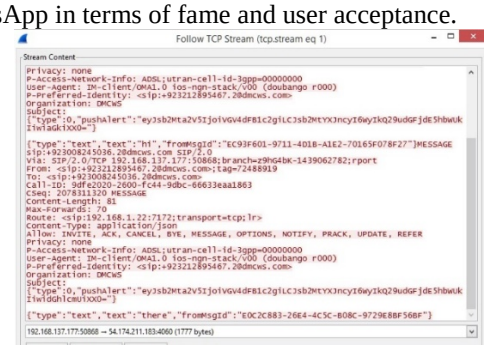

Figure 2 - Mo+ IM Packet

With about 100 million active users and 280 million registered users, Viber has also grasped a lot of attention in the domain of a reliable mVoIP and IM application. Developed by Rakuten Inc. and available across all major platforms such as BlackBerry OS, Android and iOS. Viber as of now claims that it provides end-to-end encryption, the same as that of WhatsApp in which even Viber itself cannot read the messages of its users.

3.4.1 Text Analysis:

Just like WhatsApp, Viber uses the elliptic curve Diffie-Hellman method of encryption, thereby making it impossible for anyone to decrypt. It uses the same concept of 256 bit encryption keys where 256-Curve 25519 key pairs are used to establish a secure connection among the communicating parties. The public part of their keys is saved on the server while the private part is exclusive to the device which is the basic concept of why no one can read the messages as they have no way of finding out the private key and decrypt the messages. Brute forcing a 256 bit key would take days, weeks or even months and is totally impractical. No sign of "plaintext" was found in the packets of Viber and both WhatsApp and Viber stand on equal footing of encrypting the text messages with both applications using the same encryption technique and method.

4. Comparison of the Applications:

Table 1 makes everything easy to understand at a glance:

Table 1 - General Comparison

Application	Text			Call Encryption	Protocol used for Call
	In Transit	On Server	E2E		
WhatsApp	Yes	Yes	Yes	Yes	UDP
Viber	Yes	Yes	Yes	Yes	UDP
OoVoo	No	No	No	Yes	UDP
Free Calls & Text By Mo+	No	No	No	Yes	Dynamic RTP, Type 111

As it can be clearly seen, ooVoo and Mo+ offer no encryption whatsoever with respect to the text messages. ooVoo like WhatsApp and Viber uses UDP packets for the audio call which is not easily decoded whereas Mo+ uses a dynamic RTP payload which is also difficult to decode but is somewhat easier than just UDP packets.

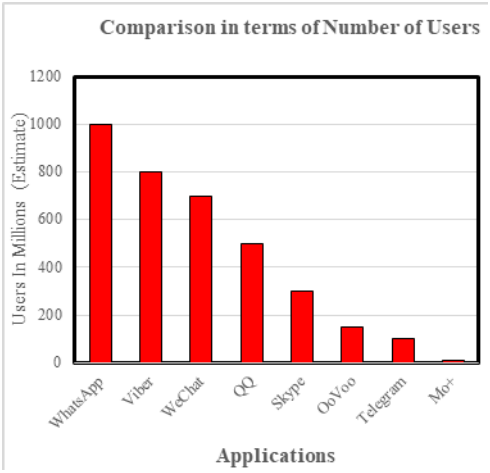

Figure 3 - Comparison Chart In Terms of Users

Another comparison can be made based on the number of users who actually use the applications day in and day out and those who downloaded the applications thinking they might be able to communicate with their loved ones keeping their privacy intact. Figure 3 depicts the number of users these applications consolidate.

4.1 Region Based Comparison:

Certain regions are facing war on terror in which communication and information is the key to not only people living in the region but to people who can prevent and exaggerate the situations. Some regions on the other hand want to promote their own creation and have blocked access to other applications and services, the important part here is that people's privacy is at stake in both the cases. Table 2 breaks down the regions facing war on terror, what applications they use the most and just some mVoIP and IM applications user intensive regions as a whole

Table 2 - Region Based Comparison

Country	Most Used App	Text			Call	
		In Transit	On Server	E2E	Allowed	Encryption
Iran	Telegram	Yes	No	No (optional)	No	-
Iraq	Viber	Yes	Yes	Yes	Yes	Yes
Syria	WhatsApp	Yes	Yes	Yes	Yes	Yes
Afghanistan	Facebook Messenger	Yes	No	No	Yes	Yes
China	QQ and WeChat	Yes	No	No (optional)	Yes	Yes

The most notable amongst these countries are Iran, Afghanistan and China. Iraq and Syria, as they use Viber and WhatsApp respectively the most, are safe in the sense that their privacy is not at stake. These applications are both end-to-end encrypted which entities that not even Viber and WhatsApp can access the messages being conveyed.

Now if we talk about Iran, it uses Telegram which is a fairly new application but it gained popularity as it claimed it also offered end-to-end encryption, there was a fine print though, this feature can only be turned on if both parties activate a "secret" feature in the app, other than this the application does not even have a voice calling feature to begin with. So all in all it falls short in comparison to Viber and WhatsApp.

Over 80% users in Afghanistan on the other hand constitute Facebook messenger's user-base in the region, little do they know that Facebook messenger is not end-to-end encrypted and the data and communication can easily be retrieved, the information is in plaintext at the servers and the communication is simply encrypted in transit which is not all that promising and in the sense of privacy, well to foreign powers that may be, the user's in Afghanistan does not have privacy in the true sense, their communications and sensitive information can be handed over and can be used against them if the foreign powers see fit.

The most unique country is China, having a history of banning various applications and websites in the name of internet censorship, over 600 million of users in China use QQ and WeChat combined with over 500 million and over 700 million users respectively between the two applications with the majority of the users being from China. Both applications are even developed by the same developer known as "Tencent Holdings Limited". Both of the applications QQ and WeChat encrypt messages in transit with QQ just recently introducing this feature in the year 2016. Contrarily, QQ does not offer its users the option to start a "secret" conversation like Telegram and its counterpart WeChat which is supposedly meant to end-to-end encrypt the communication. Both of the applications in their default state are not end-to-end encrypted thereby solidifying the claim that over 1 billion users and their privacy is under jeopardy. The communication and information can easily be retrieved from the servers if needed and again privacy in true sense is just a catchphrase when it comes to these two applications too.

5. Conclusion:

The experiment and careful evaluation makes things clear that there are all sorts of applications out there in the Google Play Store or Apple's AppStore etc. and that a normal user can get influenced by the fake marketing and fancy graphics of a few of these applications but little do they know that their entire information and privacy is at stake. While there are some extremely secure applications such as WhatsApp

and Viber, there are applications like ooVoo, Telegram, QQ, Facebook Messenger and Mo+ as well which have a huge user base but are not secure and do not exactly provide full privacy which they should. People need to familiarize themselves with the term “end-to-end encryption” and what it brings to the table, people need to adopt only those applications which promise to incorporate just that. Some regions have blocked various applications for this sole purpose as their own government and higher in power countries want to get as much information as they can from the countries which are either facing war on terror or is looked upon as a region filled with various issues. Some countries like China on the other hand want to impose their own framework and hence promote their own applications over which they have full control over, the communication on the servers is open and privacy in true sense is nowhere to be found. In this day and age, privacy and security are of the utmost concern to the user whereas solid and raw data is essential for the companies and superpower countries. Some companies may appear to cater to the users but when majority of these applications are free, you can bet that there is some hidden agenda behind these applications too. Data is valuable not only for these companies but for intelligence agencies as well. As they say, there is a lot more than what meets the eye. Mobile VoIP and IM applications are an essential part of nearly everyone’s life these days where people share their day to day experiences and sensitive information to others and it is up to the users to choose their medium. Now is the time to drop the careless attitude and really dig into these applications and what actually goes on behind the scenes because none of us want our privacy to be invaded, not by hackers and certainly not by the companies who promise to keep our information secure. Applications like WhatsApp, Viber depict what mVoIP and IM messaging applications should be like but applications like ooVoo and Mo+ depict the dark side of these applications. Now is the time to become self-aware and never settle for anything less than the best.

6. Future Work Recommendation:

As with anything in the technology and the science realm, things evolve. Nothing remains constant, these applications and the standards of security will not remain the same. The applications can even be replaced by new applications. As a future work, one should test out some different applications and some platforms altogether. With the passage of time, it is highly possible that what seems to be the pinnacle of security i.e. ECDH now would be a thing of the past, it is also possible that what seems to be impossible to decrypt now would be extreme easy to decrypt in the future. So the study cannot be a one size fits all, it is based on the present time comprising of only 5 applications in a world of millions of applications. There is a lot more that can be done in this realm as it is a topic which is either not greatly talked about or explored in much detail.

References

[1] o. LLC, "Video Chat | ooVoo," [Online]. Available: http://www.oovoo.com/.
[2] A. Jozi, "Techrasa," 13 May 2016. [Online]. Available: http://techrasa.com/2016/05/13/messaging-apps-used-middle-east/.
[3] J. Schwartz, "Digital Vision brought to you by SimilarWeb," 24 May 2016. [Online]. Available: https://www.similarweb.com/blog/worldwide-messaging-apps.
[4] "Mo+," [Online]. Available: http://mopl.us/.
[5] "Viber | Wikipedia, the free encyclopedia," [Online]. Available: https://en.wikipedia.org/wiki/Viber.
[6] "WhatsApp | Wikipedia, the free encyclopedia," [Online]. Available: https://en.wikipedia.org/wiki/WhatsApp.
[7] "ooVoo | Wikipedia, the free encyclopedia," [Online]. Available: https://en.wikipedia.org/wiki/OoVoo.
[8] WhatsApp, "WhatsApp Security," [Online]. Available: https://www.whatsapp.com/security/.
[9] Viber, "Viber Security Overview," [Online]. Available: https://www.viber.com/en/security-overview.
[10] A. Azfar, K.-K. W. Raymond Choo and L. Liu, "A study of ten popular Android mobile VoIP applications:," 2014 47th Hawaii International Conference on System Science, 2014.