Network Security Performance Analysis of Mobile Voice Over Ip Application (mVoIP): Kakao Talk, WhatsApp, Telegram and Facebook Messenger

Nur Khairani Kamarudin[1]*, Nur Syafiqa Bismi[2], Nurul Hidayah Ahmad Zukri[3], Mohd Faris Mohd Fuzi[4], Rashidah Ramle[5]
Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA, Perlis Branch, Arau, Campus, 02600 Arau, Perlis, Malaysia

*Corresponding author: *nurkhairani@uitm.edu.my*
Received Date: 18 August 2020
Accepted Date: 10 October 2020

ABSTRACT

VoIP application usage has increased from time to time and makes our daily life more convenient. VoIP application has features to make a phone call, send a text message and share the file through the apps for free. However, most of the users did not seem aware of VoIP security features such as authentication ability, password encryption ability, or voice or audio and text communication encryption ability. It is essential to ensure the VoIP used is secure from password decrypter and eavesdrops the user conversation. Thus, the first objective of this research was to study and investigate VoIP application consist of Kakao Talk, Telegram, Facebook Messenger and WhatsApp for both Android and web application. The second objective was to evaluate the four VoIP application identified based on authentication requirement, password encryption, voice or audio encryption communication, and text encryption communication. There were two mobile phones used. One acts as a client and a personal computer act as an attacker. Wireshark and packet capture were run in personal computer and mobile phone to monitoring and scanning the network traffic while both devices connected in the same WLAN. The experiment implements MITM, interception, and sniffing attacks. This research project has identified Facebook Messenger and WhatsApp web application do not provide secure password ability.

Keywords: *VoIP application, authentication, password, encryption*

INTRODUCTION

Voice over internet protocol (VoIP) is a software that allows the user to send text and have a voice calls over the internet protocol (IP). Mobile VoIP applications (mVoIP) become popular among the user since this application provides voice and video communication that is free or very low-cost calls (Azfar, Choo, & Liu, 2014). VoIP application could be on any data network that uses IP, like internet, intranet and local area network (LAN). mVoIP applications have gained attention from mobile device users such as Android devices. The example of widely used mVoIP application is WhatsApp, Kakao talk, telegram and Facebook messenger.

Besides, there are a few things user need to see on the criteria for a secure mobile application. Such as the authentication level of mobile applications, network performance, and encrypted communication. This will become an issue on the security of mVoIP when there are various ways to intercept VoIP communication (Azfar, Choo, & Liu, 2014). For example, interception. It can take place at the client devices when the conversation is being initiated or during the established communication session. So, it is essential to analyze the intercepted communication to determine whether the communication is encrypted or not.

The aims for this research project are to study and investigate VoIP application consist of Kakao Talk, Telegram, Facebook Messenger and WhatsApp for both Android and web application. Next, to evaluate the four VoIP application identified based on authentication requirement, password encryption, voice or audio encryption communication, and text encryption communication: Kakao Talk, WhatsApp, telegram and Facebook messenger.

This rest of this paper is structured as follows: Next section talks about the design and development process, followed by experimentation section explains the method on evaluating VoIP application. Next section is results and discussion and lastly, concluding remarks are presented in section conclusion and recommendation.

DESIGN AND DEVELOPMENT

This section discuss on the process involved in designing and developing the testbed architecture. As shown in Figure 1, two mobile phones were used which act as client A and client B. One personal computer was used as an attacker. Wireshark and packet capture were run in personal computer and mobile phone to monitoring and scanning the network traffic while both devices connected in the same WLAN. The VoIP applications identified were installed at both clients (Client A and Client B) and Wireshark was installed at the attacker laptop while network analyzer was installed at one of client phone.

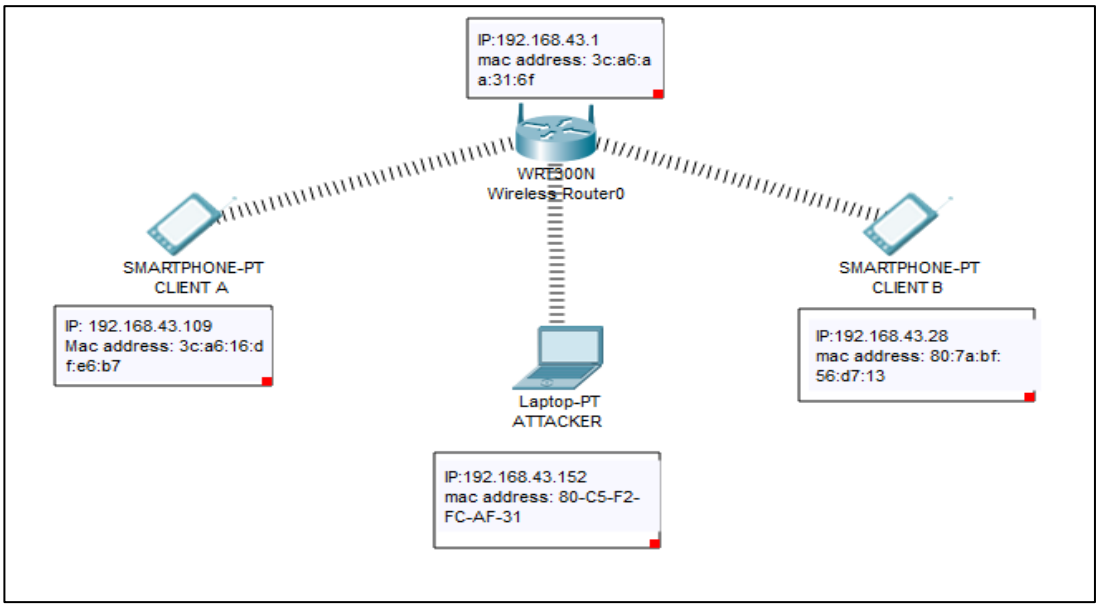

Figure 1 Testbed architecture

EXPERIMENTATION

After a pilot study was conducted to make sure all the hardware and software installed as in the testbed is running properly, four experiments have been conducted using four different VoIP application identified (Kakao Talk, Facebook Messenger, Telegram and Whatsapp). For each experiment, the steps involved are described in detail in Table 1. The test criteria tested on experimentation phase are as below.

Table 1: Experimentation

EXPERIMENT	ITEM	DESCRIPTION
1	Kakao talk	Conducted one experiment at a time. For each test, the steps involved were: 1. Installed the VoIP application on both client devices and installed Wireshark on attacker laptop. 2. Started the experiment using one VoIP application installed at a time. 3. The client A, B and attacker has been connected to one access point and established the connection. The VoIP application has been evaluated on the following criteria: ● Authentication ● password encryption ● text communication encryption ● voice/audio communication encryption 4. Repeat steps 2 to 3 using other VoIP application identified during the information-gathering phase. Client A established a connection with client B. The attacker will run Wireshark for website application and Packet Capture for android application. 5. Repeat the testing of VoIP application with the test criteria.
2	Facebook messenger	
3	Telegram	
4	WhatsApp	

RESULTS AND DISCUSSION

The analysis and discussion is based on the observation while running the experiment involving four VoIP application which is Kakao talk, telegram, WhatsApp and messenger. The VoIP applications were tested based on four criteria, which is authentication requirement, password encryption, voice or audio communication encryption and text communication encryption.

Experimental Results

This research project has identified some differences between all VoIP applications tested. It was observed that WhatsApp, telegram, Facebook messenger and Kakao talk have many things in common either a website or android application, which include authentication, password encryption, voice/audio communication encryption and text communication encryption, and all the data collected is summarized in Table 2.

Table 2 Experimental Results

VoIP APPLICATION		NETWORK SECURITY PERFORMANCE			
		Required authentication? (yes/no)	Encrypted password? (yes/no)	Encrypted voice/audio communication? (yes/no)	Encrypted text communication? (yes/no)
Kakao Talk	Web	Yes	Yes	Yes	Yes
	Android	Yes	Yes	Yes	Yes
Telegram	Web	Yes	Yes	Yes	Yes
	Android	Yes	Yes	Yes	Yes
Facebook Messenger	Web	Yes	Yes	Yes	Yes
	Android	Yes	No	Yes	Yes
WhatsApp	Web	Yes	No	Yes	Yes
	Android	Yes	Yes	Yes	Yes

Table 2 shows the captured session for Kakao Talk and Telegram in android and web version, provide encrypted password and encrypted or secure communication, no plain text password or message was visible from the captured session for Kakao Talk and Telegram conversation packets.

Facebook messenger for android version and WhatsApp web do not provide password encryption ability since the user password can be read easily. The captured session from Packet Capture application for Facebook Messenger does show the password in plain text as shown in Figure 2. WhatsApp web was not offered password encryption to the user since but it used QR code utility for user to log in the applications. It is found that, QR code can be manipulated by the attacker using QRL Jacker. With QRL Jacker, the attacker can access user WhatsApp Android data.

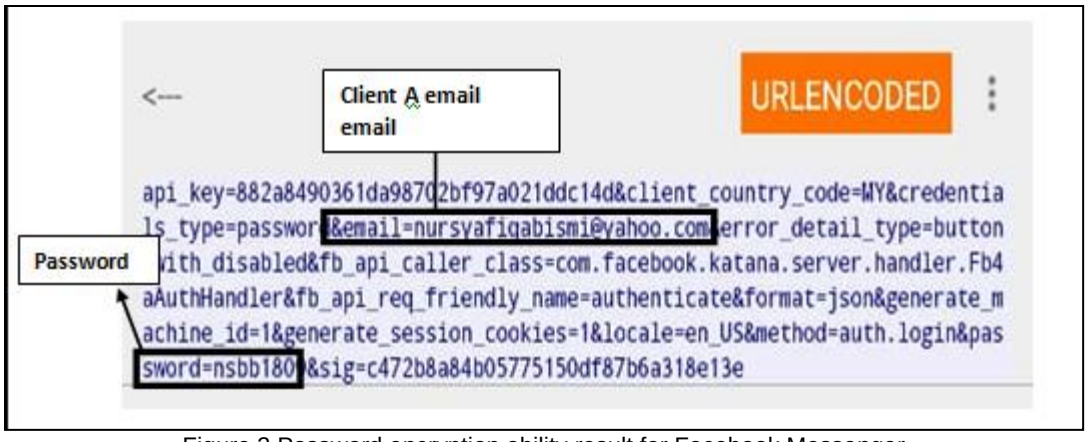

Figure 2 Password encryption ability result for Facebook Messenger

Discussion

This subtopic discusses in which situations that VoIP application tested are suitable to implement.

Authentication requirement

Authentication is a process to ensure a user's identity. User needs to enter username and password before they can log in to their account. In this research project, authentication is to ensure only the right user can log in to the account.

Based on the experimental result, all four android application such as Kakao talk, telegram, Facebook messenger and WhatsApp has authentication ability which is to identify the right use of the account. Kakao talk and Facebook messenger provide email or phone number and password utility to authenticate the user.

All four application for android and website was proven it had provided authentication ability since authentication is the first layer security for applications. Authentication can be verified by email, username, phone number, password and verification code.

Password encryption

Encryption is the conversion of plain text into ciphertext, which cannot easily understand by unauthorized people. In this research project, encryption ability was evaluated based on the password provided by each VoIP application tested. It is important to have an encryption connection to ensure the security of the confidential password. Thus, a strong password is needed to avoid the third party to guess the password, which can be harmful to the user.

Kakao talk and telegram applications, have provided password-encryption ability because Kakao talk application required a combination of 8-23 upper or lower case letters, numbers and special characters to strengthen the password. These criteria were tested using Wireshark and Packet Capture by observing the packet captured while signing to the VoIP.

However, Facebook Messenger and WhatsApp web do not provide password encryption ability since the user password can be read easily. Based on Figure 2, Facebook Messenger password can be read easily when the attacker run Packet Capture tool in the background.
On the other hand, WhatsApp web were using QR code to enable user opened their account. From the findings, the WhatsApp web was not offered password encryption to the user since the QR code can be manipulated by the attacker. By using QRL Jacker, the attacker can obtain the user Whatsapp data in mobile.

Voice or audio communication encryption

Encryption is the conversion of plain text into ciphertext, which cannot easily understand by unauthorized people. In this research project, encryption ability was evaluated based on voice or audio communication for each VoIP application. It is important to have an encryption connection to ensure the security and integrity of data, especially while exchanging confidential data through voice or audio medium.

Voice or audio communication was tested using Wireshark for website application and Packet Capture for android application. As a result, all application has encrypted communication since the pcap file contains cipher data which cannot decrypt by using online decrypt tools.

Text communication encryption

Encryption is the conversion of data into ciphertext, which cannot easily understand by unauthorized people. In this research project, encryption ability was evaluated based on text communication for each VoIP application. It is important to have an encryption connection to ensure the security and integrity of data transfer, especially while exchanging confidential data through text.

Text communication was tested using Wireshark for website application and Packet Capture for android application. Wireshark result for text communication was encrypted since the pcap file contains cipher data which cannot decrypt by using online decrypt tools. All text exchanged between client A and client B is encrypted, since all four application offer TLS protocol to encrypt their communication.

CONCLUSION AND RECOMMENDATION

From the data collected and observation on experiments, most of the VoIP applications tested have met the requirement in the criteria tested. But the Facebook messenger and WhatsApp web application failed to meet the requirement of the criteria. This is because there are many free software tools to intercept user communication, which available on the internet. As a result, this research has fulfilled the research objective to investigate various VoIP applications such as Kakao Talk, WhatsApp, Telegram and Facebook messenger and evaluate the network security performance of four popular VoIP applications based on authentication, password encryption, and encrypted communication. It can be concluded; this research project can be a guideline for another researcher for depth understanding for an unauthorized interception in VoIP applications. Future work includes decoding the captured unencrypted sessions and analyzing more VoIP applications.

REFERENCES

Azfar, A., Choo, K. K. R., & Liu, L. (2014). A study of ten popular Android mobile VoIP applications: Are the communications encrypted? *Proceedings of the Annual Hawaii International Conference on System Sciences*, 4858–4867. https://doi.org/10.1109/HICSS.2014.596

Babkin, S., & Epishkina, A. (2019). *Authentication Protocols Based on One-Time Passwords*. 1794–1798.

Carvajal, L., Chen, L., Varol, C., & Rawat, D. (2016). Detecting unprotected SIP-based Voice over IP traffic. 4th International Symposium on Digital Forensics and Security, ISDFS 2016 - Proceeding, 44–48. https://doi.org/10.1109/ISDFS.2016.7473515

Chakraborty, T., Misra, I. S., & Prasad, R. (2019). VoIP Protocol Fundamentals. 25–47. https://doi.org/10.1007/978-3-319-95594-0_2

Rohini, S., & Bairagi, V. (2010). Lossless Medical Image Security. International Journal of Applied Engineering Research, 1(3), 536–541.

Supervision, B. (2012). How Strong Is Strong User Authentication ?5. Retrieved from https://www.isaca.org/Journal/archives/2012/Volume-5/Pages/How-Strong-is-Strong-User-Authentication.aspx

Telegram. (2014). *MTProto Mobile Protocol*. 1–6. Retrieved from https://core.telegram.org/mtproto

Trabelsi, Z. (2005). Switched network sniffers detection technique based on IP packet routing. Information Systems Security, 14(4), 51–60. https://doi.org/10.1201/1086.1065898X/45528.14.4.20050901/90089.7

WhatsApp. (2019). Frequently Asked Questions KAINOS + Frequently Asked Questions. (1099), 1–3. Retrieved from https://faq.whatsapp.com/

Wireshark. (2019). Learn Knowledge is Power Go Beyond With SharkFest Sponsors About Wireshark. 1–9. Retrieved from https://www.wireshark.org/index.html#aboutWS