I. J. Computer Network and Information Security, 2018, 7, 23-35
Published Online July 2018 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2018.07.03

Assessing Vulnerability of Mobile Messaging Apps to Man-in-the-Middle (MitM) Attack

Rishabh Dudheria
Department of Electrical and Computer Engineering
New York Institute of Technology
E-mail: rdudheria@nyit.edu

Received: 01 February 2018; Accepted: 04 May 2018; Published: 08 July 2018

Abstract—Mobile apps are gaining in popularity and are becoming an indispensable part of our digital lives. Several mobile apps (such as messaging apps) contain personal/private information of the users. Inevitably, the compromise of accounts associated with such sensitive apps can result in disastrous consequences for the end user. Recently, Password Reset Man-in-the-Middle (PRMitM) attack was proposed at the application level in which an attacker can take over a user's web account while the user is trying to access/download resources from the attacker's website. In this work, we adapt this attack so that it can be applied in the context of mobile messaging apps. Specifically, we analyze 20 popular mobile messaging apps for vulnerability to MitM attack, 10 of which support secure communication through end-to-end encryption. Based on our holistic analysis, we have identified 10 of the tested apps as being vulnerable to MitM attack and elaborated on the corresponding attack scenarios. On comparing the secure messaging apps to non-secure messaging apps for vulnerability to MitM attack, we found that an app's features and design choices decide if it is susceptible to MitM attack irrespective of whether it provides end-to-end encryption or not. Further, we have proposed design improvements to increase the overall security of all mobile messaging apps against MitM attack.

Index Terms—Security, MitM attack, Mobile apps, Phone number verification, Password reset, Privacy.

I. Introduction

Mobile apps are gaining in popularity and are becoming an indispensable part of our digital lives. A wide range of mobile apps are currently available for a variety of purposes including messaging, shopping, health and fitness, utilities and productivity, sports, finance, entertainment, news and games. Flurry (a leading mobile analytics company) has stated in one of its recent reports [1] that U.S. consumers spend on average more than 5 hours per day on mobile devices. Further, this report adds that more than 90% of the user's time is spent on apps. This figure clearly shows the dominance and growing importance of mobile apps in our daily life. Moreover, a prior report [2] by Flurry concluded that the time spent by users on mobile apps grew by 69% year-over-year. According to their data, this growth is being led by messaging and social apps, which have witnessed an astounding growth of about 394% in terms of time spent by the users over the period 2015-2016. Indeed, such results seem to be plausible if one were to consider the massive popularity of messaging apps such as Facebook Messenger [3] and WhatsApp Messenger [4], which have both been installed more than a billion times just on Android devices.

Several mobile apps contain personal/private information of the users. For instance, numerous digital wallet apps that are being used for mobile payments contain sensitive financial information of the user including banking information and credit/debit card information. Similarly, mobile messaging apps are commonly used by users for sharing pictures, documents, scan of ID's, postal addresses, online banking access codes, etc. Inevitably, the compromise of accounts associated with such sensitive apps can result in disastrous consequences for the end user. At the same time, the nature of data held by such sensitive apps along with the operations that can be performed by using them makes such apps a high value target for the attackers. Hence, it is imperative to ensure the security of such apps so that an attacker cannot take over user's account associated with these apps.

Gelernter et al. [5] recently proposed the idea of Password Reset Man-in-the-Middle (PRMitM) attack at the application level in which an attacker can take over a user's web account while the user is trying to access/download resources on the attacker's website. The proposed attack is carried out in the following way: Initially, the attacker's site requests the user to register for free using her email address and/or prove that she is human by using her phone number in order to access/download resources (e.g., free software). Next, the attacker initiates a password reset request for the user's web account based on the email address and/or phone number received earlier. During this process, if the web service (associated with user's account) requires CAPTCHA challenges to be solved or answers to security questions, then the attacker relays the corresponding CAPTCHA's or security questions to users and forwards users' solutions/answers to the web service. On the other

hand, if the web service handles password reset based on a verification code sent to the user's phone number via SMS or phone call, then the attacker's site claims to send a verification code to the user's phone number. Afterwards, the attacker's site requires the user to enter the verification code (which is actually sent by the web service) to access/download the desired resource. Later, the attacker simply relays the code to the web service, thereby gaining access to user's web account. Although this study focused on the password reset process of popular websites and email providers, it included a section analyzing the vulnerability of certain popular mobile messaging applications to PRMitM attack. However, this assessment has numerous shortcomings.

Mobile messaging apps are primarily targeted for mobile devices such as smartphones (although some of them provide an associated website or PC application to access the app account). Since users frequently change their phones, most (if not all) messenger apps are designed to allow migration of accounts from one phone to another. This is quite unlike web services, which are universally accessible via Internet and a browser. While account access on websites is predominantly based on email address and password, mobile messaging apps may additionally provide account access based on a verification code sent to the phone number. This implies that while the MitM attack on web services is possible during password reset process, the same attack can be carried out on mobile messaging apps during phone number verification phase besides password reset phase depending on their design. Due to these basic differences in the nature of website accounts and mobile messaging app accounts, one needs to consider MitM attack on the messaging apps holistically.

The previous research [5] analyzing the vulnerability of popular mobile messaging apps to password reset MitM attack is inaccurate and incomplete due to the following reasons. First and foremost, it does not clearly identify which of the tested messaging apps are vulnerable to MitM attack and under what circumstances can such an attack be successful. Second, it considers the vulnerability of messaging apps by just looking at its password reset process along with the corresponding SMS and voice call message in isolation. It seems that the authors have considered MitM attack during phone number verification phase as a simple variation of MitM attack during password reset phase. However, this is inadequate as one needs to consider the overall working and features of the app to determine if it is vulnerable to MitM attack. For instance, prior work does not take into account additional security features (such as two-step verification) offered by certain apps (e.g., WhatsApp and Telegram) while analyzing them for vulnerability to MitM attack. This feature enables the user to optionally set a password (or PIN) to prevent unauthorized access to the account through another device. Third, some apps on being installed on a new device initially require a successful phone number verification and then the correct password to access the corresponding account (e.g., Kakao Talk). Therefore, MitM attack needs to be carried out twice in such cases to enable the attacker to take over user's account. Hence, one cannot ascertain whether Kakao Talk is vulnerable to MitM attack just by analyzing its phone number verification process (as has been done in the earlier paper).

Additionally, the description of password reset process for Nimbuzz and Snapchat as mentioned in the text and Table V of the previous paper is inconsistent[1]. The issue is that while the corresponding table mentions that Nimbuzz requires a username to initiate password reset, the associated text mentions that Snapchat requires a username to initiate password reset. During our evaluation, we found that only Nimbuzz requires a username to initiate password reset. On the other hand, Snapchat allows password reset to be initiated by using the email address followed by the phone number of the victim.

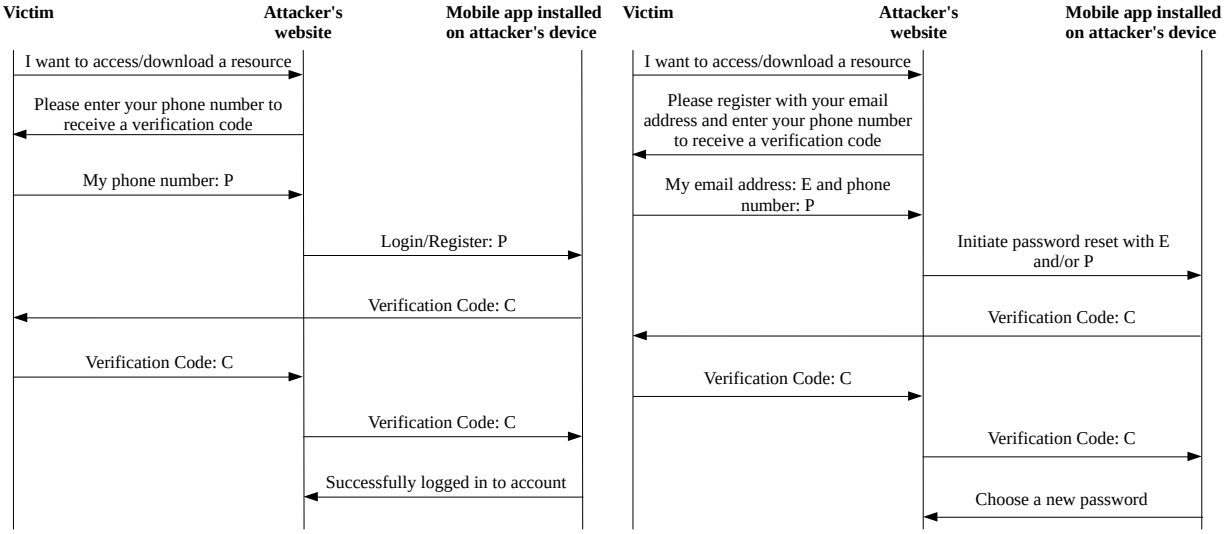
Consequently, the question of how well the messaging apps withstand MitM attack and the factors that influence their resilience to such an attack remains unanswered. Therefore, in this paper, we directly focus on analyzing the mobile messaging apps for vulnerability to the MitM attack at the application level. Additionally, there has been a rising concern about the security and privacy of messaging apps due to the sensitivity of the information shared via such apps. In response to such concerns, several companies have started offering secure messaging apps that provide end-to-end encryption [6]. Since it would be interesting to assess the vulnerabilities of such secure messaging apps to MitM attack as well, we decided to consider both the secure and non-secure messaging apps in our study. In particular, a compromise of the account information associated with such apps can result in catastrophic consequences for the end user ranging from disclosure of personal/private information to loss of reputation to financial losses.

Contributions: In this work, we evaluate the popular mobile messaging apps for susceptibility to MitM attack at the application level, which can be carried out during phone number verification phase as well as password reset phase depending on the design of the corresponding app. Specifically, we consider 20 popular mobile messaging apps in this study, 10 of which support secure communication through end-to-end encryption. We review the various approaches for login as well as password reset adopted by the popular mobile messaging apps. Based on our analysis, we identify the apps that are vulnerable to MitM attack and elaborate on the corresponding attack scenarios. Further, we compare the design and behavior of various messaging apps to ascertain if the secure messaging apps are less vulnerable to MitM attack as compared to the other messaging apps. Finally, we suggest design improvements in accordance with our results to increase the overall security of all mobile messaging apps against MitM attack. We consider this work to be beneficial to the app developers as they

[1]Assuming that these apps have not been redesigned between the third quarter of 2016 (i.e., when the previous survey was carried out) and the last quarter of 2017 (i.e., when the current experiments were carried out).

can improve the security of their products by implementing our recommendations.

The rest of this paper is organized as follows: Section 2 provides additional background necessary to comprehend this work. Our methodology for conducting this study is specified in Section 3. Section 4 outlines the features of the tested apps relevant from the point of view of the discussed MitM attack. A detailed analysis of the issues with the SMS and voice call messages being used by the various apps is presented in Section 5. Section 6 describes a case study of how the MitM attack could be conducted on the Telegram app. Based on our holistic analysis of the working of the selected apps, we have identified the apps that are vulnerable to MitM attack in Section 7. An overall discussion of this study including suggested design improvements is provided in Section 8. Finally, Section 9 presents the conclusion and provides direction for future work.



(a) Phone Number Verification MitM attack (b) Password Reset MitM attack

Fig.1. MitM Attacks

II. Background

NIST [7] defines man-in-the-middle attack as follows: "An attack in which an attacker is positioned between two communicating parties in order to intercept and/or alter data traveling between them." In this work, we suitably adapt the PRMitM attack proposed by Gelernter et al. [5] so that it can be applied in the context of mobile messaging apps. Next, we discuss the two specific scenarios in which a MitM attack can be conducted on mobile messaging apps.

Since mobile messaging apps provide access to an account based on phone number verification or password, we consider the MitM attack associated with these options as "Phone Number Verification MitM attack" and "Password Reset MitM attack" respectively (for ease of understanding). The steps required to successfully carry out these attacks are illustrated in Figure 1. We ignore the requirement of solving CAPTCHA challenges or answering security questions during this process, as the attacker can simply forward them to the user and then submit user's solutions/answers back to the app. Most of the mobile messaging apps do not provide an associated website or PC application to access the app account. Therefore, for simplicity, we assume that the attacker would attempt to perform the MitM attack by installing the messaging app on its mobile device.

The steps illustrated in Figure 1 are outlined below.

(a) *Phone Number Verification MitM attack:* In this scenario, the attacker's website requests the victim to provide her phone number to receive a verification code in order to access/download the desired resource. Once the victim enters this information, the attacker uses it to login/register on the app installed on its device. The corresponding app then sends a verification code to the victim via SMS or phone call. However, the victim is under the impression that she is supposed to receive the code from the attacker's website. Next, the victim enters this verification code on the attacker's website. Subsequently, the attacker uses this verification code to take over victim's account on the app.

(b) *Password Reset MitM attack:* In this scenario, the attacker's website requests the victim to register with her email address and to enter her phone number to receive a verification code in order to access/download the desired resource. Once the victim provides these two pieces of information, the attacker uses it to initiate a password reset for the victim's account on the app installed on its device. The corresponding app then sends a verification code to the victim via SMS or phone call. However, the victim is under the impression that she is supposed to receive the code from the attacker's website. Next, the victim enters this verification code on the attacker's website. Subsequently, the attacker uses this verification code to reset the password for victim's account and hence takes over her account.

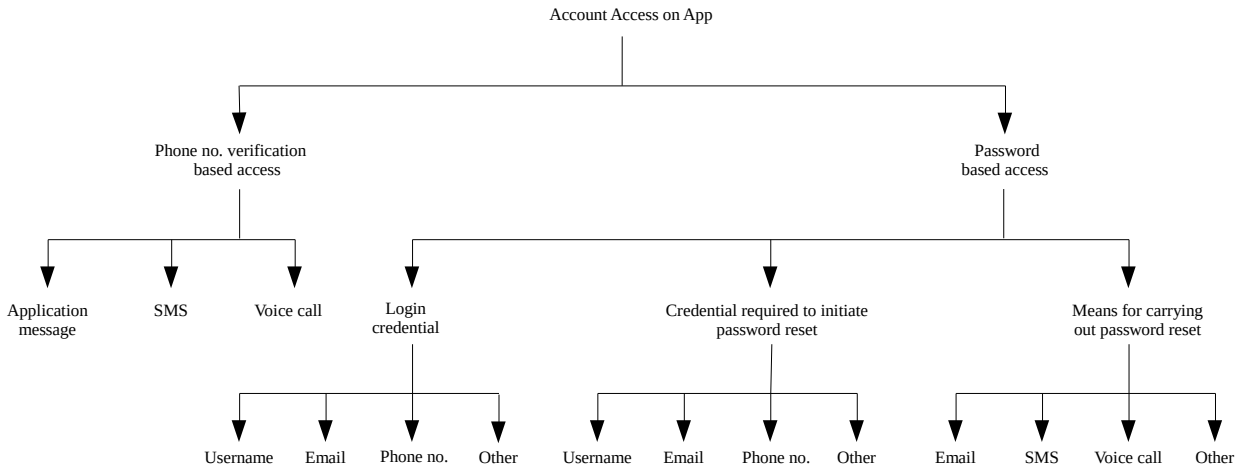


Fig.2. Options for Account Access in Mobile Messaging Apps

Figure 2 illustrates the options provided by the mobile messaging apps for accessing an account (relevant from an attacker's point of view). The apps that provide account access based on phone number verification usually send a verification code as an application message, SMS or voice call message. On the other hand, the apps that provide account access based on password need to be evaluated in terms of their login credentials and how password reset is initiated as well as carried out to assess their vulnerability to MitM attack. During our study, we found that username, email and phone number are the most commonly used credentials for login as well as to initiate password reset. Further, all of the studied apps allowed password reset to be carried out via email, SMS or voice call.

Now, let us look at the factors that decide if an attacker can successfully perform the MitM attack on the account associated with a mobile messaging app. As per the discussed attack scenarios, it is feasible for the attacker to request the following pieces of information from the user: email, phone number and verification code sent via SMS or voice call. However, the attacker cannot claim to send a verification code via an application message. Similarly, it is implausible for an attacker to trick the user to give her username associated with an app account. Thus, apps that solely depend on application message for sending verification code, username for login or for initiating password reset cannot be vulnerable to MitM attack.

Whether a user would enter the verification code received via SMS or voice call message into the attacker's website is mainly dependent on the content of these messages. Similar to Gelernter et al. [5], we consider an SMS or voice call message to be secure if it clearly specifies the sender, purpose of the message and warn the recipient about disclosing the code. If the information regarding the sender is missing from the SMS or voice call message, then even a vigilant user cannot determine the source of the message. In such situations, an attentive user would also easily fall for the MitM attack without suspecting any foul play. On the other hand, if the SMS or voice call message includes information about the sender but lacks purpose and/or warning, then giving away the corresponding verification code to the attacker's website can be considered as negligence on the part of the user. Indeed, such negligent user behavior was observed in the two user studies conducted by Gelernter et al.

The first user study involved MitM attack on Facebook password reset process carried out via SMS message. This experiment disclosed that users sometimes fall for the MitM attack because they just search for the verification code in an SMS message without reading the corresponding text. Further, participants admitted to reading the verification code directly from the pop-up notification on their phones without opening the corresponding message. The second user study involved MitM attack on the password reset process of Google accounts carried out via voice call message. Specifically, the voice call from Google in English language contained information regarding the sender and a warning about disclosing the code but did not mention about the purpose of the call. The results of this study revealed that majority of the users fell for the MitM attack since they could not determine the purpose of the verification code. Additionally, few users fell for the MitM attack as they did not pay enough attention to the voice call message.

As pointed out by Gelernter et al., password reset carried out via email does not exhibit the same characteristics as SMS or voice call message. Hence, email based password reset is not vulnerable to MitM attack as long as the attacker cannot access the data in the email account of the victim.

To summarize, the following categories of mobile messaging can be vulnerable to MitM attack: (a) For apps that provide phone number verification based account access, the ones that send verification code via SMS or voice call message. (b) For apps that provide password based account access, the apps that allow login and to initiate password reset via email or phone number and carry out password reset through verification code sent via SMS or voice call.

III. Methodology

This section outlines the methodology used for

carrying out the investigation proposed in this work. We list the various apps selected for examination and specify their overall evaluation procedure. Additionally, we also describe the assumptions on which our analysis is based and provide justification of why such an investigation is important.

Table 1. List of Selected Mobile Messaging Apps

No.	Secure Messaging App	Developer	Version	Non-secure Messaging App	Developer	Version
1	Telegram	Telegram Messenger LLP	4.4.1	imo free video calls and chat	imo.im	9.8.000000008491
2	WhatsApp Messenger	WhatsApp Inc.	2.17.395	Hike Messenger - Hide Chat, Call, Stickers, Wallet	Hike Ltd.	5.3.3
3	Kakao Talk: Free Calls & Text	Kakao Corporation	6.4.6	Snapchat	Snap Inc.	10.19.0.0
4	Viber Messenger	Viber Media S. àr.l	7.8.0.0	SNOW - Video call, Selfie, Face filter, Fun camera	SNOW, Inc.	3.7.0
5	Messenger - Text and Video Chat for Free[2]	Facebook	140.0.0.18.63	BBM: Free Calls & Messages	BlackBerry Limited	3.3.8.74
6	JusTalk	JusTalk	7.0.1	ooVoo: Video Calls, Messaging & Stories	ooVoo LLC	4.2.1
7	LINE: Free Calls & Messages	LINE Corporation	7.14.0	Skype	Skype	7.46.0.596
8	Cyphr	Golden Frog, GmbH	0.7.3	Kik	Kik Interactive	11.36.0.18816
9	Voxer Walkie Talkie Messenger	VoxerPro LLC	3.18.5.19765	Path Talk	Path Mobile, Inc.	1.3.6
10	Wickr Me - Private Messenger	Wickr Inc.	4.9.3	Nimbuzz	MSM Limited	5.2.0

[2]Henceforth, this app would be referred to as "Facebook Messenger"

We collected a sample of 20 popular free mobile messaging apps [8-10] that support English language from Google Play Store [11] for testing purposes. This collection included 10 secure messaging apps[3] that provide end-to-end-encryption. The selected apps are listed in Table I along with other pertinent details, including the name of the developer and version number. Due to the shortcomings of the previous study [5], we decided to include all the messaging apps analyzed previously in this project.

We assume that federated logins are not used to access the apps even if such choices are available. Additionally, we assume that a user registers her email address and phone number with the accounts associated with all the tested apps (wherever both these options are available). We do not consider the issue of how the victims become aware of the fact that their account has been compromised and what actions can they undertake to regain access to their account. A user study to assess the vulnerability of accounts associated with mobile messaging apps to MitM attack is out of scope of this paper.

All the apps listed in Table I have been studied and evaluated using two Android smartphones (v4.4.4 and v5.0.2). The overall investigation of the selected apps was performed in the following manner. Initially, each app was downloaded on the first Android phone and a new account was created using a fixed phone number and/or email address (as appropriate). Next, we noted down the various relevant features of these apps, i.e., availability of two-step verification, options provided for login as well as to initiate password reset and how password reset was being carried out (wherever applicable). Then, the apps were installed on the second Android device and an attempt was made to conduct MitM attack on the accounts created in the previous step. We observed whether the apps required a phone number verification code for account access or provided password based account access when installed on the second device. We also noted down the SMS and voice call messages being sent by the apps during phone number verification phase as well as password reset phase. Thereafter, a detailed analysis of each app was carried out to determine if it is vulnerable to MitM attack. Further, we tried to compare the two types of messaging apps to ascertain if the secure messaging apps are less vulnerable to MitM attack as compared to the other messaging apps.

Though the number of mobile messaging apps selected in this study is small, nonetheless they represent the most prominent mobile messaging apps in terms of number of users worldwide. Hence, these apps are quite likely to be viewed as a model for design purposes by other mobile messaging apps. Therefore, vulnerability of the studied apps to MitM attack can not only impact a large number of users but also a large fraction of other mobile messaging apps available currently. Moreover, the analysis performed in this paper can serve as a basis for evaluating other categories of mobile apps that contain sensitive user information (e.g., digital wallets).

[3]Determination of such apps was done based on the description available on the corresponding Google Play Store or company webpage along with online reports [12-13].

IV. Features of Popular Mobile Messaging Apps

This section presents the features of the studied apps relevant from the point of view of the discussed MitM

attack. Table II lists the account access options provided by the various apps. This table also provides important remarks about the behavior of various apps, which would be crucial in determining their susceptibility to MitM attack. While a majority of the apps provide account access based on password, there are several that do so based on phone number verification. Telegram and WhatsApp additionally require password/PIN for account access on another device when two-step verification is enabled. This feature enables the user to optionally set a password (or PIN) to prevent unauthorized access to the account through another device. Similarly, Cyphr additionally requires passphrase for account access on another device when multi-device feature is enabled. This passphrase is used to encrypt the private key. Kakao Talk requires phone number verification and then login via Kakao account to restore the data on a new device.

Table 2. Account Access Options Provided by Various Apps

No.	App	Requires phone no. verification	Requires password	Supports two-step verification	Remarks
1	Telegram	✓	-	✓	When trying to login on another device using phone no., a message is first sent through Telegram application. Then, an SMS can be initiated. Further, if code is still not entered within 120s, then a voice call is done by the app. After entering the code, password associated with two-step verification is required to access the account.
2	WhatsApp	✓	-	✓	When trying to login on another device with the phone no., an SMS is sent. If code is not entered within 65s, then an option for resending the SMS or initiating a voice call becomes available. After entering the code, PIN associated with two-step verification is required to access the account.
3	Kakao Talk	✓	✓	-	When trying to login on another device using phone no., an SMS is sent. After entering the code, login via Kakao account (i.e., corresponding email address and password) is required to restore the data.
4	Viber	✓	-	-	App first sends an SMS & then an option to receive a voice call becomes available.
5	Facebook Manager	-	✓	-	Assuming that login is performed using Facebook account.
6	JusTalk	-	✓	-	-
7	LINE	-	✓	-	Assuming that the user created the associated account through the mobile messaging app and not via the PC application.
8	Cyphr	-	✓	✓	When trying to login on another device, email & password are required. Then, passphrase is required to access the account (assuming that multi-device feature is enabled).
9	Voxer	-	✓	-	-
10	Wickr Me	-	✓	-	-
11	imo	✓	-	-	App first sends an SMS & if code is not entered within 60s, then a voice call is done.
12	Hike	✓	-	-	App first sends an SMS & if code is not entered within 150s, then an option for receiving a voice call becomes available.
13	Snapchat	-	✓	-	-
14	SNOW	-	✓	-	-
15	BBM	-	✓	-	-
16	ooVoo	-	✓	-	-
17	Skype	-	✓	-	New Skype accounts are Microsoft accounts.
18	Kik	-	✓	-	-
19	Path Talk	-	✓	-	-
20	Nimbuzz	-	✓	-	-

Table 3. SMS and Phone Call Messages Used by Relevant Apps during Phone number Verification

App	SMS message	Phone Call message
Telegram	Telegram code XXXXX	Hello, thank you for using our phone verification system, your code is XXXXX. Once again, your code is XXXXX. Goodbye.
WhatsApp	WhatsApp code XXX-XXX. You can also tap on this link to verify your phone: v.whatsapp.com/XXXXXX	Your verification code is XXXXXX (repeated four times).
Kakao Talk	XXXX Verification Code from Kakao Talk. [Kakao Talk]	-
Viber	Your Viber code is: XXXXXX. Close this message and enter the code into Viber to activate your account.	Hello, your Viber code is XXXXXX. Once again, your code is XXXXXX.
imo	imo code: XXXX	Your imo verification code is XXXX. Repeat again.
Hike	Hi! Your hike PIN is XXXX. Happy hiking :)	Your hike PIN is XXXX (repeated thrice).

Apps that require phone number verification for account access need to be checked for susceptibility to MitM attack by analyzing the content of the corresponding SMS and/or phone call message. On the other hand, apps that provide password based access to an account may be vulnerable to MitM attack depending on the following factors: (a) Login credential, (b) Credential required to initiate password reset, (c) Means for carrying out password reset, along with (d) Content of corresponding SMS and/or phone call message (wherever applicable). Moreover, apps that support two-step verification need to be additionally checked for how the corresponding password/PIN/passphrase can be reset.

Table 4. Types of Login Credentials Being Used by the Relevant Apps

App	Username	Email	Phone no.
Kakao Talk	-	✓	-
Facebook Messenger	-	✓	✓
JusTalk	-	-	✓
LINE	-	✓	-
Cyphr	-	✓	-
Voxer	-	✓	-
Wickr Me	✓	-	-
Snapchat	✓	✓	-
SNOW	✓	✓	-
BBM	-	✓	✓
ooVoo	✓	✓	-
Skype	✓	✓	✓
Kik	✓	✓	-
Path Talk	-	✓	-
Nimbuzz	✓	-	-

A. Apps that Require Phone Number Verification for Account Access

We noted down the SMS and voice call messages sent by the apps that require phone number verification to provide access to the account (when being used on another device). The corresponding data is presented in Table III.

B. Apps that Require Password for Account Access

Table IV provides the login credentials being used by the various relevant messaging apps. As can be seen from this table, almost half of the apps allow more than one credential to be used for login purposes. Among this set of apps, email is the most popular login credential followed by username in the second place, while phone number is the least supported login credential. Wickr Me and Nimbuzz apps solely depend on username for login purposes.

The credentials required to initiate a password reset request in the relevant apps is presented in Table V. Email, username and phone number are the commonly used credentials for initiating password reset in this sample of apps. Several apps allow password reset to be initiated based on more than one credential. Email is the most prominent credential used for initiating password reset. Snapchat allows a combination of two of the credentials among the set of username, email and phone number to be used for initiating password reset besides just email. SNOW allows password reset to be initiated based on the name of the user besides the other common options. Nimbuzz allows password reset to be initiated solely based on the username (i.e., Nimbuzz ID) associated with an account. Wickr Me does not provide an option to reset password. This app requires the user to create a new account if she forgets the password.

Table 5. Credentials Required to Initiate Password Reset in Relevant Apps

App	Username	Email	Phone no.	Other
Kakao Talk	-	✓	-	-
Facebook Messenger	-	✓	✓	-
JusTalk	-	-	✓	-
LINE	-	✓	-	-
Cyphr	-	✓	-	-
Voxer	-	✓	-	-
Snapchat	-	✓	-	(Username + email) or (Username + phone no.) or (Email + phone no.)
SNOW	✓	✓	✓	-
BBM	-	✓	✓	-
ooVoo	✓	✓	✓	-
Skype	✓	✓	✓	-
Kik	✓	✓	-	-
Path Talk	-	✓	-	-
Nimbuzz	✓	-	-	-

Table 6. Means for Carrying Out Password Reset in Relevant Apps

App	Email	SMS	Phone call
Kakao Talk	✓	-	-
Facebook Messenger	✓	✓	-
JusTalk	-	✓	✓
LINE	✓	-	-
Cyphr	✓	-	-
Voxer	✓	-	-
Snapchat	✓	✓	✓
SNOW	✓	✓	-
BBM	✓	✓	-
ooVoo	✓	✓	-
Skype	✓	✓	✓
Kik	✓	-	-
Path Talk	✓	-	-
Nimbuzz	✓	✓	-

Means for carrying out password reset in the relevant apps is presented in Table VI. Email, SMS and phone call message are the choices provided by the tested apps in this respect. Around half of the apps support at least two of the above options for carrying out password reset. Several apps (i.e., Kakao Talk, LINE, Cyphr, Voxer, Kik and Path Talk) allow password reset to be carried out only via email.

Finally, the SMS and voice call messages sent by the apps during the password reset process are mentioned in

Table VII. While some of the apps support SMS as well as voice call message for providing verification code, several do so only via an SMS message.

C. Apps that Require Two-step Verification

While Telegram and WhatsApp allow the password/PIN associated with two-step verification to be reset via email, Cyphr does not provide an option to reset the corresponding passphrase.

Table 7. SMS and Phone Call Messages Used by Relevant Apps during Password Reset

App	SMS message	Phone Call message
Facebook Messenger	XXXXXX is your Facebook password reset code[PIN]	-
JusTalk	[JusTalk] Code:XXXX. Please go back JusTalk and enter it to verify.	*Did not receive voice call*
Snapchat	Snapchat password reset code: XXXXXX. Only enter your code inside Snapchat. If you didn't request this, you can ignore this message :)	Your Snapchat verification code is XXXXXX, again that's XXXXXX. Happy Snapping!
SNOW	SNOW verification code: [XXXX]	-
BBM	[BBM] Your BBM verification code is XXXX	-
ooVoo	XXXX is your ooVoo PIN. Thanks! 80rUGOAwDLm	-
Skype	Use XXXXXXX as Microsoft account password reset code	Hello. Thank you for using our phone verification system. Your code is XXXXXXX. Once again, your code is XXXXXXX.
Nimbuzz	*Did not receive SMS message*	-

V. Analysis of SMS and Voice Call Messages of Tested Apps

We now present an analysis of the issues with the SMS and voice call messages being used by the various apps. As has already been mentioned earlier, all secure SMS and voice call messages should contain three fundamental components, i.e., sender, purpose of the message and warning about disclosing the code. Note that the presence of an issue with an SMS or voice call message does not necessarily make the corresponding app vulnerable to MitM attack. One has to consider the working of an app holistically to determine if an unsecure SMS or voice call message can lead to it being susceptible to MitM attack.

A. Issues with SMS Messages

(a) *Sender is not specified:* All of the relevant tested apps specified the sender in their SMS messages.

(b) *Purpose is missing:* Since apps may send SMS messages during phone number verification phase or during password reset phase, this purpose should clearly be specified in the corresponding messages. However, this study found that several of the considered apps send an SMS message containing information about the sender and verification code but do not specify the purpose of the message. For instance, Telegram, Kakao Talk, imo and Hike do not specify that their SMS messages have been sent to verify the phone number. On the other hand, WhatsApp and Viber clearly specify this purpose in their SMS messages. Similarly, JusTalk, SNOW, BBM and ooVoo do not specify that their SMS messages have been sent in response to a password reset request. On the contrary, Facebook Messenger, Snapchat and Skype mention that their SMS messages contain password reset code.

(c) *Warning is not mentioned:* None of the relevant tested apps (except Snapchat) include a warning about disclosing the code in their SMS messages. Specifically, Telegram, WhatsApp, Kakao Talk, Viber, imo, Hike, Facebook Messenger, JusTalk, SNOW, BBM, ooVoo and Skype suffer from this issue.

B. Issues with Phone Call Messages

(a) *Sender is not specified:* In this study, we found that the voice call messages of Telegram, WhatsApp and Skype do not include information regarding the sender. This is a serious flaw as it can cause the user to believe that such calls have been originated by the attacker's website.

(b) *Purpose is missing:* Since apps may send voice call messages during phone number verification phase or during password reset phase, this purpose should clearly be specified in the corresponding messages. However, we found that none of the tested apps that support sending a verification code via voice call specify the purpose of the message. For instance, Telegram, WhatsApp, Viber, imo and Hike do not specify that their voice calls are in response to a phone number verification request. Similarly, Snapchat and Skype do not mention that their voice calls have been initiated in response to a password reset request.

(c) *Warning is not mentioned:* None of the relevant tested apps include a warning about disclosing the code in their voice call messages. Specifically, Telegram, WhatsApp, Viber, imo, Hike, Snapchat and Skype suffer from this issue.

To better understand how one should go about evaluating an app for vulnerability to MitM attack, we

elaborate on a case study describing how the MitM attack could be conducted on Telegram app in the next section.

VI. A Case Study: MitM Attack on Telegram

Telegram provides account access based on phone number verification when being used on another device. Additionally, this app supports two-step verification. This feature allows a user to optionally set a password to prevent unauthorized access to the account through another device. Hence, both phone number verification and password are required to access user's account on another device if two-step verification is enabled. Therefore, we need to consider MitM attack on Telegram separately for the following two cases:

(a) *Two-step verification is disabled:* In this case, the attacker needs to successfully complete the phone number verification step on its device to gain access to user's account. After obtaining the phone number from the user, the attacker can simply enter it in the Telegram app installed on its mobile device. Then, Telegram sends an application message with a code to the user's mobile device (on which the app is currently being used). At this point, the attacker can initiate a request in the Telegram app for an SMS message to be sent with the code. If the code is not entered in this app within 120s, then a voice call with the code is automatically initiated by the app.

Now, the attacker's website cannot claim to send the code to the user via an application message. Hence, there is no reason for a user to give away the code received from Telegram in the form of an application message to the attacker's website. However, there are several issues with the SMS and voice call message used by this app. In particular, its voice call does not inform the recipient about the sender. Thus, the user may accidentally give away the code to the attacker's website (if she is unable to correlate the SMS or voice call message with the application message) enabling the attacker to access her account.

(b) *Two-step verification is enabled:* In this situation, besides successfully completing the phone number verification step (as mentioned above), the attacker also needs to enter the password to log in to user's account. Since the attacker does not know the password, it can choose the "Forgot Password" option at this point. This would result in Telegram app sending an email to the user assuming that the user had set up such a recovery email at the time of choosing the password. On the other hand, if a recovery email was not chosen by the user, then the password cannot be reset. Thus, an attacker cannot successfully conduct the MitM attack on user's Telegram account if two-step verification is enabled.

The above analysis assumes that the attacker is trying to perform MitM attack on user's Telegram account by installing this app on its mobile device. Another option for the attacker is to use Telegram web interface to attempt MitM attack. The behavior of Telegram web is similar to Telegram app installed on a mobile device. It only differs with respect to the timing of when the SMS and voice call with the code can be initiated by the attacker.

VII. Identifying Apps Vulnerable to MitM Attack

Among the selected apps, we found that 30% of the sample provide account access based on phone number verification and 70% do so based on password. One of the apps (i.e., Kakao Talk) requires both phone number verification as well as password for account access on another device. Further, three of the tested apps (i.e., Telegram, WhatsApp and Cyphr) support two-step verification. Based on our holistic analysis of the working of the tested apps, we have classified them into two groups consisting of apps that are vulnerable and not vulnerable to MitM attack. Table VIII lists the apps that are vulnerable to MitM attack along with the corresponding attack scenarios. Table IX lists the apps that are not vulnerable to MitM attack and the corresponding reason for this conclusion. Overall, 10 of the 20 tested apps were identified to be vulnerable to MitM attack.

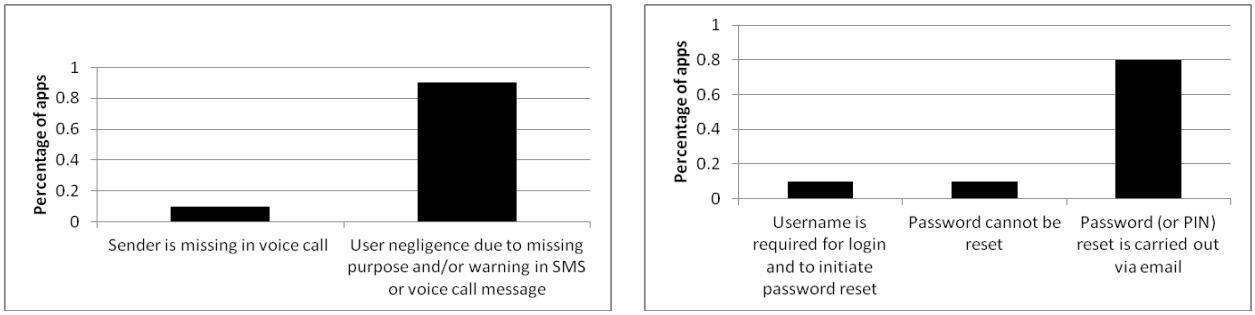
Table 8. Apps Vulnerable to MitM Attack

No.	App	How can the attacker achieve MitM attack?
1	Viber	Login/register on the app with user's phone no. & enter verification code provided by the (negligent) user.
2	Facebook Messenger	Initiate password reset via user's phone no. & enter verification code provided by the (negligent) user.
3	JusTalk	Initiate password reset via user's phone no. & enter verification code provided by the (negligent) user.
4	imo	Login/register on the app with user's phone no. & enter verification code provided by the (negligent) user.
5	Hike	Login/register on the app with user's phone no. & enter verification code provided by the (negligent) user.
6	Snapchat	Initiate password reset via user's email followed by user's phone no. & choose the option to receive code via voice call. Then, enter the code provided by the (negligent) user.
7	SNOW	Initiate password reset via user's phone no. & enter verification code provided by the (negligent) user.
8	BBM	Initiate password reset via user's phone no. & enter verification code provided by the (negligent) user.
9	ooVoo	Initiate password reset via user's phone no. & enter verification code provided by the (negligent) user.
10	Skype	Initiate password reset via user's phone no. & choose the option to receive code via voice call. Then, enter the verification code provided by the user.

Among the set of vulnerable apps, Skype is the worst affected by MitM attack as its voice call does not specify the sender, purpose of the message or warning about disclosing the code. In this case, the attacker can initiate a password reset request via user's phone number and then choose the option to receive code via voice call. Since this voice call does not include information about the sender, even a vigilant user will unsuspectingly enter the received code into the attacker's website. Consequently, the attacker would use this code to take over user's account in Skype.

Table 9. Apps not Vulnerable to MitM Attack

No.	App	Why is the app not vulnerable to MitM attack?
1	Telegram	Allows password to be reset only via email if two-step verification is enabled.
2	WhatsApp	Allows PIN to be reset only via email if two-step verification is enabled.
3	Kakao Talk	Password reset can be carried out only via email.
4	LINE	Password reset can be carried out only via email.
5	Cyphr	Password reset can be carried out only via email.
6	Voxer	Password reset can be carried out only via email.
7	Wickr Me	Password reset option is not available.
8	Kik	Password reset can be carried out only via email.
9	Path Talk	Password reset can be carried out only via email.
10	Nimbuzz	Nimbuzz ID is required to reset password.



(a) Reasons why apps are vulnerable to MitM attack (b) Reasons why apps are not vulnerable to MitM attack

Fig.3. Graph Depicting the Reasons why Apps are Vulnerable and not Vulnerable to MitM Attack

Successful MitM attacks were identified against several other apps based on the observation that a missing purpose and/or warning in the SMS or voice call message could lead a negligent user to give away the corresponding code to the attacker's website. The corresponding attack scenarios for the affected apps are as follows: (a) The SMS and voice call messages used by Viber, imo and Hike do not specify the purpose of the message and/or warn about disclosing the code. An attacker can login/register on these apps with the user's phone number and then enter the verification code provided by the (negligent) user to take over her account. Note that Hike Messenger is a highly sensitive application for MitM attack as it also contains a wallet. (b) Although the SMS message of Snapchat is secure, its voice call does not specify the purpose of the message and warn the user about disclosing the code. This fact can be exploited by an attacker to initiate password reset in Snapchat by entering user's email address and following it with user's phone number. Next, the attacker can select the option to receive code via voice call. Afterwards, the attacker can enter the code provided by the (negligent) user to take over her account in Snapchat. (c) Finally, the SMS messages sent by Facebook Messenger, JusTalk, SNOW, BBM and ooVoo on initiating password reset do not specify the purpose of the message and/or warn about disclosing the code. The attacker can simply initiate password reset for user's account on these apps via user's phone number and then enter the verification code provided by the (negligent) user to take over her account.

Half of the tested apps were determined to be not vulnerable to MitM attack due to the following reasons: (a) Telegram and WhatsApp provide additional security in the form of two-step verification. Both these apps allow the password/PIN associated with an account to be reset only via email. So, a MitM attack on these apps is unfeasible as long as two-step verification is enabled. (b) Several apps allow password reset to be carried out only via email. Hence, such apps (i.e., Kakao Talk, LINE, Cyphr, Voxer, Kik and Path Talk) are immune to MitM attack. (c) Wickr Me app has made an interesting design choice by not allowing password to be reset. This app requires the user to create a new account if she forgets the password. (d) Finally, Nimbuzz requires the account username (i.e., Nimbuzz ID) for login and for initiating password reset. Although Nimbuzz allows this username to be recovered via SMS by providing phone number of the associated account, there is no reason for a user to enter such information on the attacker's website.

Figure 3 graphically depicts the reasons why apps considered in this study are vulnerable and not vulnerable to MitM attack. Among the tested apps, Skype is completely vulnerable to MitM attack (even if the user is vigilant) as its voice call message does not include information about the sender. 90% of the other apps classified as being vulnerable do not include information regarding the purpose of the message and/or warning about disclosing the code in their SMS and/or voice call.

Hence, a negligent user may enter the received code into the attacker's website in such cases. Among the apps classified as being unsusceptible to MitM attack, 80% depend on email as a medium to carry out password (or PIN) reset. Additionally, one app (i.e., Nimbuzz) depends on the account username for login as well as to initiate password reset while another app (i.e., Wickr Me) completely does away with the option to reset password, thereby making them unsusceptible to MitM attack.

Altogether, 30% of the tested secure messaging apps are vulnerable to MitM attack whereas 70% of the non-secure messaging apps are susceptible to MitM attack. If one is to compare the behavior and resilience characteristics of secure messaging apps to the non-secure messaging apps, it is difficult to draw boundaries and clearly mark the reasons for apps to be vulnerable (or not vulnerable) to MitM attack in each of these categories. This is because both these categories contain apps that provide access to account based on phone number verification and were determined to be vulnerable to MitM attack for similar reasons. For instance, Viber and imo (which are secure and non-secure messaging apps respectively) can be exploited by an attacker in a similar fashion to take over user's account. Additionally, both these categories contain apps that provide access to account based on password and were determined to be vulnerable (or not vulnerable) to MitM attack for similar reasons. As an example, Facebook Messenger and BBM (which are secure and non-secure messaging apps respectively) can be exploited by an attacker in a similar way to take over user's account. Another pertinent example is of Voxer and Path Talk (which are secure and non-secure messaging apps respectively) that are not susceptible to MitM attack as they support password reset only via email. Thus, one cannot draw specific conclusions as to whether secure messaging apps are safer than other messaging apps with respect to MitM attack. It seems to be the case that an app's features and design choices decide if it is susceptible to MitM attack irrespective of whether it provides end-to-end encryption or not.

VIII. Discussion

During this study, we created a new account on all the tested apps using a fixed email address and/or phone number. For ethical reasons, we deleted/disabled those accounts after completing the experiments wherever the apps provided an option to do so. Overall, the assessment performed in this study indicates mixed results. Security questions are relatively easy to bypass and hence one of the positive findings of this work was that none of the apps supported password reset via security questions. However, there are several areas in which the messaging apps can be improved from a security point of view.

Telegram and WhatsApp provide additional security in the form of two-step verification. However, this feature is optional in both these apps. We think that such a crucial security feature should not be optional as one cannot depend on users to make the right choice keeping security in mind [14]. Several apps were determined to be unsusceptible to MitM attack due to their overall functionality. However, this does not imply that the SMS and voice call messages being used by these apps do not require any improvement. For instance, although Telegram app is not vulnerable to MitM attack as long as two-step verification is enabled, its voice call message is completely unsecure. Specifically, its voice call does not provide information about the sender, purpose of the message or warning about disclosing the code. This is a grave error and we encourage the corresponding developer to rectify this issue as soon as possible. Further, the SMS and voice call messages of numerous apps lack consistency in terms of including information about the sender, purpose of the message and warning about disclosing the code. As an example, while the SMS message of Skype specifies the sender and purpose, its voice call does not specify the sender and purpose of the message. We think that all apps should provide consistent SMS and voice call messages for clarity and to avoid confusion.

As has already been suggested by Gelernter et al. [5] and verified through an experiment conducted by them, including a link in an SMS instead of the code in plaintext avoids MitM attack. This is based on the idea that users are unlikely to type a link received via SMS into the attacker's website. We suggest that this approach be adopted for SMS messages sent during phone number verification phase as well as during password reset phase. Among the tested apps, only WhatsApp sent a link along with code in its SMS message to verify the phone number. In general, the SMS messages should clearly identify the sending app, the purpose of the message (i.e., whether it has been sent in response to a phone number verification request or based on a password reset request) and include a warning about disclosing the code besides containing the relevant link. In the same vein, a phone call message should clearly identify the sending app, the purpose of the message and include a warning about disclosing the code.

Besides suitably designing the SMS and voice call messages, we think that educating the users regarding the modus operandi of MitM attack can be beneficial in reducing the success rate of such attacks. Users can be alerted about the methodology used for carrying out MitM attack through articles in online media, newspapers, magazines, etc. Further, informing the users about the importance of verification codes (from a security point of view) and how such codes should be handled can significantly reduce the possibility of MitM attack due to user negligence.

The analysis presented earlier for WhatsApp is based on the assumption that the user has enabled two-step verification. If two-step verification is not enabled in this app, then it is possible for the attacker to conduct MitM attack as the voice call message used by WhatsApp during phone number verification phase does not contain information about the sender. In this case, the attacker registers the user's phone number on this app and selects the option to receive code via voice call. Then, the

attacker enters the verification code provided by the user to take over her account.

Similarly, the analysis presented earlier for Facebook Messenger is based on the assumption that the user employs her Facebook account for login. However, this app also provides an option for login based on phone number verification without requiring a Facebook account. In this case, the message sent by this app is as follows: "XXXXXX is your Messenger code to verify your phone number[PIN]". Clearly, such an SMS does not warn the user about disclosing the code. Hence, the attacker can still carry out MitM attack by registering user's phone number on this app and then entering the code provided by the (negligent) user.

The messages being used by Facebook Messenger and Snapchat have been updated since their previous evaluation in the third quarter of 2016 [5]. The SMS message of Facebook Messenger no longer provides a link to reset the password. Instead, it provides a link to turn off SMS on the corresponding mobile number for the associated Facebook account. The SMS used by Snapchat now contains information about the sender, purpose of the message and warning about disclosing the code. Its phone call message has been updated to include information about the sender, but it still does not provide information about the purpose of the message and warning about disclosing the code. So, while the SMS message used by Snapchat is currently secure, its voice call message is still unsecure. An attacker can exploit the voice call message of Snapchat to conduct MitM attack on the account associated with this app (as has been explained in Section VII).

IX. Conclusion and Future Work

Mobile apps are growing in importance in term of time spent by the users and this growth is being led by messaging and social apps. Mobile messaging apps contain personal/private information of the users and are used for sharing sensitive data. Therefore, a compromise of the account information associated with such apps can result in catastrophic consequences for the end user ranging from disclosure of personal/private information to loss of reputation to financial losses. In this work, we have evaluated the popular mobile messaging apps for susceptibility to MitM attack at the application level, which can be carried out during phone number verification phase as well as password reset phase depending on the design of the corresponding app. Based on our findings, we have proposed design improvements to enhance the security aspects of such apps. We consider this work to be beneficial to the app developers as they can improve the security of their products by implementing our recommendations.

In particular, we examined 20 popular mobile messaging apps. Our collection included 10 messaging apps that support end-to-end encryption. Based on our holistic analysis, we classified the apps into two groups consisting of apps that are vulnerable and not vulnerable to MitM attack. Among the tested apps, we found that Skype is the worst affected by MitM attack as its voice call does not specify the sender. Other apps were classified as being vulnerable as they do not include information regarding the purpose of the message and/or warning about disclosing the code in their SMS and/or voice call. On the other hand, the apps classified as being unsusceptible to MitM attack depend on email as a medium to carry out password reset, do not provide an option to reset password or require username to initiate password reset.

Some of the messaging apps support sending SMS and voice call messages containing verification code in languages other than English. Thus, checking if such messages are non-secure (in the sense that they do not contain information regarding the sender, purpose of the message or warning about disclosing the code) can be a future avenue of research. This would help in determining if apps are vulnerable to MitM attack in other scenarios. Additionally, other categories of apps that hold sensitive user information (such as digital wallets) can be apt for analysis with respect to MitM attack. A large scale user study to determine the feasibility of MitM attack on popular mobile apps could provide insightful results that may be beneficial in suggesting design improvements for preventing such an attack on mobile apps.

References

[1] Simon Khalaf and Lali Kesiraju, "U.S. Consumers Time-Spent on Mobile Crosses 5 Hours a Day," *Flurry Analytics, Tech. Rep.*, Mar. 2017. [Online]. Available: http://flurrymobile.tumblr.com/post/157921590345/us-consumers-time-spent-on-mobile-crosses-5

[2] Simon Khalaf, "On Their Tenth Anniversary, Mobile Apps Start Eating Their Own," *Flurry Analytics, Tech. Rep.*, Jan. 2017. [Online]. Available: http://flurrymobile.tumblr.com/post/155761509355/on-their-tenth-anniversary-mobile- apps-start

[3] Messenger - Text and Video Chat for Free. Facebook. (Dec. 2017). [Online]. Available: https://play.google.com/store/apps/details?id=com.facebook.orca

[4] WhatsApp Messenger. WhatsApp Inc. (Dec. 2017). [Online]. Available: https://play.google.com/store/apps/details?id=com.whatsapp

[5] N. Gelernter, S. Kalma, B. Magnezi, and H. Porcilan, "The Password Reset MitM Attack," in *2017 IEEE Symposium on Security and Privacy, SP 2017*, May 2017, pp. 251–267.

[6] (2017, Oct.) End-to-end encryption. Wikipedia. [Online]. Available: https://en.wikipedia.org/wiki/End-to-end_encryption

[7] P. Grassi, M. Garcia, and J. Fenton, Digital Identity Guidelines, *National Institute of Standards and Technology (NIST) Std*. 800-63-3, June 2017.

[8] Joseph Schwartz. (2016, May) The Most Popular Messaging App in Every Country. *SimilarWeb*. [Online]. Available: https://www.similarweb.com/blog/worldwide-messaging-apps

[9] Alisia Watson. (2016, Sep.) 12 Most Used Messaging Apps. engadget.[Online].Available: https://www.engadget.com/2016 /09/30/12-most-used-messaging-apps/

[10] Leslie Walker. (2017, Jul.) The 10 Best Mobile Messaging Apps. lifewire. [Online]. Available: https://www.lifewire.com/best-mobile-messaging-apps-2654839
[11] Google Play. Google Inc. (Dec. 2017). [Online]. Available: https://play.google.com/store?hl=en
[12] (2016, Oct.) Snapchat, Skype among apps not protecting users privacy. *Amnesty International*. [Online]. Available: https://www.amnesty.org/en/latest/news/2016/10/snapchat-skype-among-apps-not-protecting-users-privacy/
[13] (2017, Nov.) Comparison of instant messaging clients. Wikipedia.[Online].Available: https://en.wikipedia.org/wiki/Comparison_of_instant_messaging_clients
[14] A. Mylonas, A. Kastania, and D. Gritzalis, "Delegate the smartphone user? Security awareness in smartphone platforms," *Computers & Security*, vol. 34, pp. 47–66, 2013.

Author's Profile

Rishabh Dudheria is an Assistant Professor in the Department of Electrical and Computer Engineering at New York Institute of Technology. He completed PhD and MS in Electrical and Computer Engineering at Rutgers, The State University of New Jersey in 2013 and 2008 respectively. His research is broadly focused in the field of Security.

How to cite this paper: Rishabh Dudheria,"Assessing Vulnerability of Mobile Messaging Apps to Man-in-the-Middle (MitM) Attack", International Journal of Computer Network and Information Security(IJCNIS), Vol.10, No.7, pp.23-35, 2018.DOI: 10.5815/ijcnis.2018.07.03