It Cannot Get Away: An Approach to Enhance Security of User Account in Online Social Networks

Abdulrahman Muthana† **Abdul Azim Abd Ghani††** **Rmlan Mahmod††**

Thamar University, Thamar, Yemen Universiti Putra Malaysia, 43400 Serdang, Selangor, Malaysia Universiti Putra Malaysia, 43400 Serdang, Selangor, Malaysia

Summary
The rapid development of internet technologies, lead to the growth of Online Social Networks (OSNs). Facebook, Twitter, Google Plus, MySpace, Orkut are well-known examples of online social networks. Although, existence of OSN networks makes the communication easier than ever, it introduces various types of security issues like identity impersonate, privacy-related issues due to losing user account. Online Social Networks (OSNs) provide various security schemes to protect user account, however in many situations such schemes are not adequate and the owners of the accounts find themselves unable to regain control of their accounts. This paper proposes a simple yet reliable security approach that allows users to protect their accounts in online social networks OSNs from unauthorized access. The proposed approach will improve the Quality of Service (QoS) by enhancing the existing security schemes and will considerably mitigate the effects of unauthorized access in online social networks OSNs.

Key words: Online Social Networks (OSNs), Recovery Token, Security, Quality of Service (QoS), Authentication

1. Introduction

The rapid development of internet technologies makes the connection among people much easier through Online Social Networks (OSNs). The web 2.0 technology developments led to forming a kind of communication named as Online Social Networks (OSNs) [1], which allow people to create accounts, setup profiles and share information available on their profile with other users. Facebook, Twitter, Google Plus, MySpace, Orkut are well-known examples of online social networks. (OSNs) .The active users of some Online Social Networks (OSNs) such as Facebook, and twitter almost crossed more than one billion [2] [3].

The main example of social networking websites is Facebook, which was founded on February 2004 and operated by Facebook community [4]. Facebook attracted many users in all around the world and crossed over one billion active users during the month of September 2012, and more than half of whom use on mobile devices [4]. To open an account in Facebook one needs a registration, which can be done with an Email id. The user of Facebook can share information through messages, comments or simply posts information on the wall of the user. Facebook also allows user to post pictures and videos and do chat with the other friends on Facebook.

Facebook has various useful privacy settings and allows its users to set their own privacy policy, which enables the users to control information of their profile and the information shared by them. As other Online Social Networks (OSNs), number of security issues do exist [12]. Facebook security scheme still has certain limitations regarding preventing losing user account. While Facebook provides full privacy policy to the information on the user account, it fails to provide a full protection to user account. It seems that more efforts still required to improve Quality of Service (QoS) provided to its users through enhancing the security scheme.

In this paper, we firstly introduce threats to user account in OSN networks. Then we describe Facebook existing security model as well as point out the limitations in Facebook security model. Finally, we propose a new approach to improve the Quality of Service (QoS) by enhancing the existing security schemes in which a special-use password is introduced. In addition, we make a comparison between Facebook security model and the new enhancement, and analyze the security of the enhancement.

Motivation. The proposed approach addresses the problem of losing ownership of online social network (OSN) user account and inability to access the user account due to hacking. The proposed approach helps users to regain control of their accounts from attackers.

Contributions. We propose an approach to improve (QoS) in (OSNs) networks by enhancing their security schemes; (2) we introduce the notion of recovery password; (3) our approach shows how security schemes in (OSNs) can be enhanced with no or little overhead; (4) we show the feasibility of our approach to protect users accounts from unauthorized access in online social networks (OSNs).

Outline. The remainder of this paper is organized as follows: section 2 gives a summary of the related work. Section 3 lists threats to user account in OSN networks. Existing Security model in Facebook, the most popular OSN, is described in Section 4. Our approach is described in Section 5 showing the implementation and security analysis and Section 6 concludes.

Manuscript received April 5, 2015
Manuscript revised April 20, 2015

2. Related Work

Several studies have discussed the security issues related to Online Social Networks (OSNs). The survey paper in [12] highlighted different security issues in OSNs. The research in [5] suggested that users can set privacy policy to their profile object and control the privacy of information on the account. This can be done by dividing their total number of friends into various groups and set privacy options to each group based on the priority. Grouping of friends was carried out based on clustering technology. The research in [5] focused mainly on user-to-user interactions in social networks only.

With the growth of using third party applications with online social networking websites, the third party applications request the right to access the information from the users in those websites. The research in [1] presented a framework to control the access of third party application to user information. The framework is based on enabling the user to specify the data attributes to be shared with the application and at the same time be able to specify the degree of specificity of the shared attributes.

Other related work has analyzed both privacy risks associated with information disclosure in social networks, and proposed a framework for deriving a "privacy score" to inform the user of the potential risks to their privacy created by their activities and activities with other users within the social network [6]. However the previous researches [1,5,6, 7] concentrated on how to give more security to the data available on user profile. All these privacy and security mechanisms provide protection only to the profile data of the user but not to the entire user account.

The most close work to ours is [11], in which they attempted to enhance the security scheme in Facebook when the user account is temporarily locked. They suggested that Facebook should not verify the originality of the user by verifying the birthdate or identifying the photos of friends. They argue that, most of users especially very important persons (VIP) users do not wish to provide real birthdate in their homepages and put dummy birthdates instead. And after long time of not accessing their accounts it is unlikely that they can remember what birthdate information they provided to Facebook. They advised not to use photos of friend in the originality verification procedure because in many situations it is difficult for the owners of the accounts to recognize properly the correct photos and as a result losing their accounts permanently.

They proposed security approach for verifying the originality of users based on email and mobile phone device instead, however, their approach does not guarantee the security of user account. Their approach only deals with the issue of losing access to the account which is temporarily locked provided that that email and mobile phone are intact. They ignore the events when mobile phone and/or email account have been stolen or compromised.

unlike [11] our approach is comprehensive and can prevent losing access to user account due to hacking. Our approach enables Facebook to verify the originality of account owner in a simple manner.

3. Threats to OSN User Account

There exists number of threats on the authenticity means used in OSNs account including email, mobile phone, login password. Therefore, these threats pose a risk on the ability of the user to access his or her account in OSNs networks and reduce the means available to the user to regain control of the account. It should be noted that being user is unable to prove authenticity due to failing of one or some of authenticity means does not necessarily lead to losing access to the account. However, failing of user to fulfill all authentication requests would render the user account inaccessible. Some of threats are:

- The user forgot username or account password
- The user forgot birthdate registered in his profile
- The user could not recognize photos of friends
- Mobile phone device was stolen and exploited by hacker for hacking user account
- Mobile phone number was temporarily or permanently blocked by network operator
- Mobile phone number changed because of travelling abroad
- The user cannot use the last device from which he/she logged in
- The user forgot the recovery email
- The user forgot recovery email login password
- The recovery email was hacked

4. Facebook Security Model

The most popular Online Social Networks (OSNs) Facebook allows users to create personal profile, post photos, videos, share information and send message to friends. Facebook has various useful privacy settings, which enable the users to control information of their profile and the information shared by them. However, number of security issues do exist [12]. Facebook security scheme still has limitations regarding preventing losing user account. While Facebook provides full privacy policy to the information on the user account, it fails to provide a full protection to user account. It seems that more efforts still required in order to enhance user account security and

protect it from unauthorized access. In the following we discuss the main processes in Facebook security model.

- Forgot password
- Identify the account
- Change general and security settings
- More Security Features

Forgot password. When user forgets the password and clicks on "Forgot password", Facebook website will prompt the user to enter email, mobile phone, username, or full name (Fig. 1).

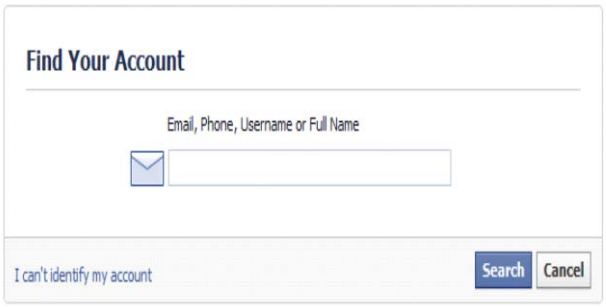

Fig. 1 Forgot Password Screen.

The issues that may arise are:

-Email entered might be already attacked by an attacker, or blocked by Email Service Provider ESP for some reason, thus the user will not be able to receive reset password message.

-Mobile phone number might be changed by the user or blocked by network operator. Furthermore, not all users do register mobile numbers in Facebook account.

-Most of users do not care of username (Facebook URL) and, thus they do not remember username.

-many users tend to use dummy names in Facebook account, and thus they may not be able to remember full name.

Identify your account. If the user could not identify the account and failed to provide correct email or username, Facebook website may prompt him to find a friend**,** who can help by looking at contact or URL. This idea may not succeed since most of users hide their contact information.

Change general and security settings. Facebook allows user to change information in user account profile including password, emails, mobile phone, and username provided that the password is given. This flexibility has a risk as it allows an attacker to change the account authenticity information by providing password only. This hardens the task of the owner to regain control of the account.

More Security Features. Facebook offers more features to securing user account including Login Approvals and Trusted Contacts (Fig. 2). These features still have limitations.

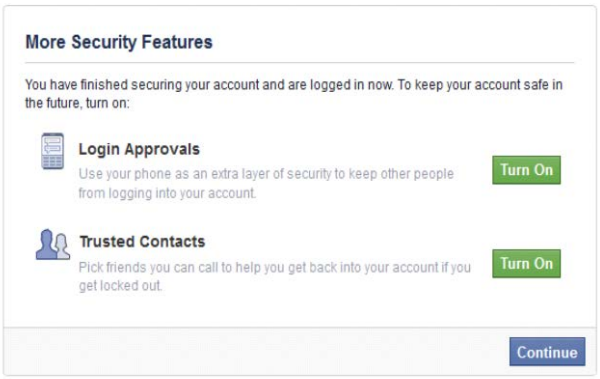

Fig. 2 More Security Features.

Login Approvals uses mobile phone as an extra authentication factor to prove user originality. Facebook allows users to turn "Login Approvals" ON and OFF, provided that password is given. Having the password, an attacker can change mobile phone number and/or turns Login Approvals OFF.

Trusted Contacts cannot be always a reliable mechanism and it is not clear how to regain control of account if the user did not turn this feature ON previously.

In the following we will show the limitations of Facebook security model to handle user account locking and hacking.

4.1 Account is locked

If user account was locked, Facebook prompts the user to authenticate the user originality in the following ways.

- Provide your birthday.
- Identify the photos of friends.
- Try logging into Facebook from a device you have logged in before.

Work in [11] highlighted the limitations of Facebook security model to deal with account locking. Please refer to [11] for more details.

4.2 Account is Hacked

This section shows how Facebook may hinder legitimate users to regain control of their accounts that have been compromised by attackers. The point can be illustrated clearly with the following scenario. If user account was hacked by an attacker, the user will try to regain control of the account through "Forgot Password" procedure. Facebook website then prompts the user to prove the user authenticity (Fig. 3) using:

- Email registered in Facebook account, or

- Mobile device number registered with Facebook account, or
- Username or,
- Full name

Allowing the user to choose any method to prove user originality. Let us now discuss each option available to the user.

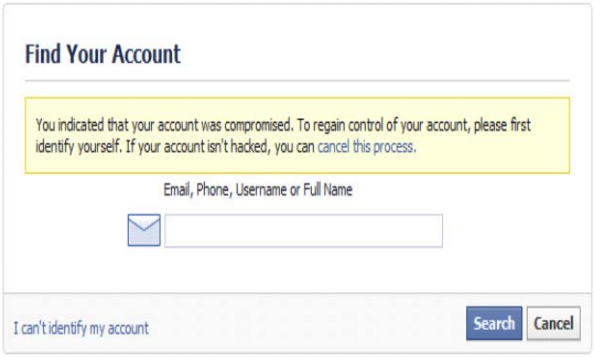

Fig. 3 Identify User .

Case 1- Validation Through Email. If the user decided to regain control of the account through the email, then Facebook website will prompt the user to provide the email registered in Facebook account. If the correct email was entered, Facebook will send a reset password to the provided email enabling the user to reset the password and access the account. It seems an easy but the following examples show that it is possible for the account owner to lose the access to the account due to inability to prove the authenticity through email.

- The user could not remember the correct email, or
- The email entered by user was correct but has already been blocked by Email Service Provider ESP, or
- The email entered by user was correct but has already been hacked by an attacker, or
- The email entered by user was correct but has already been changed in Facebook user profile by an attacker.

As a result, the user will not be able to receive reset password message through email, and thus cannot access Facebook user account.

Case 2- Validation Through Mobile Phone. The user may select mobile phone to prove authenticity to Facebook website, which in turn will prompt the user to provide mobile phone number registered in Facebook account. The Facebook sends SMS verification message or makes a call to the entered mobile number enabling the user to access the account. Some issues may prevent the user to access the account though this method:

- Mobile number has been temporarily or permanently blocked by Network operator, or
- The user has changed mobile number due to travelling abroad, or
- Mobile number entered by the user has been already changed in Facebook user account profile by an attacker.

Case 3- Validation Through Username. Most of users do not care of username (Facebook URL) and, thus they do not remember username. Moreover, it is possible for attacker to change username in user profile.

Case 4- Validation Through Full name. Many users tend to use dummy names in Facebook account, and thus they may not be able to remember full name

5. The Approach

This section presents the proposed security approach to protect the user account in online social networks from unauthorized access. Sections 5.1 and 5.2 give an overview of the proposed approach and present its implementation respectively. The implementation of the proposed security approach is discussed in the context of Facebook, however the proposed approach is applicable to other OSN websites. Finally, Section 5.3 analyzes the security of the proposed approach.

5.1 An Overview

Our approach aims to prevent losing access to user account in online social networks (OSNs) by enhancing existing security models in OSNs. For that end, our approach suggests that OSNs networks should allow each user to be having two passwords instead of one password. The first password (ordinary password) which is used to login to user account while the second one (additional password) is used only in exceptional cases.

The proposed additional password is called *Recovery Token*, which is randomly generated by OSN website while opening an account. *Recovery Token* serves two purposes. On the user side, *Recovery Token* serves as an important recovery tool in the hand of account owner used in emergency cases to regain account control. And on the OSN website, *Recovery Token* serves as trusted identity authentication tool to prove the originality of the user. Having said that, we know *Recovery Token* cannot be used in normal login process but would be exclusively dedicated to recover user account and used in other processes that affect account ownership.

In order to prevent losing access to user account, *Recovery Token* scheme should be given the highest priority above

all other authentication methods to access user account. Several facts support this assumption:

First, the task assigned to *Recovery Token* to recover the account makes it very important to the account owner, and thus it is assumed that the owner would give more attention to *Recovery Token* and keep it in safe place. It would be much difficult for an attacker to know the *Recovery Token* as it is stored in safe place, and thus cannot impersonate the identity of the account owner;

Second, as the *Recovery Token* is randomly generated by OSN website, it would be much harder for an attacker to guess it, even if the attacker has a knowledge about the user and his logic in creating passwords;

Third, as the *Recovery Token* is infrequently used, utilized only for special purposes and kept away from prying eyes, the possibility of an attacker to steal it through key loggers and other spyware is very small.

5.2 Implementation

We present the implementation of the proposed approach focusing on the newly introduced password (*Recovery Token*). Number of processes can be performed on *Recovery Token* during Facebook user account life cycle. The discussion first highlights the requirements of the *Recovery Token*.

Recovery Token Requirements. To ensure the reliability of the proposed mechanism, *Recovery Token* must be random, unpredictable, and cannot be sub sequentially reliable reproduced [8]. It should not be shared and must be kept securely in safe place. *Recovery Token* should be given the highest priority over all other user authenticity proving mechanisms to recovering access to the account.

5.2.1 Opening User Account

When internet user wishes to register and open an account in Facebook, *Recovery Token* is generated as a part of opening account process.

Generation Recovery Token. After completing account registration process and the correctness of the provided information is verified, Facebook process generates the *Recovery Token* and prompts the user to keep the *Recovery Token* in safe place and to use it only for recovery purpose.

5.2.2 Normal Access to User Account

During the life cycle of Facebook user account, the account owner may need to perform number of processes including: *Recovery Token* replacement, *Recovery Token* reporting, and obtaining new *Recovery Token*.

Replacing* Recovery *Token. If user suspected a leakage of *Recovery Token*, he or she may request new *Recovery Token* and replacing the existing one**.** To get a new token, OSN website (eg., Facebook) prompts the user to provide current *Recovery Token* and then to prove user authenticity through email and mobile phone as well.

Report of Missing Recovery Token. The user may forget the *Recovery Token*. Losing *Recovery Token* should not increase opportunities of compromising user account unless it falls in the hands of an attacker. But losing the *Recovery Token* will reduce the opportunities of recovering the account in absence of other verification mechanisms (Email, mobile phone, etc.). If our fear comes true and the user lost and misplaced the invaluable token, there should be existing a mechanism to handle this case. The user can report lost *Recovery Token* to OSN website and obtains new *Recovery Token* under certain conditions.

Obtaining new Recovery Token. After reported of lost Token, the user may go into a process to obtain a new token for the account. because *Recovery Token* is crucial to regain control of user account, special attention must be paid into this process. The online social network OSN website prompts the user to:

1. prove the authenticity through email; and
2. prove the authenticity through mobile device; and
3. enter the first password used by user when the account was opened; or
4. try logging into Facebook from a device the user has logged in before registered email, mobile device and password have been changed.

Points 3 and 4 are precaution steps to prevent attackers from impersonating the identity of legitimate uses.

5.2.3 Inability to Access User Account

The *Recovery Token* plays an important role when user loses access to the account.

Recovering User Account. Number of threats (Section 3) may pose a risk on Facebook user account rendering it inaccessible (Sections 4.1 and 4.2). The worst case occurs when user fails to access both Facebook account and authenticity verification factors including email and mobile. In this case *Recovery Token* becomes the only available option for user to recover the account.

5.3 Security Analysis

We analyze the resilience of our approach against a number of attacks. We show that hacking one or all authentication factors cannot prevent the owner to use *Recovery Token* regain the control of account. Furthermore, we show that an attacker cannot carry out impersonation attacks. We will compare our security approach with Facebook security model.

-Hacking Email Used in Facebook Account. Facebook security model allows users to regain account control

through email or mobile phone. Let us consider the following two scenarios. An attacker hacked the email registered in Facebook account and attempts to compromise Facebook account impersonating user identity. The attacker follows 'forgot the password' procedure and enters the email to receive the reset password message from Facebook website. Once the attacker receives the new password, the account is compromised and the attacker can take control of the account and change information in user profile.

Our solution can mitigate this impersonation attack and allows the user to regain the control of the account through the *Recovery Token*.

-Compromising Mobile Phone Used in Facebook Account. If an attacker gets a possibility to access user mobile phone and tries to login to user account. Following "forgot the password' procedure the attacker enters the mobile phone number impersonate user identity and receives the access code from Facebook website. Once the attacker receives the access code, the account is compromised and the attacker takes the control of the account.

Our solution can protect user account from such impersonation attack and allows the user to regain the control of the account through the *Recovery Token*.

It should be noted that, *the Recovery Token* serves as another protection layer for user account. On the other side, using the *Recovery Token* would make it easy for the account owner to bypass traditional verification process and regain the control of the account.

-Unauthorized Changes to Profile Settings. Facebook allows users to change information in their account profile including: password, email, mobile phone, username provided that the password is given. Facebook also allows users to change security features like Login Approvals and trusted contacts. This way, it would be very easy for an attacker to change the account authentication information if the attacker already got the password by key loggers, spyware or any other means. On the other side, it would be very hard to the account owner to regain account control if information has been illegally changed by an attacker.

Our solution can protect user account from unauthorized changes attack by allowing OSN user to regain the control of the account, and thus discards all unauthorized changes have been made to user profile. The user can provide the *Recovery Token* and regain the control of the account.

-Losing account under the threat of force. In certain circumstances, the user may be forced to hand over account password to an adversary under the threat of force. After taking the control of user account, the attacker may change the login password as well as information in user account profile. In Facebook existing security model the user will lose access to the account and becomes unable to regain control of the account. Unlike Facebook security model, our solution can help the legitimate user to regain the control of the account with help of *Recovery Token*.

-Losing account because of untrusted employee. A company manager may authorize an employee to administer Facebook account in the name of company. Having the administrative privileges, the employee can change information in company Facebook account. In case it could not retrieve the password from the employee for any reason, the company will lose the access to the account. Unlike Facebook security model, our solution can help the legitimate user to regain the control of the account with help of *Recovery Token*.

-Hacking Facebook User Account. In Facebook existing security model, when an attacker compromises user account and changes profile information used in authentication process, it would be very difficult for the owner to regain control of the account. And it would be almost impossible for the owner to regain the control of the account if the email used with Facebook account was hacked and the mobile phone number was changed, for example.

No matter how the account owner loses the access to the account, by using *Recovery Token* the owner can regain the control of the account even if all authentication means are compromised.

6. Conclusion

In this paper, we propose an approach that allows users to protect their accounts in online social networks OSNs from unauthorized access. Our approach mitigates the security risks resulting from unauthorized access by introducing an additional protection layer, *Recovery Token*. The proposed approach does not dedicated infrastructure and poses no overhead. The approach improves the Quality of Service (QoS) by enhancing the existing security schemes and provides users with an adequate assurance of account protection. The advantages of our solution are analyzed in the context of Facebook as an example. We believe the proposed approach is applicable and can be generalized to enhance security schemes in all other online social networks as well as Email Service Providers (ESPs) websites like Gmail, Yahoo, Hotmail, etc. Further research should investigate techniques to improve the resistance of OSNs networks that implement *Recovery Token* to impersonation attacks.

7. References

[1] Mohamed Shehab a, Anna Squicciarini b, Gail-Joon Ahn c, Irini Kokkinou “Access control for online social networks third party applications” Elsevier- Computers

& Security 31 (2012) 897-911.
[2] Facebook, Facebook Statistics, March 2011. <http://www.Facebook.com/press>.
[3] Twitter, Twitter Numbers, March 2011. <http://blog.twitter.com/2011/03/numbers.html>.
[4] Facebook, http://en.wikipedia.org/wiki/Facebook
[5] Gorrell P. Cheek, Mohamed Shehab "Policy-by-Example for Online Social Networks" SACMATO 12, JUNE 20-22, 2012 NEWARK, NEW JERSY, USA, ACM, YEAR 2012.
[6] Liu Kun, Terzi Evimaria. A framework for computing the privacy scores of users in online social networks. In: ICDM 2009, the ninth IEEE international conference on data mining, pp.288e297; December 2009.
[7] H. Kim, J. Tang, R. Anderson, Social authentication: harder than it looks, in: Proceedings of the 2012 Cryptography and Data Security Conference, 2012.
[8] M. Gjoka, M. Kurant, C.T. Butts, A. Markopoulou, Walking in Facebook: a case study of unbiased sampling of osns, in: Proceedings of IEEE INFOCOM '10, San Diego, CA, 2010.
[9] A.S. Yuksel, M. E. Yuksel, and A. H. Zaim. An approach for protecting privacy on social networks. In Proceedings of 5th International Conference on Systems and Networks Communications, Washington, DC, USA, 2010. IEEE Computer Society.
[10] A. Acquisti and J. Grossklags. Privacy and rationality in individual decision making. IEEE Security and Privacy, 3(1):26{33}, 2005.
[11] M. Milton Joe, Dr. B. Ramakrishnan, Dr. R.S. Shaji "Prevention of Losing User Account by Enhancing Security Module: A Facebook Case", Journal of Emerging Technologies in Web Intelligence, Vol. 5, No. 3, August 2013, Page No: 247-256.
[12] M. Milton Joe, Dr. B. Ramakrishnan "A Survey of Various Security Issues in Online Social Networks", International Journal of Computer Networks and Applications Vol. 1, No. 1, November - December (2014), Page No:11-14.

Abdulraman Muthana received his B.Sc in Computer Science from Mosul University, Iraq, M.Sc in Computer Applications from Bangalore University, India and PhD in Information Security from University Putra Malaysia in. His research areas include information security, smartphone security, network security, software security. He is now an Assistant Professor in Faculty of Computer Science and Information Systems, Thamar University, Yemen.

Abdul Azim Abdul Ghani received his M.S. degrees in Computer Science from University of Miami, Florida, U.S.A in 1984 and Ph.D. in Computer Science from University of Strathclyde, Scotland, U.K in 1993. His research areas include software engineering, software metric, software quality, software testing. He is now a professor in Department of Software Engineering and Information System, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia.

Ramlan Mahmod holds a PhD from University of Bradford, United Kingdom. Currently, he is now Professor and the Dean of Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, His research area are artificial intelligence and Information Security.