International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 04 | Apr -2017 www.irjet.net p-ISSN: 2395-0072

Security of Trustee Based Social Authentication

Prof. S.N. Maitri[1], Mayur Agnihotri [2], Ashutosh Borde[3], Pratik Salvi[4]

[1] H.O.D., Dept. of ComputerEngg., Trinity Academy Of Engineering, Pune.
[2,3,4] Student, Trinity Academy Of Engineering, Pune.

Abstract – *Now-a-days, the trend is to authenticate users with the help of their friends. This technique is commonly known as 'trustee-based social authentication'. This method is most likely destined to be successful as compared to its competitors. It involves a user who selects a few trusted associates from his friend list. These trusted associates are known as 'trustees'. When the user wishes to recover his account, the service provider sends verification codes which are unique in nature to the user's trustees. A recovery threshold (k) is set and when the user obtains these k verification codes from his trustees, he is directed to reset his password. Access is given to the account of the user by using some backup authentication mechanisms. Here, we propose to introduce a pioneering framework of attacks, which we will refer to as 'forest fire attacks' wherein compromised users are obtained in small number by the attacker and iterative attacks are done on the remaining users by using the trustee networks.*

Key Words: **Social authentication, security model, backup authentication, forest fire attacks.**

1. INTRODUCTION

Authentication has become important for organizations to provide accuracy and consistency in security against thefts and terrorism. Web services such as Gmail, Facebook, and online banking very often use passwords for authentication purposes but they come across two serious issues like: users forgetting passwords, and passwords being changed and, therefore, accounts being compromised by the attackers. Hence a backup authentication mechanism is often provided by these web services to the users to help them redeem access to their accounts. Unfortunately, now a-days, widely used backup authentication mechanisms such as alternate email addresses and security questions are vulnerable to attacks. Security questions can be easily speculated and phished. The user may even forget the answers to the particular security questions. Also, previously set alternate email address may expire with time or upon change of institutions. Hence, it is essential to design a dependable and steadfast backup authentication mechanism.

In fact, our experimental results show that setting the recovery threshold to be four could better balance between security and usability.

Let us have a detailed look about the working of trustee-based social authentication system. Here we have a social network of different users and then we will introduce a trustee network for a user.
Here we will see two phases:

1.1 Registration Phase

The system will help to select the user with trustees in this phase. The user is proven to be genuine with help of a password, and then the user or the service provider will select a few friends (eg.3) as the user's trustees. These friends are the user's friends from the social network.

1.2 Recovery Phase

In this phase if the user forgets password or the users account is compromised and the password is changed by the attacker. The user can recover the password using his/her trustees.

The service provider will help in the password recovery. The user will send an account recovery request to the service provider along with her user-name/email address. The service provider will authenticate the user's trustees and send verification codes to the trustees. The user can obtain the verification codes from the trustees via mails or call them or meet them in person. If the user obtains a recovery threshold (the minimum number of codes required for authentication) of the verification codes and send them to the service provider, then the user is considered genuine and is directed to reset his/her password. As the user can forget the trustees the service provider will help the user to remember his/her trustees.
Let us consider Facebook's Trustee-Based Social Authentication: Facebook's trustee-based social authentication system is called Trusted Friends, whose improved version is Trusted Contacts. In the Registration Phase of Facebook's Trustee-Based Social Authentication, a user selects three to five friends from his/her friend list as trustees. The recovery threshold is also set to be three. Facebook does not remind a user of his or her trustees, but it asks the user to type in the names of his or her trustees instead. However, once the user gets one trustee correctly, Facebook will remind him or her of the remaining trustees. We will show that the service provider will put a constraint on the user to select a specific number of trustees such that no user can be a trustee of too many other users. This helps in giving more security.
In fact, our experimental results show that setting the recovery threshold to be four could better balance between security and usability.

2. ATTACK STRATEGIES

Here, we will consider the attackers background knowledge and then a sequence of attacks which we will call the Forest Fire attacks.
We first we accept that the attacker know the trustee network. The practicality of the model is supported by two factors. First, attackers are able to obtain the users usernames (string of letters, digits, and special characters).. Second, as the users cannot remember their own trustees. Therefore, a usable trustee-based social authentication system helps the user to recollect their trustees. As we know that an account recovery request only requires a username to be sent to the service provider. As a result, an attacker could send account recovery requests with the obtained usernames to the service provider which reminds the attacker of the trustees of each user.

3. DEFENSE STRATEGIES

We can discuss defense strategies in 3 ways, i.e. hiding trustee networks from attackers, mitigating spoofing attacks, and constraining the selection of trustees.

A. Hiding Trustee Networks:

In order to prevent the attacker from getting the trustee network we need to take some measures which are necessary against the forest fire attacks. It is necessary for the user to remember his/her trustees in order to retrieve the verification codes from the service provider.

Another method is that the service provider directly sends the verification codes to the trustees of the user when the service provider receives the account recovery request from the user. Here the user is not needed to remember his/her trustees. So it becomes hard for the attacker to obtain trustee network. The trustees are needed to send the verification codes to the user. This method is unreliable and will annoy both user and the trustee, also the trustee will forget that they are the trustees of the user and take the verification codes as spam and not share with anyone. Also if this is the case the attacker will frequently send recovery request to the service provider ,where there will be frequent sending of the verification codes to the trustees and the user which will annoy them both and the trustees may start to think that the verification codes are spam and not share the verification code when its needed.

B. Mitigating Spoofing Attacks:

In order to prevent attacking in forest fire attack is to remind the trustees to not share the verification codes through messages. Now days the social authentication systems are using the method of mitigating spoofing attacks. Here we can ask the user in return that why are they requesting the verification codes and encourage the trustees to share the verification code with the user via phone calls or meeting the user in person. However the attacker can still obtain the verification codes via message-based spoofing which will be an interesting future work to design a system to reduce spoofing probability.

C. Constraining Trustee Selections:

We use a strategy to constraint trustee selection, which help in defending against forest fire attacks. We take into consideration both local trustee selection strategies and global trustee selection strategies.

A local trustee selection strategy is based on a user's local social network structure while a global selection strategy is based on the entire social network structure.
Here the service provider will put a constraint on the user to select a specific number of trustees such that no user can be a trustee of too many other users. This helps in giving more security and prevents or makes it hard for the attacker to obtain the trustee network.

4. ARCHITECTURE

First and foremost, the user is required to provide a list of friends to the service provider to commence the registration process. It is also obligatory that the user select his trustees or, in some cases, the service provider does this job for the user. When the user forgets the password or if the attacker compromises the user's account, the user sends a request for password recovery. This leads to the service provider sending verification codes to the trustees. The trustees then send the obtained verification codes to the user. Eventually, the user is able to reset his/her password. The overall framework of the method is shown in Fig.1.

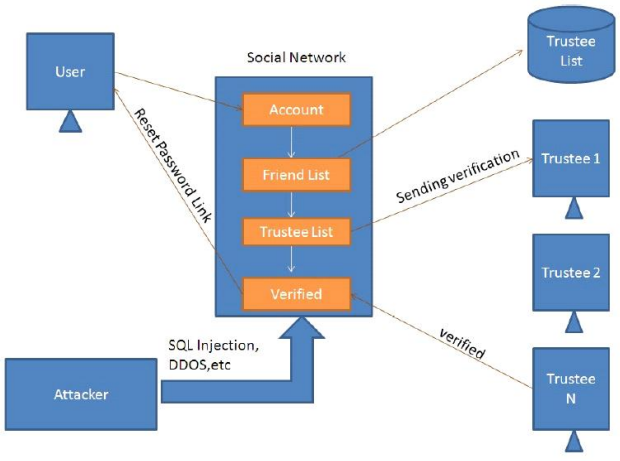

Fig -1: Workflow for authentication

1. **Registration Phase:**

a) User's Login

The user has to create an account with a unique e-mail id. Once an e-mail id is registered with the service provider, the same cannot be used for creating another account.

b) **Send/Confirm friend requests**
User can send and receive friend requests to and from the other users.

c) **Trustee Selection**
Here, trustees are selected from the user's friend list. If the user wants to alter his list of trustees, he can use the reset option available to reselect his or her trustees. This will be updated at the server automatically.

2. Recovery Phase:

a) Identify Trustees
In this step, it is mandatory that the user select at least one trustee name from his/her trustee list in order to proceed further with the recovery process. If the user selects the correct trustee, the system automatically displays the trustee name.

b) Reset Password
This is the final step wherein the user is allowed to reset his or her password in case of loss of password or e-mail id. Fig. 4. represents the architecture of trustee based authentication and its work flow in Fig.1.

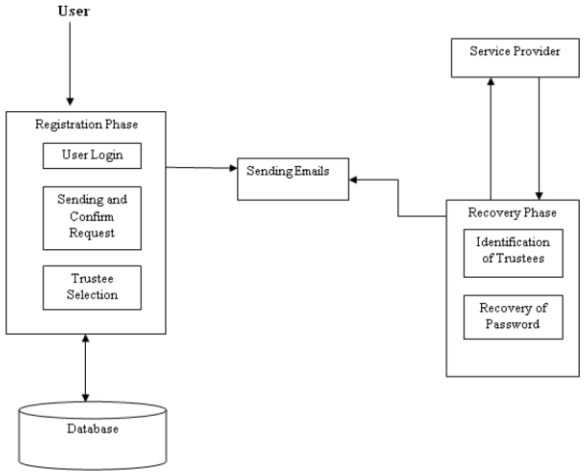

Fig -2: Architecture of Trustee-Based Authentication System

5. MODULES DESCRIPTION

Here is the brief study of the modules involved in the system.
I. User Registration
II. Add Friends
III. Announce Trusted Users
IV. Set Recovery Threshold
V. Set Time Limit for Verification Code Recovery

I. User Registration
Details of the user like User Name, User ID, Address, E-mail ID and Passwords are saved and registered. These are stored in the 'Users' table.

II. Add Friends
Details of the user's friends in his social network are saved in the 'Friends' table. There is no constraint on the number of friends a user can add.

III. Announce Trusted Users
The trusted users' list is added to the selected user. The user now selects his trustees which he thinks are the most trustworthy contacts from his friend list. The list is saved in the 'User Trustee' table. There can be a limit on the number of selected trustees for reliability purposes.

IV. Set Recovery Threshold
The count on the number of trustees is set so that in the event of recovering the password, the verification codes can be sent hassle-free.

V. Set Time Limit for Verification Code Recovery
There is a time limit set in hours for the retrieval of the verification codes from the trustees and submission of the same to the service provider, else those codes will be deemed invalid and the user will have to request the codes a second time. The set time limit value is stored in the table named 'Time Limit'.

VI. User Compromisation Using Forest Fire Attack
The forest fire attack is implemented. Here to compromise the node 'U', the Attacker User 'A' iteratively attacks other users by making use of the "trusted contacts" or the trustee network.

VII. Block User Compromisation
If the user trying to regain access to his account asks one trustee for his verification code, all the other trustees receive an alert message regarding the incident. Now the trustee can communicate with the original user about the password recovery mechanism via a private channel. The time limit is monitored simultaneously so that recovery beyond the set time limit is forbidden.

6. RELATED WORK

As authentication processes involve friends, social authentication is categorized into trustee-based and knowledge-based social authentications. In trustee-based social authentications, the user's friends are considered as trustees and are used in authenticating the user whereas in knowledge-based social authentication, questions regarding the trustees or friends are asked; hence, there is no direct involvement of friends.

1. Trustee-Based Social Authentication Systems:

Authentication is mainly based on three factors: something you know (e.g. password), something you have (e.g. RSASecurID), and something you are (e.g. fingerprint).
Brainard et al. brought a fourth factor in the market, i.e., somebody you know, which can be used in the authentication process which we call trustee-based social authentication. It was earlier considered as the main authentication purpose but then it was adapted as a backup authenticator. A prototype was designed by Schechter et al. which was used by Microsoft's Windows Live ID system as well as by Facebook.

2. Knowledge-Based Social Authentication Systems:
This type of authentication focuses on something that you know.

Facebook recently started a photo based social authentication system where Facebook asks to name a few friends by randomly showing the user the photos of his/her friends. But this system is reliable only if the user has the required knowledge about the friends shown in the photo. However, recent studies doubt the reliability of these authentication systems as they are prone to automatic face detection technique attacks, to name a few.

7. CONCLUSION AND FUTURE WORK

We have presented a systematic study about the security of trustee based social authentication, including the forest-fire attacks, a probabilistic model to normalize the threats of forest-fire attacks and their costs for attackers, security and defense strategies along with attack-ordering, algorithms and their efficient implementation. Furthermore, we found out that in order to better the balance between security and usability; the recovery threshold should be set to 3. The rationale behind the design will be analyzed, especially on the scalability and accuracy issues, in order to show how our system can tackle a huge number of trustee networks. The complexity of our approach is low and it can be used in reality without any hassle.

A few future directions includes,

1. Evaluating forest fire attacks on real social authentication systems such as Facebook's Trusted Contacts,
2. Designing of new attack and defense strategies.
3. Optimizing forest fire attacks in a given time.
4. Design a better user interface in order to reduce spoofing probability.

ACKNOWLEDGEMENT

We would like to take this opportunity to thank all the people who were part of this project in numerous ways, people who gave an un-ending support right from the initial stage. In particular, we would like to thank our Project guide Prof. S. N. Maitri, who gave her co-operation timely and precious guidance without which this project would not have been a successful.

REFERENCES

[1] N. Z. Gong and D. Wang, \On the security of trustee-based social authentications," IEEE TIFS, vol. 9, no. 8, 2014.
[2] L. A. Adamic and E. Adar, "Friends and neighbors on the web", Social Netw., vol. 25, no. 3, pp. 211230, 2003.
[3] Yu, L., Wang, S. A. and Lai, K. K. 2008. Credit risk assessment with a multistage neural network ensemble learning approach. Expert systems with applications. vol. 34. pp. 1434-1444.
[4] J. Bonneau and S. Preibusch, "The password thicket: Technical and market failures in human authentication on the web", in Proc.9thWork-shop Econ. Inform. Security (WEIS), 2010.
[5] J. Brainard,A. Juels, R. Rivest, M. Szydlo, and M. Yung, "Fourth-factor authentication: Somebody you know", in Proc. 13th ACM Conf.Comput. Commun. Security (CCS), 2006.
[6] J. Podd, J.Bunnell, and R. Henderson, "Cost-e_ective computer security: Cognitive and associative passwords", in Proc. 6th Australian Conf.Comput.-Human Interact.,1996.
[7] A. Rice. (2011, Jan.). "Facebooks Knowledge-Based Social Authentication [Online]". Available: http:// blog.facebook.com/blog.php?post=486790652130.
[8] (2013, May). "Facebooks Trusted Contacts [Online]". Available:goo.gl/xHmVHA
[9] (2011, Oct.). "Facebooks Trusted Friends [Online]". Available: goo.gl/KdyYXJ
[10] S. Schechter, A. J. B. Brush, and S. Egelman, "Its no secret: Measuring the security and reliability of authentication via secret questions", in Proc.IEEE Symp. Security Privacy, May 2009, pp. 375390.
[11] A. Mislove, H. S. Koppula, K. P. Gummadi, P. Druschel, and B. Bhattacharjee, "Growth of the Flickr social network", in Proc. 1st Workshop Online Social Netw. (WOSN), 2008.
[12] S. Yardi, N. Feamster, and A. Bruckman, "Photo-based authentication using social networks," in *Proc. 1st Workshop Online Social Netw.(WOSN)*, 2008.