Scientific Journal of Impact Factor (SJIF): 4.14

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 3, Issue 11, November -2016

Security of Trustee-Based Social Authentications

Mayur Agnihotri[1] , Pratik Salvi[2], Ashutosh Borde[3]

[1]*Computer Department, Trinity Academy Of Engineering, Pune.*
[2]*Computer Department, Trinity Academy Of Engineering, Pune.*
[3]*Computer Department, Trinity Academy Of Engineering, Pune.*

Abstract — *Now a days, the trend is to authenticate users through their friends. This technique is commonly known as 'trustee-based social authentication'. This method seems to have a bright future amongst the various backup authentication mechanisms. This system 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. We propose to establish a probabilistic model to normalize the threats of forest fire attacks and their costs for attackers. We also introduce various defense strategies and apply our framework to broadly assess various palpable attacks and defense strategies.*

Keywords- *Social authentication, security model, backup authentication, forest fire attacks.*

I. 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.

II. LITERATURE SURVEY

Below we are going to compare some of the authentication techniques used for security purposes. Authentication methods which are divergent from one another are considered. Knowledge based and trustee based authentication are a part of Backup authentication. Lawrence O'Gorman [Comparing passwords, token and biometrics for User Authentication] has studied the authenticators like the passwords, security tokens and biometrics and differentiated their respective combinations. There are number of algorithms used in this paper like an encryption algorithm, Hash algorithm and Biometric algorithm. Whereas Ariel Rabkin [Personal knowledge questions for fallback authentication: Security questions in the era of Facebook] explains that some of the private bankings websites the password recover mechanisms depends on weak security backup authentications like the security questions with low usability. There are some photo based authentication methods which is explained by Nick Feamster[Photo-Based Authentication using Social Networks] where photographs are used for authentication purpose in real world social network where there may be problems regarding the real world social networks. Many times the users forgets their passwords and need some backup authentication to recover their access to the account which is explained by Stuart Schechter[It's Not What You Know, But Who You Know] where the users are needed to remember who their trustees are. There are various threats when it comes to social networks and their respective challenges to provide some solutions to it which is explained by Racha Ajami[Security Challenges and Approaches in Online Social Networks: A Survey] where the drawbacks is that there is in consistency to what can be revealed by the attacker of the user. Iasonas Polakis[All Your Face Are Belong to Us: Breaking Facebook's Social Authentication] is another author who did a detailed study of the threats and the ordering of an attacker to gain the information and the challenges to overcome them. Algorithm he used is Face recognition algorithm for the security purpose.

III. MODULE DESCRIPTION

3.1. Trustee-Based Social Authentication Module:

The aim here is to authorize the users who are the communicating entities to establish a level of trust and then flourish in a mutual authentication using a scheme suitable for low-resource devices in smart environments. The variation in our trustee module is that it uses a precise approach to calculate trust in distinct situations, and incorporate a human-based feature for trust feedback, which is user rating. Authenticating users with the help of their friends (i.e., trustee-based social authentication) has been considered as an encouraging backup authentication mechanism. In a system, a user selects a few trustees from the user's friends list. When the user wants to recover the account, the service provider sends unique verification codes to the user's trustees. When the user obtains at least *k* (i.e., recovery threshold) verification codes from the trustees, they are directed to reset his or her password.

3.2. Security Module:

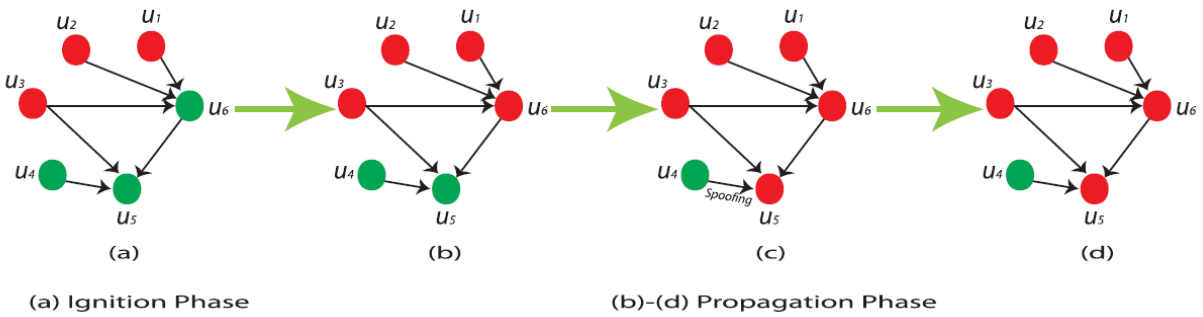
Authentication is of utmost importance when it comes to providing security to a user's account and forestalling spoofing messages from vandalizing one's online status. What would happen if someone hacked your account and sent a phishing email from your mail? You will have a big pile of mess to clean up (angry recipients of your email and spam complaints resulting from it) so as to restore your reputation. Hence, we can see that the users' security, in trustee-based social authentication is interconnected, i.e., if a user's trustees are compromised, then the user will eventually be compromised. Based on this key observation, we propose a new probabilistic security model to deduce the expected number of users that can be compromised by an attacker. We will also instigate various attack and defence strategies and use the security model on real-world social networks.

3.3. Backup Authentication Module:

A user in the system is associated with a few trustees selected from his friend list. When he wants to recoup access to his account, the service provider sends unique verification codes to all his trustees. To be able to be directed to reset his password, the user must obtain at least *k* (i.e., recovery threshold) number of verification codes from his trustees. If in case the user forgets his password or his account gets hacked, each of the selected trustees will be able to get a verification code for him. Using these security codes, he can recover his account.

3.4. Forest Fire Attack:

In a forest fire attack, phishing and guessing are the two traditional methods to compromise some users (are also called 'seed users'), and then the attacker iteratively attacks other users by making use of the "trusted contacts" or the trustee network. This module consists of two phases:



3.4.1. Ignition Phase:

In this phase, the goal of an attacker is to obtain a small number of jeopardized users, also called as the 'seed users'. They use traditional methods like phishing, statistical guessing, and password database leaks.

3.4.2. Propagation Phase:

After the Ignition phase, the attacker gains the seed users and thereafter repeatedly attacks other users. In each action known as 'attack iteration', the attacker executes one 'attack trial' to each of the uncompromised users. This attack trial is done as per the some 'attack ordering'. Consider an attack trial being conducted on a user, say, 'U'. During this, the attacker sends an account recovery request with username of U to the service provider. The service provider then issues unique verification codes to all of U's trustees. The attacker aims to gather verification code from at least one trustee. If even one trustee of U is compromised then the attacker can jeopardize the user eventually. Another thing that the attacker can do is impersonate U and send a spoofing message to each of U's uncompromised trustees to seek the verification code.

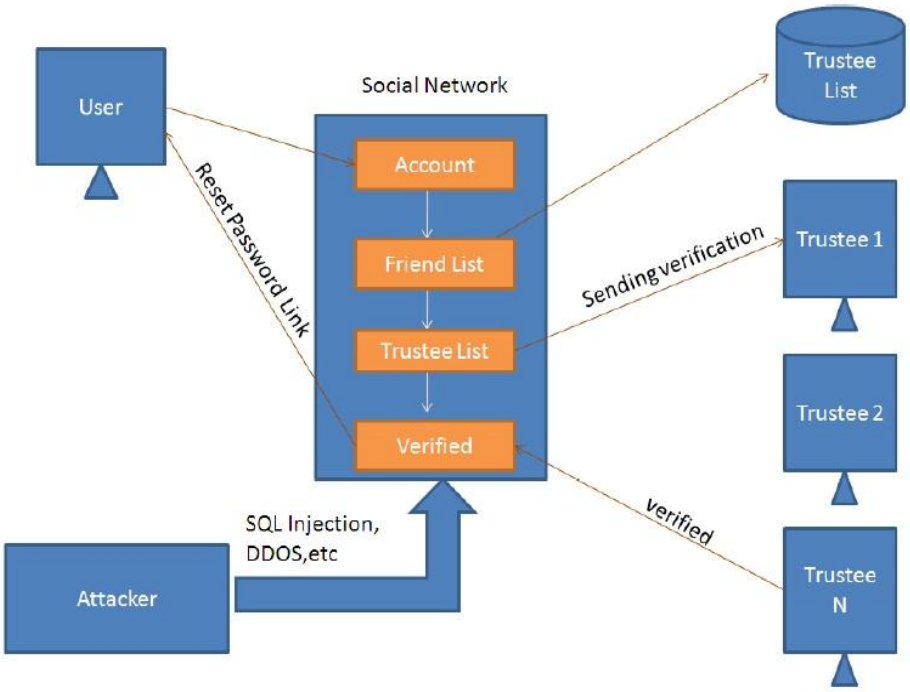
Algorithm 1 Our Model of Forest Fire Attacks

Input: G_T, k, $p_{(t)s}(v, u)$, n_s, n, S, O, c_e, c_I, and $p_{(t)r}(u)$.
Output: $n_c(G_T, k, n_s, n, S, O)$, $c(G_T, k, n_s, n, S, O)$.
begin
//Selecting seed users in the Ignition Phase.
$S \longleftarrow S(G_T, n_s)$
//Calculating the compromise probabilities.
//Ignition Phase.
for $u \in V_T$ **do**
if $u \in S$ **then**
$p_{c}^{(0)}(u) \longleftarrow 1$
else
$p_{c}^{(0)}(u) \longleftarrow 0$
end
$p_{a}^{(0)}(u) \longleftarrow p_{c}^{(0)}(u)$
end
//Propagation Phase.
$t \longleftarrow 1$
$C \longleftarrow 0$
while $t \leq n$ **do**
//Constructing an attack ordering.
$O_{(t)} \longleftarrow O(G_T, p_{a}^{(t-1)}(V_T))$
for $i = 0$ *to* $O_{(t)}.size() - 1$ **do**
$u \longleftarrow O_{(t)}[i]$
Apply Equation 4 to u.
$p_{a}^{(t)}(u) \longleftarrow 1 - (1 - p_{a}^{(t-1)}(u))(1 - p_{c}^{(t)}(u))$
$p_{a}^{(t)}(u) \longleftarrow (1 - p_{r}^{(t)}(u))p_{a}^{(t)}(u)$
$c_{(t)}(u) \longleftarrow$ Apply Equation 10
$C \longleftarrow C + c_{(t)}(u)$
end
$t \longleftarrow t + 1$
end
//The expected number of compromised users.
$n_c(G_T, k, n_s, n, S, O) \longleftarrow \sum_{u \in V_T} p_{a}^{(n)}(u)$
//The expected cost.
$c(G_T, k, n_s, n, S, O) \longleftarrow c_I + c_e C$
return $n_c(G_T, k, n_s, n, S, O)$, $c(G_T, k, n_s, n, S, O)$
end

III. ARCHITECTURE

For registration user has to give a list of close companions to the service provider. A list of trustees can be selected by the service provider or the user. When the system is attacked by an attacker, an email is sent to the trustees of the user from a service provider. These email consist of a verification code which can be used for the authentication of the user. After which the user is able to reset the password.

The overall framework of the method is shown in figure below:



IV. CONCLUSION

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 defence 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 analysed, 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.

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.

