Scientific Journal Impact Factor (SJIF): 1.711
International Journal of Modern Trends in Engineering and Research
IJMTER
ISSN (ONLINE) : 2349 - 9745
ISSN (PRINT) : 2393 - 8161

Multi Level Trustee based Social Authentication for Internet Services

Mrs. J. Vinodhini., II ME CSE
Mrs. P. Banumathi M.E., Assistant Professor,
Mr. T.P. Jayakumar. M.E., (Ph.D)., AP/HOD/CSE
Maharaja Engineering College for Women, Perundurai, Tamilnadu, India

Abstract-Internet provides different types of services to the users. Electronic mail, chat, photo sharing and social network services are provided by the Internet community. Most of the Internet services perform the user authentication using passwords. Password forgets and password changed by attackers requires user verification with security questions and alternate e-mail account support. Backup authentication mechanisms such as security questions and alternate email addresses are insecure or unreliable or both

Friends based verification is one of the backup authentication mechanism. A user in this system is associated with a few trustees that were selected from the user's friends. When the user wants to regain access to the account, the service provider sends different verification codes to the user's trustees. The user must obtain at least k verification codes from the trustees before being directed to reset his or her password. Forest fire attacks are applied on the trustee based social authentication scheme. In forest fire attacks an attacker initially obtains a small number of compromised users and then the attacker iteratively attacks the rest of users by exploiting trustee-based social authentications. A probabilistic model is constructed to formalize the threats of forest fire attacks and their costs for attackers. Various defense strategies are used to verify the forest fire attacks. The framework is applied to extensively evaluate various concrete attack and defense strategies using three real-world social network datasets.

The forest fire attack handling mechanism is enhanced with time bounded verification strategies. Two level trustee based verification model can be introduced to improve the social authentication process. Multiple service based authentication can be used in the attack defending process.

I. Introduction

A social approach to last-resort authentication As long as websites authenticate users via credentials that are either memorized or stored, users will inevitably forget or lose them. The 'secret' personal questions and alternate email addresses currently used for backup authentication by web mail providers are unfortunately unreliable. For personal questions, prior and concurrent research has shown that users forget their answers and their acquaintances may be able to guess them. An account holder who tries to authenticate via an alternate email address may find that the configured address expired upon a change of job, school, or Internet service provider [8]. As other websites rely on email addresses to authenticate their account holders when passwords fail, it is especially important for us and other webmail providers to have a secure and reliable authentication mechanism of last resort.

We thus designed and built a new backup authentication mechanism of last resort and studied its performance by making it appear to be part of Windows Live ID. The mechanism uses social authentication, in which account holders initially appoint and later rely on account trustees to help them authenticate. To regain access to their accounts, account holders contact their trustees by phone or in person, so that their trustees may recognize them by their appearance or voice. A trustee who recognizes an account holder may provide him or her with an account-recovery code. An account holder must present a sufficient number of these codes to authenticate. The overall success of an authentication mechanism dependson four important measurement categories:

Setup and Maintenance Costs:

The time or effort required of the account holder to configure or reconfigure the authentication mechanism

Efficiency:

The time or effort required of the account holder each time he or she authenticates to the system

Reliability:

The likelihood that the account holder can successfully authenticate his or her identity

Security:

The time or effort required to impersonate an account holder, or likelihood of doing so successfully.

Reliability is especially important for a backup authentication mechanism of last resort: account holders who find themselves needing to use this mechanism may have no other chance to regain access to their accounts [11]. Yet, reliability cannot be achieved at the expense of security; if a backup authentication mechanism is less secure than the primary mechanism it supports, its very existence will make users' accounts less secure. Fortunately, backup authentication occurs less often than primary authentication and so efficiency may be sacrificed to achieve reliability and security.

II. Related Work

2.1. Social Authentications

Depending on how friends are involved in the authentication process, social authentications can be classified into trustee based and knowledge-based social authentications. In trustee based social authentications [4], the selected friends aid the user in the authentication process. Knowledge-based social authentication, asks the user questions about his or her selected friends and thus friends are not directly involved.

1) Trustee-Based Social Authentication Systems: Authentication is traditionally based on three factors: something you know, something you have and something you are. Brainard et al. [4] proposed to use the fourth factor, i.e., somebody you know, to authenticate users. We call the fourth factor trustee-based social authentication. Brainard et al. combined trustee-based social authentication with some other factor as a two-factor authentication mechanism. It was later adapted to be a backup authenticator [12]. For instance, Schechter et al. [2] designed and built a prototype of trustee-based social authentication system which was integrated into Microsofts Windows Live ID system. Moreover, Facebook designed Trusted Friends in October, 2011 [8] and it was improved to be Trusted Contacts [7] in May, 2013.

2) Knowledge-Based Social Authentication Systems: Such social authentications are still based on something you know. Yardi et al. [6] proposed a knowledge-based authentication system based on photos to test if a user belongs to the group that he or she tries to access. Facebook recently launched a similar photo-based social authentication system [1], in which Facebook shows a few photos of a friend of a user and asks the user to name the friend. Such system essentially relies on the knowledge that the user knows the person in the shown photos. Recent work has shown, via theoretical modeling [5] and empirical evaluations [10], that photo-based social authentication are not resilient to various attacks such as automatic face recognition techniques, questioning their use as a backup authentication mechanism.

2.2. Diffusion Models

Our forest fire attacks essentially describe diffusion processes in a trustee network. We review a few representative diffusion models from different research areas and discuss the differences between them and our work.

1) Updates Propagation Models: Malkhi et al. proposed the l-Tree propagation model to diffuse updates among a large distributed system of data replicas, some of which might exhibit Byzantine failures. Their model assumes a point to- point communication for each pair of nodes. A node that already receives the update is called active, otherwise it is called inactive. Initially, a small set of nodes are active. Each active node is associated with a candidate set of nodes. In each iteration, each active node is allowed to send the update to at most F nodes which are selected from the corresponding candidate set uniformly at random. An inactive node becomes active if it receives the update from at least k other nodes.

There are two key differences between our forest fire attacks and the l-Tree propagation model. First, an uncompromised node can receive verification codes from uncompromised trustees via spoofing attacks in forest fire attacks while an inactive node can only receive updates from active nodes in the l-Tree model. Second, in each iteration, each compromised node sends verification codes to all nodes that select it as a trustee in forest fire attacks while an active node can only send the update to at most F nodes in the l-Tree model.

2) Information Propagation Models: Models for how products and innovations propagate on a social network have been studied in various domains such as viral marketing and the spread of technological innovations. These models can be divided into two categories: linear threshold model and independent cascade model. Again, a node is said to be active if it already adopts the corresponding product or innovation, otherwise it is inactive. In both models, a small set of nodes are active initially.

a) Linear threshold model: In this model, each node u is associated with a threshold, which indicates the fraction of u's friends that must become active before u becomes active. The propagation proceeds deterministically in discrete iterations: in the tth iteration, an inactive node becomes active if its fraction of active friends is no less than u' activation threshold.

b) Independent cascade model: Different from the linear threshold model, the independent cascade model proceeds in discrete iterations according to the following randomized rule: when a node u first becomes active in the tth iteration, it has a single chance to activate each of its currently inactive friend v and succeed with some probability which encodes the influence of u to v.

The key difference is that verification codes can be propagated from an uncompromised node to another uncompromised node via spoofing attacks in forest fire attacks while an inactive node can only be activated by active nodes in the linear threshold model and the independent cascade model. Moreover, an active node only has a single chance to activate its friends in the independent cascade model while a compromised node can send verification codes to the uncompromised nodes that select it as a trustee as many times as it wants.

3) Epidemic Propagation Models: Epidemic propagation models describe the propagations of various contagious diseases such as sexually transmitted diseases, inuenza and measles.

One popular epidemic model is the so-called SIR model. Different from the above reviewed models in which each node can be either active or inactive, SIR model assumes that each node can be in one of the three states, i.e., susceptible, infectious and removed. Initially, a set of nodes are infectious and all other nodes are susceptible. Each infectious node u remains infectious for a fixed number of iterations I. In each of the iterations, u has some probability of passing the disease to each of its susceptible neighbors. After I iterations, u becomes removed, which means that u cannot catch nor propagate the disease any more.

Again, a susceptible node can only be influenced by infectious nodes in the SIR model, which is different from the forest fire attacks. Moreover, the state removed is not meaningful in the context of forest fire attacks since a node could be compromised again even if it recovers the account and resets the password.

III. Trustee-Based Social Authentications

Web services today most commonly rely on passwords to authenticate users. Unfortunately, two serious issues in this paradigm are: users will inevitably forget their passwords and their passwords could be compromised and changed by attackers, which result in the failures to access their own accounts.

Therefore, web services often provide users with backup authentication mechanisms to help users regain access to their accounts. Current widely used backup authentication mechanisms such as security questions and alternate email addresses are insecure or unreliable or both. Previous work [3] has shown that security questions are easily guessable and phished and that user might forget their answers to the security questions. A previously registered alternate email address might expire upon the user's change of school or job. For the above reasons, it is important to design a secure and reliable backup authentication mechanism.

Trustee-based social authentication has attracted increasing attentions and has been shown to be a promising backup authentication mechanism. Brainard et al. [4] first proposed trustee-based social authentication and combined it with other authenticators as a two-factor authentication mechanism. Later, trustee-based social authentication was adapted to be a backup authenticator. In particular, Schechter et al. [12] designed and built a prototype of trusted based social authentication system which was integrated into Microsoft's Windows Live ID. Schechter et al. found that trustee-based social authentication is highly reliable. Facebook announced its trustee-based social authentication system called Trusted Friends in October, 2011 [8] and it was redesigned and improved to be Trusted Contacts [7] in May, 2013.

These previous work either focus on security at individual levels or totally ignore security. In fact, security of users is correlated in trustee-based social authentications, in contrast to traditional authenticators where security of users are independent. Specifically, a user's security in trustee-based social authentications relies on the security of his or her trustees; if all trustees of a user are already compromised, then the attacker can also compromise him or her because the attacker can easily obtain the verification codes from the compromised trustees. The impact of this key difference has not been touched. Moreover, none of the existing work has studied the fundamental design problems such as how to select trustees for users so that the system is more secure and how to set the system parameters to balance between security and usability. In summary, our key contributions are as follows:

- We propose a novel framework of attacks, which we call forest fire attacks.
- We construct a model to formalize the threats of forest fire attacks and their costs for attackers. Moreover, we explore various attack scenarios and defense strategies.
- We apply our framework to extensively evaluate these attack scenarios, defense strategies and the impact of system parameters using three real-world social networks. Our results have strong implications for designing more secure trustee-based social authentications.

IV. Problem Statement

Trustee based social authentication mechanism users the verification codes in the recovery process. Different verification codes are sending to the user's trustees. Recovery threshold is used to indicate the minimum verification code requirements. User accounts are activated using K verification codes received from their trustees. Forest fire attack initiates the attack by compromising small set of users. The attacker iteratively attacks the rest of users by exploiting trustee-based social authentications. Forest fire attack framework is selects the compromised users are seed users. Probabilistic model is constructed to handle the threats of forest fire attacks. Ordering Gradient (O-Gradient) algorithm is used to identify the ordering construction strategy. Trustee Degree (T-Degree) algorithm is used to minimize the out degree for the trustee. Three defense strategies are used to secure the social authentication process. They are hiding trustee networks from attackers, mitigating spoofing attacks and constraining the selection of trustees. The following problems are identified from the existing system.

- Single service based verification mechanism
- Community based trustee selection is not supported
- Trustee levels are not considered
- Time consuming verification strategy

V. Forest Fire Attacks

Our forest fire attacks consist of Ignition Phase and Propagation Phase.

1) Ignition Phase: In this phase, an attacker obtains a small number of compromised users which we call seed users. They could be obtained from phishing attacks, statistical guessings and password database leaks, or they could be a coalition of users who collude each other. Indeed, a large number of social network accounts were reported to be compromised, showing the feasibility of obtaining compromised seed users.

2) Propagation Phase: Given the seed users, the attacker iteratively attacks other users. In each attack iteration, the attacker performs one attack trial to each of the uncompromised users according to some attack ordering of them. In an attack trial to a user u, the attacker sends an account recovery request with u's username to the service provider, which issues different verification codes to u's trustees. The goal of the attacker is to obtain verification codes from at least k trustees. If at least k trustees of u are already compromised, the attacker can easily compromise u; otherwise, the attacker can impersonate u and send a spoofing message to each uncompromised trustee of u to request the verification code. Schechter et al. [12] found that such spoofing attacks can successfully retrieve a verification code with an average probability around 0.05.

Although the spoofing attacks can help attackers compromise more users, we want to stress that they are optional. We will show in our experiments that an attacker can still compromise a large number of users even if he does not use spoofing attacks to retrieve verification codes in some cases.

3) Example: A forest fire attack to a service with 6 users. Note that a good attack ordering can increase the probability that users are compromised and decrease the number of required spoofing messages. In our example, if the attacker performs attack trials with an attack ordering of u_5, u_6, u_4, the attacker needs to spoof both u_4 and u_6 to compromise u_5, which requires two spoofing messages. With the attack ordering of u_6, u_5, u_5, the attacker only needs to spoof u_4 to compromise u_5, which only requires one spoofing message and could succeed with a higher probability.

4) Compromised Users Could be Recovered: Users could recover their compromised accounts to be uncompromised after they or the service provider detect suspicious activities of the accounts. For instance, a trustee of u receiving a spoofing message might report to u, who then changes his or her password; the phenomenon that a trustee requests lots of verification codes for different users within a short period of time is a possible indicator of forest fire attacks and the service provider could then notify the users, whose trustees have requested verification codes, to change passwords. Moreover, a recovered account could be compromised again in future attack iterations, e.g., when the trustees of the recovered user are still compromised. The process of being compromised and being recovered could repeat for many attack iterations.

VI. Multi Level Trustee based Social Authentication

The trustee based social authentication scheme security is enhanced with verification code request control mechanism. Time bounded verification strategy is used for the authentication process. Hierarchical trustee based verification scheme is used to improve the security. Multiple service based authentication is used in the attack defending process.

The trustee based verification scheme is used to recover the user accounts. User level and service level trustee selection scheme is applied for the authentication process. Trustee hierarchy level and time bound constraints are used in the social authentication process. The system is divided into six major modules. They are internet services, trustee selection, forest fire attacks, social authentication, hierarchical verification and multi service verification.

Internet service module is used to manage user account in Internet services. Trustee selection module is designed to assign trustees for the user accounts. Forest fire attacks are raised against the user accounts. User account recovery is carried out under the social authentication process. Hierarchical verification is initiated to perform trustee hierarchy based verification. Multi service verification process performs the social authentication using different service mediums.

6.1. Internet Services

E-mail, social networks and chat services are provided under Internet environment. Internet services are provided with user accounts. Friends and contacts list are updated by the user. Community and group assignment operations are also managed by the users.

6.2. Trustee Selection

Trustees are involved in the user account recovery process. Trustee selection is carried out in two ways. Service level trustee selection process is initiated by the service providers. User level trustee selection is managed by the account holder.

6.3. Forest Fire Attacks

Forest fire attacks are initiated to recover user accounts. Compromised users are involved in the attack process. Compromised users are referred as seed users for the attacks. Forest fire attacks are raised against group of users.

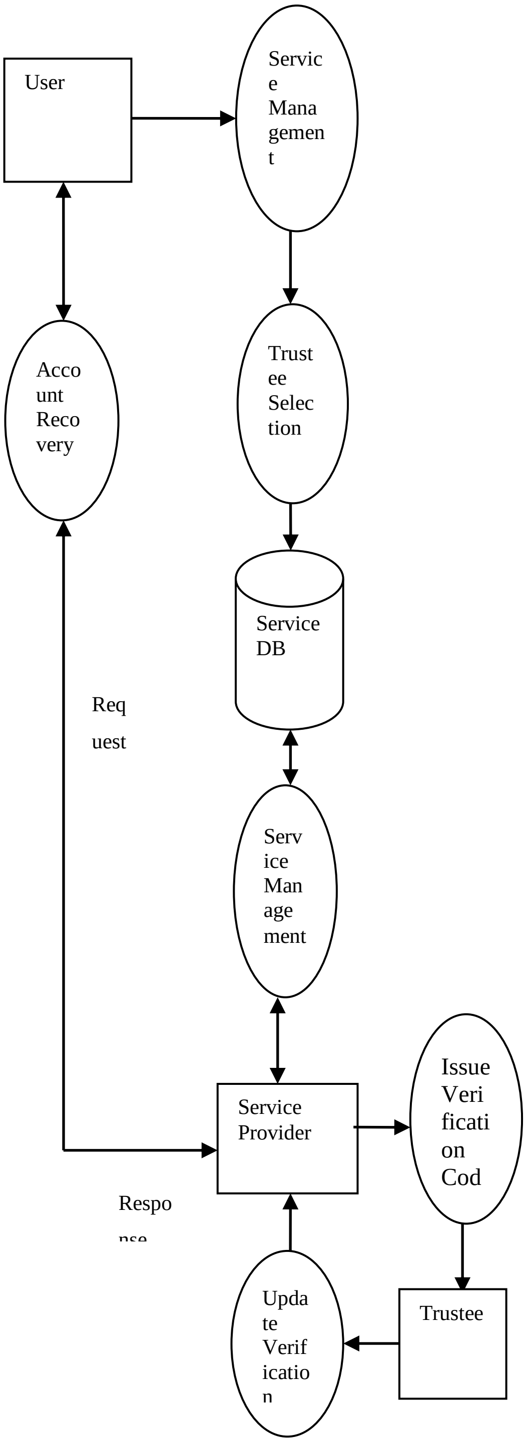

Fig. No: 6.1. Multi Level Trustee based Social Authentication

6.4. Social Authentication

The social authentication is performed to recover the user accounts. Verification code is issued to the trustees. User accounts recovery is carried out with K-verification codes. Time bounded verification code submission scheme is used in the system.

6.5. Hierarchical Verification

Social authentication scheme is improved with hierarchical verification mechanism. Trustees are assigned with different hierarchies. Minimum trustee verification code is required for each hierarchy levels. Trustee groups and communities are used in the hierarchy level based social authentication process.

6.6. Multi Service Verification

Social authentication is carried out with the support of different user level services. Verification codes are issued through E-mail and SMS services. Separate communication channels are assigned to collect verification codes. Different verification threshold is used for each service.

VII. Conclusion

Trustee-based social authentication performs user authentication with the help of their friends. Forest fire attacks are raised by compromising users from the trustees. Probabilistic models and defense strategies are used to control forest fire attacks. Hierarchical level verification, multi service verification and time bound based verification methods are used to improve the security. Efficient attack controlling mechanism is used in user authentication process. Authentication is improved with trustee levels with different priorities. Multi service based verification mechanism is used to improve the authentication tasks. Deadline based verification code model is adopted to support boundary based verification process.

Reference

[1] A. Rice. (2011, Jan.). Facebook’s Knowledge-Based Social Authentication [Online]. Available: http:// blog.facebook.com/blog.php?post=486790652130

[2] (2013, May). BadRank [Online]. Available: http://pr.efactory.de/epr0. html

[3] S. Schechter, A. J. B. Brush and S. Egelman, “It’s no secret: Measuring the security and reliability of authentication via ‘secret’ questions,” in Proc. IEEE Symp. Security Privacy, May 2009, pp. 375–390.

[4] 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.

[5] H. Kim, J. Tang and R. Anderson, “Social authentication: Harder than it looks,” in Proc. Financial Cryptography (FC), 2012.

[6] S. Yardi, N. Feamster and A. Bruckman, “Photo-based authentication using social networks,” in Proc. 1st Workshop Online Social Netw. (WOSN), 2008.

[7] (2013, May). Facebook’s Trusted Contacts [Online]. Available: goo.gl/xHmVHA

[8] (2011, Oct.). Facebook’s Trusted Friends [Online]. Available: goo.gl/KdyYXJ

[9] Michele Nitti, Roberto Girau and Luigi Atzori, “Trustworthiness Management in the Social Internet of Things”, IEEE Transactions On Knowledge And Data Engineering, Vol. 26, No. 5, May 2014

[10] I. Polakis et al., “All your faces are belong to us: Breaking facebook’s social authentication,” in Proc. Annu. Comput. Security Appl. Conf. (ACSAC), 2012.

[11] Xiaohui Liang, Xiaodong Lin and Xuemin (Sherman) Shen, “Enabling Trustworthy Service Evaluation in Service-Oriented Mobile Social Networks”, IEEE Transactions On Parallel And Distributed Systems, February 2014

[12] S. Schechter, S. Egelman and R. W. Reeder, “It’s not what you know, but who you know,” in Proc. Conf. Human Factors Comput. Syst. (CHI), 2009.