Scientific Journal Impact Factor (SJIF): 1.711

International Journal of Modern Trends in Engineering and Research

ISSN (ONLINE) : 2349 - 9745 ISSN (PRINT) : 2393 - 8161

An Efficient User Account Recovery Scheme for Internet Applications

Ms. K. Dhivya[1], Ms. K.M. Padmapriya[2]

[1]MCA, MPhil., Research Scholar, Department of Computer Science, SSM College of Arts and Science, Komarapalayam, Tamilnadu, India

[2]MSc., MPhil., Assistant Professor, Department of Computer Science, SSM College of Arts and Science, Komarapalayam, Tamilnadu, India

Abstract-User account management is an important task in all applications. Online services are employed to support mail, chat, media data sharing and social network features. User ID and password are the key requirements in the user authentication process. Security questions and alternate mail account details are required in the account verification process due to password missing problems. Security and reliability issues are raised in the security questions and alternate mail account based methods.

Account recovery is achieved with backup authentication methods. Contact based user verification scheme uses the trustees that are selected from the contact list of the user account. Verification codes are issued to the trustees for the user account recovery process. The password recovery is achieved with K verification codes that are received from the trustees. Trustee based authentication model is threaten by forest fire attacks. Compromised users are used to iteratively attack the social authentication mechanism. Forest fire attacks are handled with probabilistic models. Defense methods are applied to discover and control the forest fire attacks.

Time limit based account recovery mechanism is adapted to control the forest fire attacks. Social authentication process is enhanced with multi level trustee based verification mechanism. The attack controlling scheme is employed with multiple service based account verification mechanism. The system is equipped with service level, user level and hierarchical level trustees for account recovery process.

I. Introduction

Social authentication may be effective against pure strangers. The people against whom we frequently require privacy protection are precisely those in our own social circle. For example, if a married man is having an affair, some person in another country is not likely to be interested; the people who are Interested are his friends and his wife's. In short, users may share a lot of the r for ends with their adversaries. This is nothing new; 2,400 years ago, Sun-Tzu said `Keep your friends close and your enemies closer'. So a proper assessment of the protective power of social authentication in real social networks must be made using real data.

We observe that there exists a potential adversary a who can impersonate the target user u with a high probability if the number of challenges k is small. This is because a shares many mutual friends with the user. In this case, random selection of challenge images may be ineffective. We propose instead \community-based challenge selection"; our intuition is that a user's friends often fall into several social groups with few, if any, common members. So if we select challenges from different groups, this may cut the attack success probability significantly.

II. Related Work

Recognising the difficulty of deploying single sign-on schemes, automated password management systems seek to achieve the same effect by have a trusted delegate perform log-in on behalf of a user, without any changes to the relying server. Gabber et al. proposed an initial scheme called Janus in 1997 which would accomplish this by proxying web traffic through a paid, trusted anonymising proxy which would automatically fill strong passwords into web forms for the user when needed. Such a service never materialized, but password management by the operating system has been widely implemented, at least since Apple's Key Chain software debuted for MacOS 8.6 in 1999. There are now many free software programs to automatically store passwords.

Most modern browsers, along with some desktop software such as email clients, will automatically remember previously entered passwords and optionally secure them through a master password. This solution adds little for security, though, as users must still create the passwords initially. Advanced users may install add-ons to generate secure passwords but these require skilled manual intervention and trust in the tools. A 2006 user survey indicated that 93% of users have never used any automated tools, although about two-thirds did make use of a browser with automatic password entry.

Academic research by Halderman et al. focused on building browser extensions to automatically derive domain-specific passwords by hashing a master password with the current domain. A similar approach was taken by Ross et al., who also supported the difficult case of remote access to domain specific passwords when needed through a secure server; their PwdHash browser extension has been installed by about 100,000 Mozilla Firefox users. Florêncio and Herley have re-visited the trusted server approach, proposing to use trusted proxy servers to securely access websites even from highly untrusted computers by using one-time password schemes to authenticate the proxy and having the proxy then authenticate with the desired web server.

III. Trustees and Internet Services

Trustee-based social authentication has attracted increasing attentions and has been shown to be a promising backup authentication mechanism. Brainard et al. 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. 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 and it was redesigned and improved to be Trusted Contacts in May, 2013. 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. 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. 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.

The following issues are discovered from the user account recovery scheme for Internet services. Single service based verification mechanism, Community based trustee selection is not supported, Trustee levels are not considered and Time consuming verification strategy.

IV. User Account Recovery Scheme for Internet Applications

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.

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. 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.

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. 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.

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. 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.

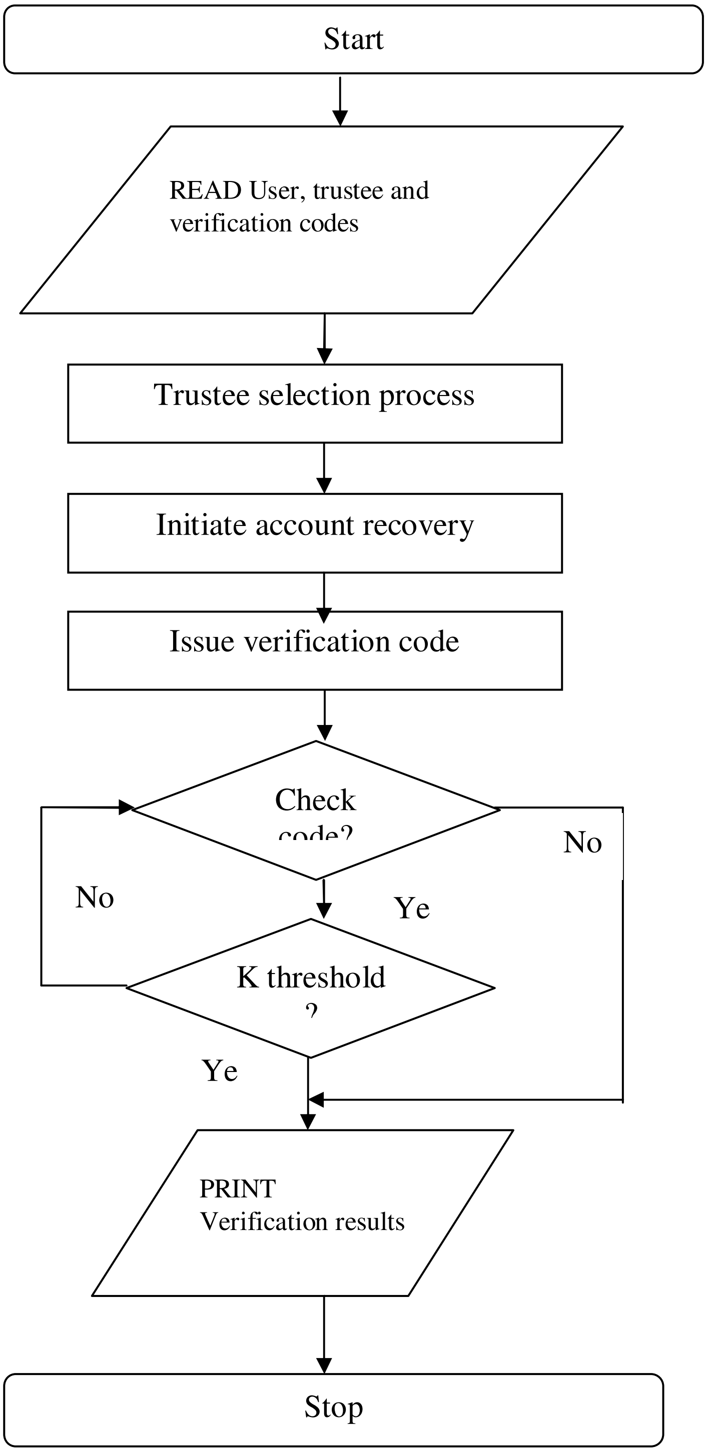
Start
READ User, trustee and verification codes
Trustee selection process
Initiate account recovery
Issue verification code
Check code?
No
No
Ye
K threshold ?
Ye
PRINT Verification results
Stop

Fig. No: 4.1. User Account Recovery Scheme for Internet Applications

V. Conclusion and Future Enhancement

User account recovery operations are carried out with the support of contacts in their account. 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. The system can be enhanced with the following features.

The system can be enhanced to control service request based attacks against service providers. The trustee based social authentication scheme can be improved with spatial constraints for account recovery. Cryptography techniques can be adapted to improve the security for account recovery process. The account recovery process can be enhanced with digital signature based verification mechanism.

References

1. Gianluca Stringhini, Christopher Kruegel and Giovanni Vigna, "Detecting Spammers on Social Networks", ACM, 2010
2. H. Gao, J. Hu, C. Wilson, Z. Li, Y. Chen and B. Zhao, "Detecting And Characterizing Social Spam Campaigns," in Proc. Internet Meas. Conf. (IMC), 2010.
3. H. Kim, J. Tang, and R. Anderson, "Social authentication: Harder than it looks," in Proc. Financial Cryptography (FC), 2012.
4. Huansheng Ning, Hong Liu and Laurence T. Yang, "Aggregated-Proof Based Hierarchical Authentication Scheme for the Internet of Things", IEEE Transactions On Parallel And Distributed Systems, Vol. 26, No. 3, March 2015.
5. Jure Leskovec, Daniel Huttenlocher and Jon Kleinberg, "Signed Networks in Social Media", ACM, 2010.
6. Magdalini Eirinaki and Iraklis Varlamis, "A Trust-Aware System for Personalized User Recommendations in Social Networks", IEEE Transactions On Systems, Man, And Cybernetics: Systems, Vol. 44, No. 4, April 2014
7. Michail Tsikerdekis and Sherali Zeadally, "Multiple Account Identity Deception Detection in Social Media Using Nonverbal Behavior", IEEE Transactions On Information Forensics And Security, Vol. 9, No. 8, August 2014
8. 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
9. N. Z. Gong et al., "Evolution Of Social-Attribute Networks: Measurements, Modeling, And Implications Using Google+," in Proc. ACM Conf. Internet Meas. Conf. (IMC), 2012.
10. Neil Zhenqiang Gong and Di Wang, "On the Security of Trustee-Based Social Authentications" IEEE Transactions On Information Forensics And Security, Vol. 9, No. 8, August 2014
11. Richard Shay, Patrick Gage Kelley, Lorrie Faith Cranor and Serge Egelman, "Of Passwords And People. Measuring The Effect Of Password-Composition Policies", ACM, 2011
12. Sha Ma, Qiong Huang, Mingwu Zhang and Bo Yang, "Efficient Public Key Encryption With Equality Test Supporting Flexible Authorization", IEEE Transactions On Information Forensics And Security, Vol. 10, No. 3, March 2015.
13. Vanga Odelu, Ashok Kumar Das and Adrijit Goswami, "A Secure Biometrics-Based Multi-Server Authentication Protocol Using Smart Cards", IEEE Transactions On Information Forensics And Security, Vol. 10, No. 9, September 2015.
14. Xiaohui Liang, Xiaodong Lin and Xuemin Shen, "Enabling Trustworthy Service Evaluation in Service-Oriented Mobile Social Networks", IEEE Transactions On Parallel And Distributed Systems, February 2014
15. Yuhui Zhong, Bharat Bhargava, Yi Lu and Pelin Angin, "A Computational Dynamic Trust Model for User Authorization", IEEE Transactions On Dependable And Secure Computing, Vol. 12, No. 1, January/February 2015.