ISSN:2348-2079

Volume-6 Issue-2

International Journal of Intellectual Advancements and Research in Engineering Computations

Trustee-Base Social Authentication Process using Alert System

[1]Mr. R. NavinKumar, M.C.A.,M.Phil.,Assistant Professor/MCA
[2]Mr. C. Seenivasan, III MCA
Department of MCA ,Nandha Engineering College(Autonomous),Erode-52
E-Mail ID: navinsoccer07@gmail.com, kamalrenu888@gmail.com

Abstract **- Web services present 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. Unfortunately, current widely used backup authentication mechanisms such as security questions and alternate email addresses are insecure or unreliable or both. Recently, authenticating users with the help of their friends (i.e., trustee-based social authentication) has been shown to be a promising 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 (i.e., recovery threshold) verification codes from the trustees before being directed to reset his or her password. This project provides the first systematic study about the security of trustee-based social authentications. This project introduces a novel framework of attacks, which is called as forest fire attacks. In these 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. Then, a probabilistic model is constructed to formalize the threats of forest fire attacks and their costs for attackers. Finally, the framework is applied to extensively evaluate various concrete attack and defense strategies using three real-world social network datasets. The application used for simulation is designed using Microsoft Visual Studio .Net 2005 as front end. The coding language used is C#.Net. MS-SQL Server 2000 is used as back end database.**

Index Terms- Alert System , Networking , Social Authentication, Trustee.

I.INTRODUCTION

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. Unfortunately, current widely used backup authentication mechanisms such as security questions and alternate email addresses are insecure or unreliable or both. 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. The proposed trustee-based social authentication and combined it with other authenticators (e.g., password, security token) as a two-factor authentication mechanism.

Later, trustee-based social authentication was adapted to be a backup authenticator. In particular 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. 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 (e.g., recovery threshold) to balance between security and usability.

II .RELATED WORK

Joseph Bonneau et al reports the results of the first large-scale empirical analysis of password implementations deployed on the Internet. Their study included 150 websites which offer free user accounts for a variety of purposes, including the most popular destinations on the web and a random sample of e-commerce, news, and communication websites. Although all sites evaluated relied on user-chosen textual passwords for authentication, they found many subtle but important technical variations in implementation with important security implications. Many poor practices were commonplace, such as a lack of encryption to protect transmitted passwords, storage of clear text passwords in server databases, and little protection of passwords from brute

force attacks. While a spectrum of implementation quality exists with a general correlation between implementation choices within more-secure and less-secure websites, they find a surprising number of inconsistent choices within individual sites, suggesting that the lack of a standards is harming security.

HONGYU GAO et al present an initial study to quantify and characterize spam campaigns launched using accounts on online social networks. They study a large anonymized dataset of asynchronous "wall" messages between Facebook users. They analyze all wall messages received by roughly 3.5 million Facebook users (more than 187 million messages in all), and use a set of automated techniques to detect and characterize coordinated spam campaigns. Their system detected roughly 200,000 malicious wall posts with embedded URLs, originating from more than 57,000 user accounts. They find that more than 70% of all malicious wall posts advertise phishing sites. They also study the characteristics of malicious accounts, and see that more than 97% are compromised accounts, rather than "fake" accounts created solely for the purpose of spamming.

ROSS ANDERSON ET ALstated that thenumber of web service firms have started to authenticate users via their social knowledge, such as whether they can identify friends from photos. Theyhave investigated attacks on such schemes. First, attackers often know a lot about their targets; most people seek to keep sensitive information private from others in their social circle. Against close enemies, social authentication is much less effective. They formally quantify the potential risk of these threats. Second, when photos are used, there is a growing vulnerability to face-recognition algorithms, which are improving all the time. Network analysis can identify hard challenge questions, or tell a social network operator which users could safely use social authentication; but it could make a big difference if photos weren't shared with friends of friends by default.

HaewoonKwakEtAlhave crawled the entire Twitter site and obtained 41.7 million user profiles, 1.47 billion social relations, 4, 262 trending topics, and 106 million tweets. In its follower-following topology analysis they have found a non-power-law follower distribution, a short effective diameter, and low reciprocity, which all mark a deviation from known characteristics of human social networks [24]. In order to identify influentials on Twitter, they have ranked users by the number of followers and by PageRank and found two rankings to be similar. Ranking by retweets differs from the previous two rankings, indicating a gap in influence inferred from the number of followers and that from the popularity of one's tweets. They have analyzed the tweets of top trending topics and reported on their temporal behavior and user participation. They have classified the trending topics based on the active period and the tweets and show that the majority (over 85%) of topics are headline news or persistent news in nature. A closer look at retweets reveals that any retweeted tweet is to reach an average of 1, 000 users no matter what the number of followers is of the original.

IASONAS POLAKIS ET ALexplained Two-factor authentication is widely used by high-value services to prevent adversaries from compromising accounts using stolen credentials. Facebook has recently released a two-factor authentication mechanism, referred to as Social Authentication, which requires users to identify some of their friends in randomly selected photos. A recent study has provided a formal analysis of social authentication weaknesses against attackers inside the victim's social circles. In this paper [25], they extend the threat model and study the attack surface of social authentication in practice, and show how any attacker can obtain the information needed to solve the challenges presented by Facebook. They implement a proof-of-concept system that utilizes widely available face recognition software and cloud services, and evaluate it using real public data collected from Facebook.

III.METHODOLOGY

Problem Definition

The attacker could use a greedy strategy to select seed users. Specifically, the attacker selects seed users one by one. To select a seed user, the attacker iterates over each user that is not a seed user yet; for each such user u, the attacker pretends that u is a seed user and simulates our security model to predict the corresponding expected number of compromised users; and the user u which increases the expected number of compromised users by the most is added as a new seed user. However, it is not scalable to large social networks. It is a proposed research work to make the strategy scalable.In thesis design a trustee selection strategy based on some notion of community. Specifically could select trustees for users such that the trustee network consists of isolated communities, which could constrain the propagation of forest fire attacks.A compromised user u might request a verification code from the service provider when the attacker performs an attack trial to a user who selects u as a trustee. Thus, a compromised user who is a trustee of many other users might request many verification codes eachattack rations.

A. TRUSTEE-BASED SOCIAL AUTHENTICATIONS

A trustee-based social authentication includes two phases Registration Phase. The system prepares trustees for a user Alice in this phase. Specifically, Alice is first authenticated with her main authenticator (i.e., password), and then a few friends, who also have accounts in the system, are selected by either Alice herself or the service provider from Alice's friend list and are appointed as Alice's trustees.Recovery-Phase. When Alice forgets her password or her password was compromised and changed by an attacker, she recovers her account with the help of her trustees in this phase. Specifically, Alice first sends an account recovery request with her username to the service provider which then shows Alice an URL. Alice is required to share this URL with her trustees.

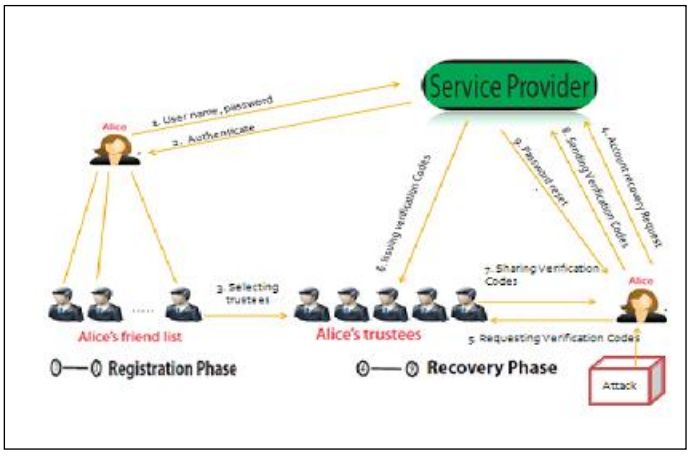

Fig 1. Trustee-Based social

B. SOCIAL NETWORKS AND TRUSTEE NETWORKS

In social network as G = (V, E), where each node in V corresponds to a user in the service and an undirected edge (u, v) represents that users u and v are friends. Moreover, in a trustee-based social authentication system, users and their trustees form a directed network. The user call this directed network a trustee network and denote it as $G_T = (V_T , E_T)$, where a node in V_T is a user in the service and a directed edge (v, u) in E_T means v is a trustee of u. One fundamental challenge in trustee-based social authentication is how to construct the trustee network from a social network so that the system is more secure.

C. FOREST FIRE ATTACKS

.

Ignition Phase:

In this phase, an attacker obtains a small number of compromised users which trustee call seed users. They could be obtained from phishing attacks, statistical guessing, 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, 2 showing the feasibility of obtaining compromised seed users.

Propagation Phase

Given the seed users, the attacker iteratively attacks other users. 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 username to the service provider, which issues different verification codes to 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 otherwise, the attacker canimpersonate u and send a spoofing message to each uncompromised trustee of u to request the verification code.

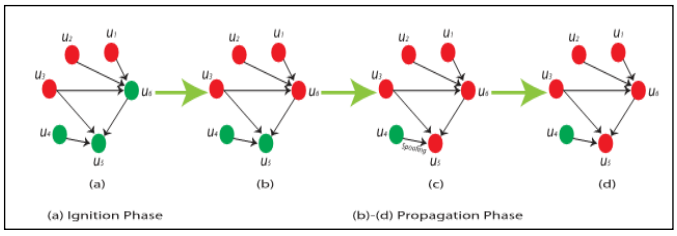

Fig 2. Forest Fire Attack

D. SOCIAL AUTHENTICATIONS

Depending on how friends are involved in the authentication process, social authentications be classified into trustee based and knowledge-based social authentications. In trustee based social authentications the selected friends aid the user in the authentication process.

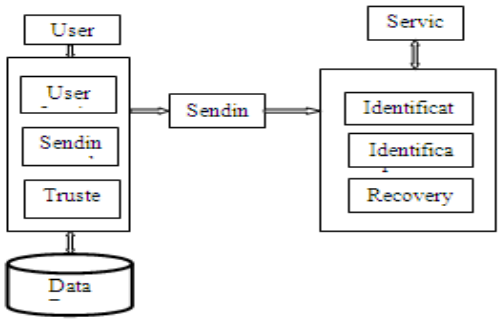

Fig 3. Social Authentication

IV. EXPERIMENTAL SETUP

A. USER REGISTRATION

In this module, the user details such as User Id, User Name, Password, EMail Id, Mobile are registered and the details are saved in 'Users' table.

B. ADD FRIENDS

In this module, the friend user list added to given users. The details are saved in 'Friends' table. Any number of users can be added as friends to given user.

C. ANNOUNCE TRUSTED USERS

In this module, the trusted users' list is added to selected user. The users are selected by the user himself after login to the application. The details are saved in 'TrustedUsers' table. Any number of users can be added as trusted users to given user.

D. SET RECOVERY THRESHOLD

In this module, the trusted users count is set so that the verification code is sent to those members during password recovery phase. The trusted users count value is stored in 'Threshold' table.

E. *SET TIME LIMIT FOR VERIFICATION CODE RECOVERY*

In this module, the time limit in hours is set so that before that time limit, the verification code need to be retrieved from trusted users and submitted for password recovery. Otherwise, it would be invalid and again, the user needs to ask the service provider for new password recovery process. The time limit value is stored in 'TimeLimit' table.

F. *USER COMPROMISATION USING FOREST FIRE ATTACK*

In this module, forest fire attack is implemented. Here to compromise the node 'U', the Attacker User 'A', first one trusted user the time limit in hours is set so that before that time limit, the verification code need to be retrieved from trusted users and submitted for password.

G. *BLOCK USER COMPROMISATION*

In this module, as soon as one trusted user is asked for verification code by Recovering user, then all the trusted users are alerted with that information.

V. CONCLUSION

In this project new proposed system is introduce forest fire attacks. In these attacks, an attacker first obtains a small number of compromised seed users and then iteratively attacks the rest of users according to a priority ordering of them. Second, construct a probabilistic model to formalize the threats of forest fire attacks and their costs for attackers. Third, introduce a few strategies to select seed users and construct priority orderings, and we discuss various defense strategies. For instance, with a small number of users, an attacker can further compromise two to three orders of magnitude more users in some scenarios with low (or even no) costs of sending spoofing messages. However, defense strategy, which guarantees that no users are trustees of too many other users, can decrease the number of compromised users by one to two orders of magnitude and increase the costs for attackers by a few times in some cases. Moreover, the recovery threshold should be set to better balance between security and usability. The recovery threshold is not set to better balance between security and usability. Time boundary is not set so that after verification code is retrieved from trusted user, the original user or attacker user can use the code at any time in future.

Future Enhancements

In future the project involves General Symmetric Encryption process which includes tag generation. Here Group based user management is not provided. Also Session based outsource data access is not provided. In future these options can be included so that Session based outsource data access can be provided to increase the security. User Revocation management can also implemented. Key Storage cost can be reduced when compared to existing system.

REFERENCES

[1] J. Bonneau and S. Preibusch, "The password thicket: Technical and market failures in human authentication on the web," in Proc. 9th Workshop Econ. Inform. Security (WEIS), 2010.

[2] Nancy J. Lightner What users want in e-commerce design: effects of age, education and income. Ergonomics, 46(1):153–168, 2003.

[3] ShirleyGaw and Edward W. Felten Password Management Strategies for Online Accounts. In SOUPS '06:

[4] Proceedings of the Second Symposium on Usable Privacy and Security, pages 44–55, New York, NY, USA, 2006.

[5] Gilbert Notoatmodjo and Clark Thomborson. Passwords and Perceptions. In LjiljanaBrankovic and Willy Susilo, editors, Seventh Australasian Information Security Conference (AISC 2009), volume 98 of CRPIT, pages 71–78, Wellington, New Zealand, 2009.

[6] Shirley Gaw and Edward W. Felten. Password Management Strategies for Online Accounts. In SOUPS '06: Proceedings of the Second Symposium on Usable Privacy and Security, pages 44– 55, New York, NY, USA, 2006.

[7] 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.

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