IJSEAT International Journal of Science Engineering and Advance Technology

A Authentication model to Trustees based Social Networks

Sravya Lakshmi Malyala[1], **D.Ramesh**[2]

[1]PG Scholar, Pydah College of Engineering, Kakinada, AP, India, E-mail: r sravya.malayala@gmail.com.
[2]Assistant Professor, Pydah College of Engineering, Kakinada, AP, India.

Abstract—authenticating users with the help of their friends 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 user's trustees. The user must obtain at least k reset his or her password. In this paper, we provide the first systematic study about the security of trustee based social authentications. In particular, we first introduce verification codes from the trustees before being directed to small framework of attacks, which attacks. In these attacks, an attacker initially obtains we call forest fire iteratively, attacks the rest of users by exploiting trustee-based social authentications. Then, we construct a probabilistic model to for attackers. Moreover, we introduce number of compromised users, and then the attacker a novel various defense formalize the threats of forest fire attacks and their costs strategies. Evaluate various concrete attack and defense our results have finally, we apply our framework to strategies using three real world social network datasets. Extensively strong implications for the design of more secure trustee-based social authentications.

Key words: ***Security model, backup authentication, social networks***

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. Previous works have shown that security questions are easily guessable and security questions. A previously registered alternate email address might expire upon the user's change of school phished and those users might forget their answers to the or job. For the above reasons, it is important to design a secure and reliable backup authentication mechanism. Recently, trustee-based social authentication has attracted increasing attentions and has been shown to be a promising backup authentication mechanism and. Brainard et al. first 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, Schechter et al. [24] designed and built a prototype of trusted based social authentication system which was integrated into. found. However, 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.

II. Background

The Trustee Based Social Authentication

A trustee-based social authentication includes two phases, registration phase and recovery phase.

1)* Registration Phase:* The system prepares trustees for a user Alice in this phase. Specifically, Alice is first authenticated with her main authenticator friends, who also have accounts in the system, are selected by either Alice herself or the service provider from friend list and are appointed trustees.

***2)* 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, her trustees authenticate themselves into the system and retrieve verification codes using the given URL. Alice then obtains the verification codes from her trustees via emailing them, calling them, or meeting them in person. If Alice obtains a sufficient provider, then Alice is authenticated and is directed to reset her password. We call the number of verification. Note that it is important for Alice to know who her trustees are in the Recovery Phase. Schechter showed that users cannot remember their trustees via performing user studies. Thus, a usable trustee-based social authentication system should remind Alice of her trustees. Next, we provide details about two representative trustees based social authentication systems which were implemented by Microsoft his or and Facebook, respectively. In the Registration Phase of Trusted Contacts, a user selects three to five friends from 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 instead. However, once the user gets one trustee correctly, Facebook will remind him of his or her trustees, but it asks the user to type in the names or her of the remaining trustees.

III. Threat Model

A. Background Knowledge

We assume that attackers know the trustee network in the target service. The reasonableness of this threat model is supported by two evidences. First, attackers can obtain users‟ usernames. A username is usually a string of letters, digits, and special characters. Moreover, Bonneau et al. [3] showed that a majority (e.g., 96% in their studies) of websites enable attackers to probe if a string is a legitimate username. Thus, strong attackers, who have enough resources to perform username probing, can obtain all usernames in the target service. Second, Schechter found, via performing user studies, that users cannot remember their own trustees. Therefore, a usable trustee-based social authentication system must remind users of their trustees. Recall that an account recovery request only requires a username. As a result, an attacker could send account recovery requests with the collected usernames to the service provider which reminds the attacker of the trustees of each user. Next, we take Facebook as an example to show how an attacker obtains the trustee network. First, Facebook provides an interface1 to test if a user is in Facebook. Thus, the attacker can perform username to collect Facebook users. Second, the attacker sends account recovery requests to Facebook using the collected names. Recall that Facebook shows all trustees to a user once the Facebook users. Thus, the attacker can repeatedly guess the trustees of a user until success. We note that Facebook only allows a user to try around 10 times for typing in the trustees within a short period of time. However, such rate limit cannot prevent a strong attacker from obtaining the trustee network eventually, though it can increase the attackers cost.

B. Forest Fire Attacks

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 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, 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 us username to the service provider, which issues different verification codes to us 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. [24] 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.

3) Compromised Users could be Recovered: Users could recover their compromised accounts to be uncompromised after them or the service provider detects 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.

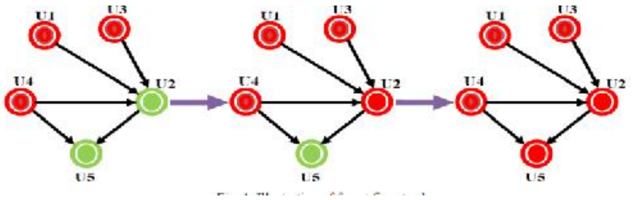


Fig. 1 Illustration of forest fire attacks

IV. Security Model

In this section, we introduce our security model to formalize the threats of forest fire attacks and their costs for attackers.

1) Ignition Phase: If u is a seed user, then us initial compromise probability is 1, otherwise we model us initial compromise probability as 0. 2) Propagation Phase: The key component is to update the aggregate compromise probability of u when the aggregate compromise probabilities of us trustees are given.

C. Obtaining One Verification Code

We denote by A the event that the attacker obtains a verification code from a trustee v of u and the probability that A happens in the attack iteration. Moreover, we denote the event that v is already compromised when the attacker attacks u in the attack iteration as B. When B does not happen, the attacker can impersonate u and send a spoofing message to request attacks succeed spoofing probability. Spoofing probability might a verification code. We call the probability that such spoofing probability might be different in different attack iterations spoofing differently to spoofing messages impersonating different users because be different for different trustees. A trustee might behave he or she might have different levels of trusts with the users that are impersonated. Moreover, because trustees might gradually become aware of the spoofing attacks.

D. Computing Compromise Probabilities

Recall that u is compromised if the attacker codes from at least k trustees of u. Thus, given the natural assumption that we trustees are independent, the compromise probability of you can obtain verification in the attack iteration is calculated.

E. Aggregating Compromise Probabilities

Assuming that whether u is compromised in one attack iteration is independent with whether u is compromised in attack iteration, we can iteratively compute the aggregate compromise probability.

V. Attack Strategies

The attacker could design the seed user selection strategy and the attack ordering construction strategy to maximize the expected number of compromised users. First, we show that finding the optimal set of seed users and the optimal ordering construction strategy is NP-Complete. Then, we explore various scenarios where seed users have different properties and introduce two ordering construction strategies.

A. Strategies for Selecting Seed Users

A seed user’s selection strategy S is essentially to assign a score which represents some metric of importance to each user and to select ns users with the highest scores as seed users. This is closely related to the node centrality problem [18] in the network science community. In the following, we modify a few node centrality heuristics as seed user’s selection strategies. These strategies work on a trustee network, and we name them with a prefix S to indicate they are used to select seed users.

B. Mitigating spoofing Attacks

Another way to defend against forest fire attacks is to remind trustees of not sharing verification codes via messages. This strategy is not novel, and we include it for completeness. Indeed, existing social authentication systems [7], [24] already try to mitigate spoofing attacks. For instance, Microsoft’s system [24] asks a trustee why she is requesting the verification code and encourages her to share the code with the user via phone or meeting in person.

C. Constraining Trustee Selections

Finally, we introduce strategies to constrain trustee selections, which are easy to implement and effective at defending against forest fire attacks. We consider both local trustee selection strategies and global trustee selection strategies. A local trustee selection strategy is based on a user local social network structure while a global one is based on the entire social network structure. We name these strategies with a prefix „T-‟ to indicate that they are used to select trustees. We note that how users select their trustees in a real trustee-based social authentication system such as Facebooks Trusteed Contacts is not clear and thus might not be one of our strategies. However, our work focuses on a comparative study about different trustee selection strategies and can shed light on which strategy is more secure.

***1*) Local Trustee Selection Strategies**

For a user u, a local trustee selection strategy essentially computes a score for each friend v of u and then selects mu friends with the highest scores as us trustees. T Random: As a baseline, T the number of common friends of two users is an informative indicator about the level of trust between them. Thus, one speculation is that a user might select friends with which he or she shares many common friends as trustees. To quantify the security of this speculation, we design the strategy which uses the number of common friends shared by u and his or her friend v as the score s(v, u), However, there are two drawbacks of T-CF. First, the fact that u shares many friends with a popular user v does not necessarily mean that u and v have a high level of trust because it is normal for many friends of u to be in friend list. Second, if a common friend of u and v is a popular user, then sharing him or doesn’t necessarily indicate a high level of trust between u and v. Next, we introduce two strategies to overcome the two drawbacks, respectively.

2) Global Trustee Selection Strategies

Global strategies leverage the entire social network structure and thus are potentially better than local strategies. As we discussed, seed users could be those having large outdegrees in the trustee network, and they could enable an attacker to compromise many other users. Thus, we propose the T-Degree strategy to minimize the maximum outdegree in the trustee network. Intuitively, T-Degree constrains that no users are selected as trustees by too many other users. T-Degree selects trustees for users one by one. For each user u that has adopted the trustee-based social authentication service, T-Degree selects his or her mu friends whose current outdegrees in the trustee network are the smallest as yours trustees; ties are broken uniform at random.

VII. Experimental Results

A. Impact of Attacker’s Resources and Attack Orderings

The number of attack iterations is closely related to the costs of sending spoofing messages.

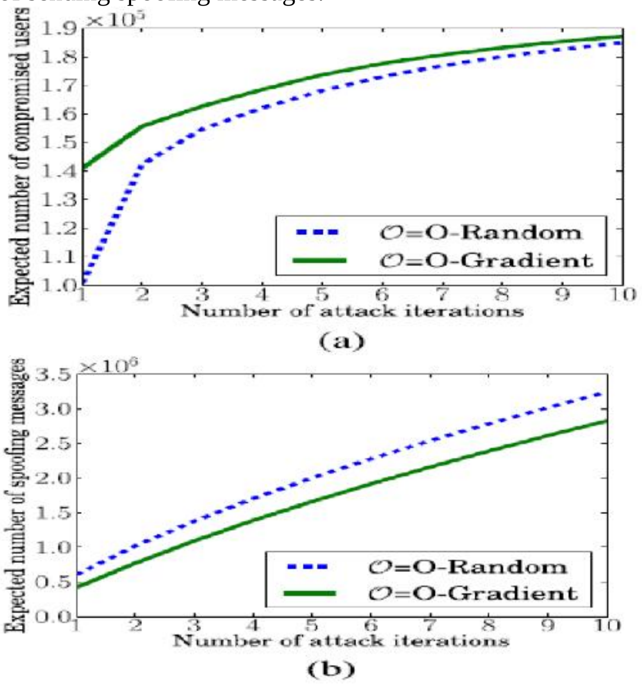
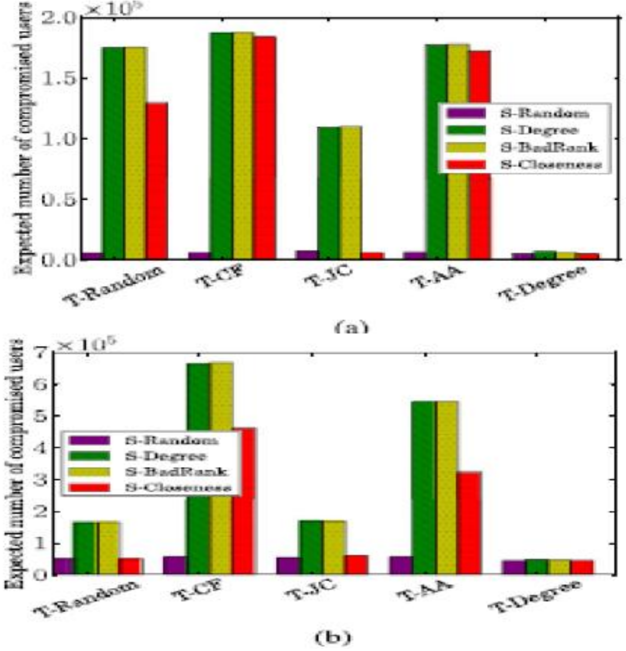


Fig. 2 Impact of Attacker’s Resources and Attack Ordering

Figure 2 illustrates the expected number of compromised users (Figure 2a) and the expected number of required spoofing messages can perform forest fire attacks with low costs. This is because such an attacker can send out billions of messages per day with a low cost which is far more than that needed to spoof trustees in our experiments. Second, we find that the ordering construction strategy O-Gradient compromises more users and requires fewer spoofing messages than O-Random when the attacker performs a given number of attack iterations. In other words, given the number of spoofing messages the attacker can send, the attacker should adopt O-Gradient to construct the attack orderings.

B. Impact of Seed Users’ Selection Strategies and Trustee Selection Strategies

Figure 3 and Figure 4 show the expected number of compromised users and the expected number of required spoofing messages respectively for different seed selection strategies and trustee selection strategies. We can draw a few conclusions. First, we find that forest fire attack is a potential big threat. For instance, when the seed users are appointed as trustees of many in the three social networks, respectively. This represents a growth of two to three orders of magnitude from the 1,000 seed users. However, our strategy T-Degree can decrease the expected number of compromised users by one to two orders of magnitude. For instance, the expected number of compromised users of T-Degree is 53 times smaller than that o selection strategy is S-Degree. Moreover, our strategy T-Degree can increase the costs for attackers by a few times in some cases. For instance, the cost of sending spoofing messages of T-Degree is 3 times bigger than that of T-CF and that of T-AA on reason is that the trustee networks constructed by T-Degree are more loosely connected, which makes it harder for forest fire attacks to propagate among them. Second, even if the seed users are distributed among a social network uniformly at random (i.e., S-Random), the attacker can still compromise dozens of times more users. For instance, the attacker can still compromise 65 to 80 times more users in Twitter depending on how trustees are selected. Third, T-JC works better than T-AA which performs better than T-CF for all seed selection strategies except S-Random. We find that the outdegree distributions of the trustee networks constructed by T-CF are skewed towards high degrees the most while those constructed by T-JC are skewed towards low degrees the most. Thus, the seed users in the trustee networks constructed by T-JC have lower outdegrees than those constructed by T-AA, which have lower outdegrees than those constructed by T-CF. As a result, T-JC performs better than T-AA and T-AA performs better than T-CF.



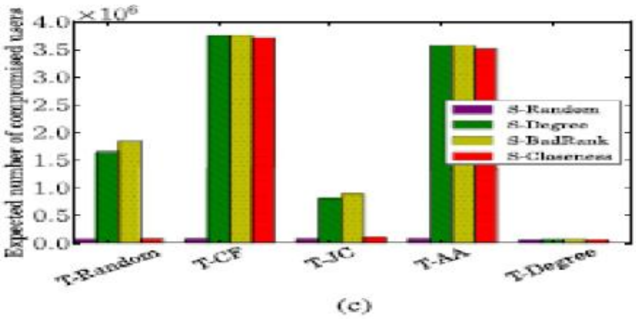


Fig. 3 The expected number of compromised users for different seed users selection strategies and trustee selection strategies a) Flickr b) Google+ c) Twitter

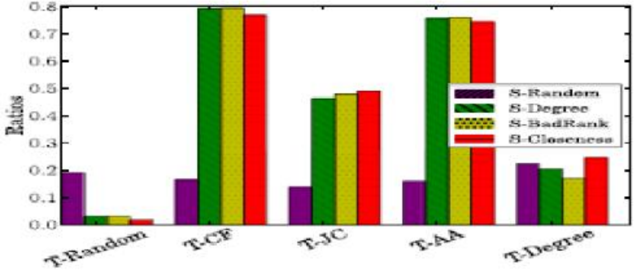


Fig. 4 The ratio between the expected number of users that are compromised without spoofing attacks and those with spoofing attacks for different seed selection strategies and trustee selection strategies

VIII. Conclusion And Future Works

We provide the first systematic study about the security of trustee-based social authentications. First, we 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. threats of forest fire attacks and their costs for attackers. Third, Second, we construct a probabilistic model to formalize the introduce a few strategies to select seed users and construct priority orderings, and we discuss various defense strategies. Of seed users, an attacker can further compromise two to three orders of magnitude more users in some scenarios with low costs of sending spoofing messages. However, our 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 be 4 to better balance between security and usability. A few future directions include evaluating forest firest attacks on real social authentication systems such as Facebook‟s Trusted Contacts, designing new attack and defense strategies, and optimizing forest fire attacks given a time constraint.

References

[1] S. M. Metev and V. P. Veiko, *Laser Assisted Microtechnology*, 2nd ed., R. M. Osgood, Jr., Ed. Berlin, Germany: Springer-Verlag, 1998.

[2] G. Eason, B. Noble, and I. N. Sneddon, "*On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,*" Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. (references)

[3] L. A. Adamic and E. Adar, "*Friends and neighbors on the web*," Social Netw., vol. 25, no. 3, pp. 211–230, 2003.

[4] BadRank [Online]. Available: http://pr.efactory.de/epr0.shtml

[5] 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.

[6] 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.

[7] J. Podd, J. Bunnell, and R. Henderson, "*Cost-effective computer security: Cognitive and associative passwords*," in Proc. 6th Australian Conf. Comput.-Human Interact., 1996.

[8] D. Easley and J. Kleinberg, "*Networks, Crowds, and Markets: Reasoning About a Highly Connected World*", Cambridge, U.K.: Cambridge Univ. Press, 2010.

[9] Facebook‟s Trusted Contacts [Online]. Available: goo.gl/xHmVHA

[10] Facebook‟s Trusted Friends [Online]. Available:goo.gl/KdyYXJ

[11] 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.

[12] E. Gilbert and K. Karahalios, "*Predicting tie strength with social media*,"in Proc. SIGCHI Conf. Human Factors Comput. Syst., 2009.

[13] 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.

[14] P. Jaccard, "*Étude comparative de la distribution floraledansune portion des Alpes et des Jura*," Bulletin Soc. Vaudoise Sci. Naturelles, vol. 37,no. 1, pp. 547–579, 1901.

[15] D. Kempe, J. Kleinberg, and E. Tardos, "*Maximizing the spread of influence through a social network*," in Proc. 9th ACM SIGKDD Int.Conf. Knowl.Discovery Data Mining (KDD), 2003.

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

[17] H. Kwak, C. Lee, H. Park, and S. Moon, "*What is Twitter, a social network or a news media?*" in Proc. 19th Int. Conf. World Wide Web(WWW), 2010.

[18] D. Malkhi, Y. Mansour, and M. K. Reiter, "*Diffusion without false rumors: On propagating updates in a Byzantine environment*," Theoret. Comput.Sci., vol. 299, no. 1, pp. 289–306, 2003.

[19] 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.

[20] Node Centrality [Online]. Available: https://en.wikipedia.org/wiki/Centrality

[21] K. Okamoto, W. Chen, and X.-Y. Li, "*Ranking of closeness centrality for large-scale social networks*," in Proc. 2nd Annu. Int. Workshop Frontiers Algorithmics, 2008.

[22] 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.

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

[24] G. Sabidussi, "*The centrality index of a graph*," Psychometrika, vol. 31, no. 4, pp. 581–603, 1966.

[25] 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.

[26] 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.

[27] Spam Messages [Online]. Available:http://en.wikipedia.org/wiki/Botnet

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

[29] M. Zviran and W. J. Haga, "*User authentication by cognitive passwords: An empirical assessment*," in Proc. 5th Jerusalem Conf. Inform. Technol.(JCIT), 1990.