Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 79 (2016) 668 – 674

Procedia Computer Science

7th International Conference on Communication, Computing and Virtualization 2016

Measuring the Security and reliability of Authentication of Social Networking Sites

Kumud Sagar*[a] ,Vijaya Waghmare[b]

Saraswati college of engg & technology,Kharghar,Navi Mumbai,410210,India
Saraswati college of engg & technology,Kharghar,Navi Mumbai,410210,India

Abstract

Social Networking sites nowadays use passwords to authenticate users. But there are certain problems with this; the user may forget his password or the account may be hacked by the attacker. The web services nowadays provide users' with an alternative email address or security question to recover password. Unfortunately, this authentication mechanism is insecure or unreliable.

To overcome the drawbacks of this mechanism, a backup mechanism for account recovery is considered. Backup authentication mechanism helps the users' to regain accounts with the help of trusted friends. In this mechanism user depends on multiple trustees and recover their account via verification mails. A trust model which is implemented in social networking sites is associated with an authentication protocol. Trust evaluation models are really needed in smart environments is that they create a secure yet more flexible environments because security policies cannot do that. Trust systems are very adaptive to the user needs, actions and behaviors.

Peer-review under responsibility of the Organizing Committee of ICCCV 2016

Keywords: trusted authentication; Blowfish algorithm; Password recovery

1. Introduction

Authentication is a mechanism in which the credentials provided are compared to those on file in a database of authorized users' information on a local operating system or within an authentication server. Social networking sites have become popular in recent time. However, in traditional authentication mechanism password,

* Corresponding author. *E-mail address:* kumud.shailee@gmail.com

Peer-review under responsibility of the Organizing Committee of ICCCV 2016
doi:10.1016/j.procs.2016.03.085

fingerprint, security questions are used [9]. However, password based authentication didn't provide strong security for the system with sensitive data. Many attackers are still able to overcome those security countermeasures by different techniques. Currently used authentication mechanism security question is easily guessable and phished by the attackers.

In Social networking sites, general users are involved with a number of friends. In trustee based authentication users' use trusted friends for account recovery, which is described in this paper. Here authentication is more secure and reliable because user depends on trustees which are selected by him. The user regains the account with the verification codes which he receives from the selected trustees through email which is highly secured than other backup mechanism. Here the account recovery threshold is set while selecting the trustees which (is k=3 k is recovery threshold). The user has to selectonly three trustees and in the account recovery process the user has to get all three verification codes for account recovery. The previous work has shown that any one of the verification code is used for account recovery.

As there are various security issues in sending the messages over social networking sites, the messages are easily decrypted by the attackers. Here we are using the Blowfish algorithm for sending the messages from one user to another user.

2. Literature Survey

Shehab m, squicciarini a, and g [1]: -In this paper proposed an access control framework to manage third party applications. Their solution is based on enabling the user to specify the data attributes to be shared with the application and at the same time able to specify the degree of specificity of the shared attributes.

Bethencourt J, Sahai A, Waters [2]: -The proposed technology is a new model of CP-ABE without source decryption. With this technique they have significant reduction of computing resources imposed on users. This scheme is both secure and verifiable, without relying on random oracles.

LAI Junzuo, DENG R H, and GUAN Chaowen [3]: - They present a technique for realizing complex access control on encrypted data called as a Ciphertext - Policy Attribute-Based Encryption. With this technique, a user's private key will be associated with an arbitrary number of attributes expressed as strings, when a party encrypts a message in our system; they specify an associated access structure over attributes. This technique attributes are used to describe a user's credentials and a party encrypting data determines a policy for who can decrypt. The advantage is that it attains confidentiality even if the server is interested.

LAI Junzuo, DENG R H, and GUAN Chaowen [5]: - They proposed Multi-message Ciphertext Policy Attribute Based Encryption (MCP-ABE) technique. In this it encrypts multiple messages within one cipher text so as to enforce flexible attribute-based access control on scalable media. The scheme constructs a key graph which matches users' access privileges, encrypts media units with the corresponding keys, and then encrypts the key graph with MCPABE; only those data consumers with the required user attributes can decrypt the encryption of the key (sub) graph and then decrypt the encrypted media units

J. Brainard, A. Juels, R. Rivest, M. Szydlo, and M. Young [4]: -They proposed trustee-based social authentication and combined it with other authenticators (e.g., password, security token) as a two-factor authentication mechanism.

S. Schechter, S. Egelman, and R. W. Reeder [15]: - 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.

From the above mentioned papers, we studied that there are various security issues in social authentication process and the user data privacy is compromised. 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. Specifically, a user's security in a trustee-based social authentication relies on the security of his or her trustees. There are various encryption techniques used for access control, but they have certain issues.

The objective of this proposed system is to overcome the various drawbacks and evaluates the trustworthiness of communicating entities before the phase of service provision. In proposing system we tend to detect attackers and try to optimize the number of attacks, and do safely data dissemination from one user to another user without data missing and with using a high security process. The proposed approach can protect user and platform privacy.

3. Existing System

The existing backup authentication mechanism uses 'secret' questions and alternate email addresses for account recovery if the users forgets his password or account is being compromised [11] [13]. Unfortunately, this method of authentication is unreliable.

If the user is using the personal question for authentication, it is often possible that a user may forget the answers, or is easily guessable by the attackers. If the user tries to authenticate by using an alternate email address may finds that the configured address is expired .Hence this authentication mechanism has certain loop holes. In the existing system, there is no constraint on selection of trustees which affect the security of the system. The verification code from any one of the selected trustees can recover passwords, but this code can easily phished by the attackers and thus the user can be compromised. Previous work does not show the mechanism of safely data dissemination from one user to another. As there are various security issues in existing social authentication and the user data privacy is compromised. The objective of this proposed system is to overcome the various drawbacks and evaluates the trustworthiness of communicating entities before the phase of service provision. In proposing system we tend to detect attackers and try to optimize the number of attacks, and do safely data dissemination from one user to another user without data missing and with using a high security process. The proposed approach can protect user and platform privacy

4. Proposed Methodology

The proposed methodology introduces social authentication for account recovery. This scheme uses multifactor authentication process.The proposed methodology comprises of two phases.

1. Registration Phase
2. Recovery Phase

Registration Phase:The fig 1 shows registration phase. It includes following modules.

a. User Registration: - In this phase first the registration details of the user with username is registered. The user is the main authenticator with the password and email address and details of the user are saved .Whenever the user tries to login into his account an email is received by the user by the service provider about the login details such as IP address and login time. Hence, if the attacker tries to hack user account,user will come to know about it, which provides better security than existing system.

b. Add Friends:-Here the user can add the friends in the users' friend list.The user can add any number of friends.

c. Selection of Trustees:- The user selects the trusted friends from the friend list. Here we are selecting three trusted friends of the user, not more than three friends should be selected. These trusted friend list is saved in a trust friend list.

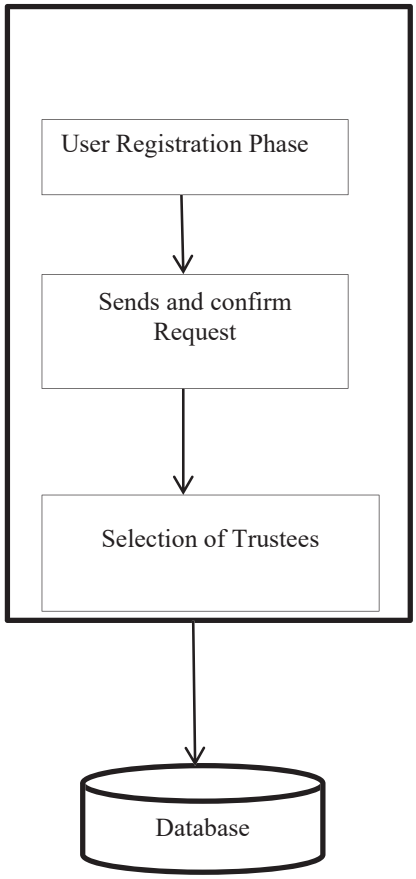

Fig 1 Registration Phase

Recovery Phase: The Fig 2 shows the recovery phase of account recovery.In this phase if the user forgets his or her password or is compromised by the attacker, he can recover his password with the help of selected trustees in this phase. The user sends the account recovery request with his username to the service provider. Then the service provider, sends the verification codes to the selected trustees. Now the trustees have to send the codes which they have received via email from the service provider to the user through email.Here in the proposed system we are using all the three verification codes from the trustees.Here the user uses the sum of three verification codes for account recovery,whereas in existing system it uses any one of the verification code to recover password which is not secured and reliable.The proposed approach of selecting trustees is much more reliable and secured,even if the attacker phishes the trustee account and gets the verification code ,then he can easily gets users password.But the proposed system uses sum of all the three verification code to recover password.Hence this scheme is most reliable in terms of security.

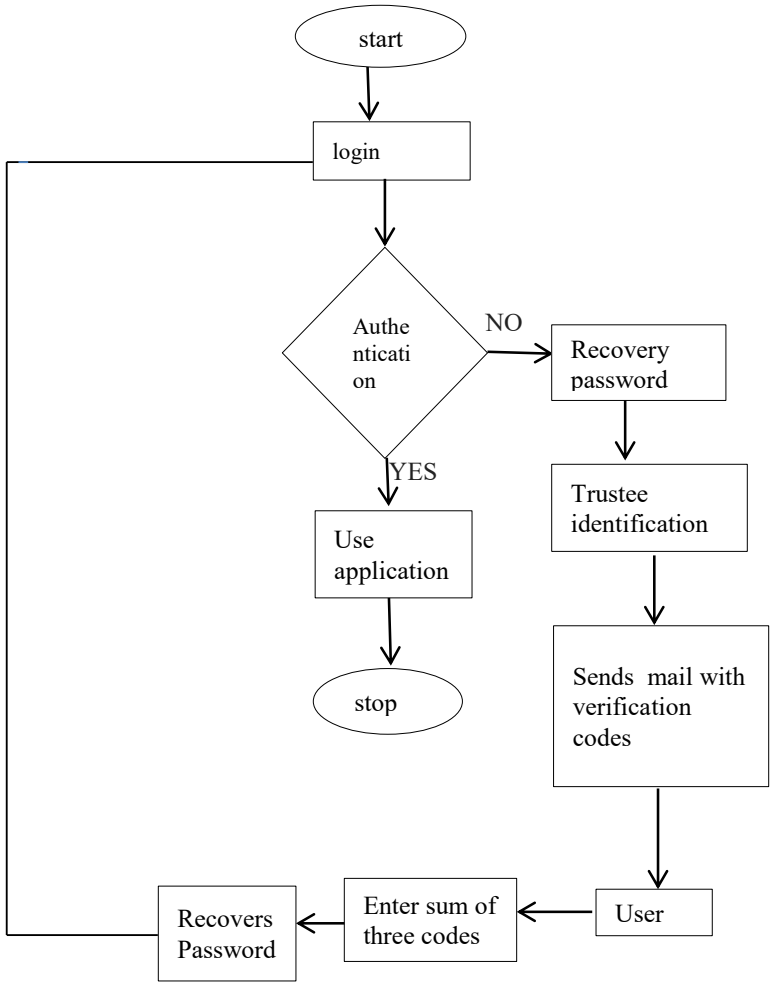

Fig 2 Recovery Phase

Security Module:Authentication is essential for securing your account and preventing spoofed messages from damaging your online reputation. In this module we are providing the high security of data dissemination from one user to another without data missing through blowfish encryption decryption algorithm.

5. Results and observations

Here we are using NetBeans IDE 8.0.2, WampServer.

Fig 2 shows the two key generation, key1 from blowfish algorithm and key2 from key generation algorithm

Blowfish Algorithm: Blowfish is an encryption algorithm. This algorithm uses a variable-length, key from 64 bit block cipher. The above fig shows during data dissemination from one user to another we are using blowfish algorithm. Key 1 which is variable length key is generated by blowfish whereas key 1 from the normal key generation algorithm.

The advantage of this algorithm is that it suffers from weak key problems; no attack is known to be successful against it

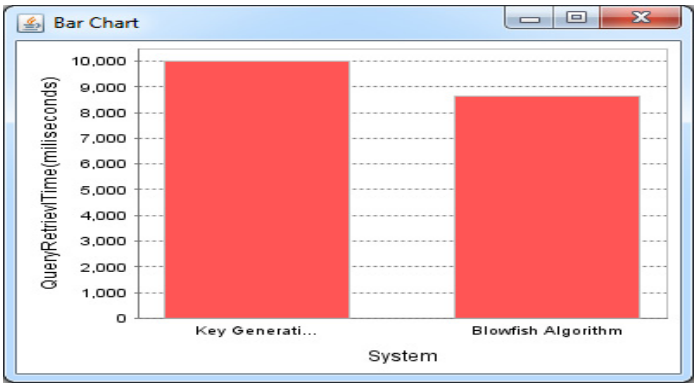

Fig 3 shows the comparison key generation algorithm and Blowfish algorithm.

The Fig 3 shows the performance graph of Blowfish algorithm and key generation algorithm. From the observations we can conclude that while sending message from one user to another this algorithm is more reliable and secured from attackers. This Blowfish have better encryption than other algorithms because it is stronger against data attacks.

6. Conclusion

In this paper new proposed scheme is introduced of how to select the trustees in order to minimize the attacks and increases the security of the system.The, various authentication techniques are introduced which have their own advantages and disadvantages. The proposed Trustee –based authentication method is used to recover user's account by sending security codes to user's trustees who is more reliable than the existing system, which uses security questions to recover the user's account.The proposed strategy uses the sum of three verification code to recover password in contrast to existing systems which uses any one of verification coders. The proposed system uses Blowfish algorithm is used for data dissemination from one user to another user, providing a high level of security. Blowfish algorithm is used for encryption and decryption .In future the paper involves the SQL injection based attacks in the social networks and also checking on the usability level of bit stuffing length.

References

1. Shehab m, squicciarini a, and g, "Access control for online social networks, third party applications", IEEE 2012.
2. Bethencourt J, Sahai A, Waters, "Cipher text-Policy Attribute-Based Encryption", IEEE 2007
3. LAI Junzuo, DENG R H, GUAN Chaowen, "Attribute-Based Encryption With Verifiable Outsourced Decryption", IEEE 2013
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. 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.
6.]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.
7. A. Rice. (2011, Jan.). Facebook's Knowledge-Based Social Authentication [Online]. Available: http:// blog.facebook.com/blog.php?post=486790652130
8. (2013, May). Facebook's Trusted Contacts [Online]. Available: goo.gl/xHmVHA
9. M. Zviran and W. J. Haga, "User authentication by cognitive passwords: An empirical assessment," in Proc. 5th Jerusalem Conf. Inform. Technol. (JCIT), 1990.
10. J. Brainard, A. Juels, R. L. Rivest, M. Szydlo, and M. Yung. Fourth-factor authentication: somebody you know. In CCS '06: Proceedings of the 13th ACM Conference on Computer and Communications Security, pages 168–178, New York, NY, USA, 2006. ACM.
11. A. Rabkin. Personal knowledge questions for fallback authentication: security questions in the era of facebook. In SOUPS '08: Proceedings of the 4th Symposium on Usable Privacy and Security, pages 13–23, New York, NY, USA, 2008. ACM.
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.
13. 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.
14. B. Schneier, Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish) Fast Software Encryption, Cambridge Security Workshop Proceedings (December 1993), Springer-Verlag, 1994, pp. 191-204.
15. 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.
16. Neil Zhenqiang Gong, Di Wang ," On the Security of Trustee-Based Social Authentications", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 8, AUGUST 2014