Implementation of Identity Authentication Model for Online Social Network

Ms. Snehal D. Rajgure, Dr.A.S.Alvi

Abstract— Identity authentication model is new security approach to verify users identity before performing any important operations When user wants to perform any operation regarding documents, change password, password recovery he have to go through identity authentication model. It consists of three approaches: 1.Trustee based social authentication system, 2. Knowledge-Based Social Authentication Systems, 3. 3d Security code Verification. 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.

Index Terms— Social authentication ,backup authentication, security model.

1 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. So the new model is developed known as identity authentication model for online social network [1].

Identity authentication model is new security approach to verify users identity before performing any important operations. When user wants to perform any operation regarding documents, change password, password recovery he have to go through identity authentication model. At the time of registration user will choose which authentication approaches should be used by the system to verify his identity. It consists of three approaches: 1.Trustee based social authentication system, 2. Knowledge-Based Social Authentication Systems, 3. 3d Security code Verification. Now the User can choose minimum one and maximum three approaches at a time. These model will provide protection against novel frame work of attack basically known as forest fire attack , password guessing attack and shoulder surfing attack.

- *Snehal D. Rajgure is currently pursuing masters degree program in Comp.Science Department at PRMIT&R, Badnera.*
- *Dr. A. S.Alvi is currently working as an Professor in Comp.Science Department at PRMIT&R, Badnera.*

Identity authentication model will give excellent security policies. It will provide easily locking or unlocking system. In this model security provided to every activity such as Uploads/downloads, Change password,Change security model,Password recovery.

2 RELATED WORK

Trustee-based social authentication has attracted increasing attentions and has been shown to be a promising backup authentication mechanism [2], [3], [4], and [5].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 [2], [4], [5]. 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 Moreover, Facebook announced its trustee-based social authentication system called Trusted Friends in October, 2011 [4], and it was redesigned and improved to be Trusted Contacts [5] in 2013.

These previous work either focus on security at individual levels [2], [3] or totally ignore security [4], [5].In fact, security of users are correlated in trustee-based social authentications, in contrast to traditional authenticator (e.g.,passwords,security questions, and fingerprint) 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.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.

3 OBJECTIVE

This project looks to meet some of the following objectives:

- To develop a secure and official social networking site.
- To implement new Identity Authentication Model to verify users identity and improve security of social networking.
- To increase security of documents stored on social networking using AES encryption techniques.
- To prevent attacks occurring on current social networking sites
    - forest fire attack
    - Password guessing attack
    - shoulder surfing attack

4 PROBLEM DEFINATION

Today Gmail, facebook mostly rely on passwords to authenticate users. Sometimes it may cause problem such as password is changed by hacker or forget password which result in the failures to access their own accounts. There exist different attacks such as forest fire attack, shoulder surfing attack which directly affect on users security.

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. For these reasons, it is important to design a secure and reliable authentication mechanism.

5 MODULES

Following are the modules of the project:

- Admin
- User management
- Encryption/Decryption
- Identity Authentication Model
    - Trustee-Based Social Authentication Systems
    - Knowledge-Based Social Authentication Systems
    - 3d Security code Verification

1.Admin:

- View users log
- View occupied server space reports
- View account locking summary

2. User management**:**

- Registration
- Login/Logout
- Group creation
- Send friend request
- Accept friend request
- Delete friend

3.Encryption/Decryption**:**

- When user uploads any document, system will upload it in encrypted format.
- Proposed system will use AES for encryption and decryption.
- Every document will have unique key for encryption/decryption .
- When user wants to download/decrypt any document, he have to prove his identity by using Identity Authentication model.

4 .Identity authentication Model**:**

- This is new security approach to verify users identity before performing any important operations
- When user wants to perform any operation regarding documents, change password, password recovery he have to go through identity authentication model.
- At the time of registration user will choose which authentication approaches should be used by the system to verify his identity.User can choose minimum one and maximum three approaches.

A. Trustee-Based Social Authentication Systems:

- User will register no. of trustees from already registered users
- Specify trustee related security question and answers
- At the time of identity authentication system will ask user about any of the specified trustee related security questions
- If user specified correct answer, system will proceed further otherwise authentication will be failed

B. Knowledge-Based Social Authentication Systems:

a. Behavioral Pattern based question creation

system will create any intelligent question with the help of historical data about users account.If user specifies correct answer, users identity will be proved

b. Personal questions selection

At the time of registration user will specify his personal information in the form of questions and answers. System will fetch any of the specified question randomly

C. Security code Verification**:**

- In this approach, system will generate unique security code every time using users personal information and historical data.
- Code will be generated randomly using user defined algorithm.
- System will generate the algorithm run time.
- The generated code will be sent to users email id.
- User has to specify correct code picked from registered email id.

6 CONCLUSION

Web services today most commonly rely on passwords to authenticate users but there are different security issues such as forest fire attack, shoulder surfing attack and password guessing attack. Identity authentication model provide security against this attack.It verify users identity before performing any task.In this model security is given to every activity such as uploading,downloading, change password and password recovery. It increases the security of documents stored on social networking using AES encryption technique.

REFERENCES

[1] Di Wang "On the Security of Trustee-Based Social Authentications" IEEE Transactions on information forensic and security, vol. 9, no. 8, august 2014.

[2] 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.

[3] 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

[4] *Facebook's Trusted Friends* [Online]. Available: https://www.facebook.com/notes/facebook-security/introducing-trusted-friend,oct 2011.

[5] *Facebook's Trusted Contacts* [Online]. Available: https://www.facebook.com/notes/facebook-security/introducing-trusted-contacts, may 2013.