Authentication from Forest Fire Attacks using Trustee Based System

Anwaya Patil[1], Kalpana Thakare[2], Kishor Sadafale[3]

[1] *Student, Information Technology, Sinhgad College of Engineering, Pune, Maharashtra, India*
[2] *Associate Professor, Information Technology, Sinhgad College of Engineering, Pune, Maharashtra, India*
[3] *Assistant Professor, Information Technology, Sinhgad College of Engineering, Pune, Maharashtra, India*

---***---

Abstract - *Social networking has become more popular from last few decades for users to meet and interact online. Users spend their significant amount of time to share their personal information on social networking sites such as Gmail, Twitter, Facebook etc. Password provides reliable security and protection against unwanted access to resources to the social network platform. Password security like textual password or graphical password is not convenient to the users who forget their passwords. To overcome the drawback of these authenticators, a backup authentication mechanism is taken into consideration. Backup authentication mechanism helps the users to regain their passwords. Recently, a new backup authentication mechanism called as trustee based social authentication has shown promising results. In this authentication method, every user depends on multiple trustees for backup* ***mechanism. So hacking of one user's profile affects*** *many numbers of users. This is* ***called as "Forest Fire attack"*** *In this paper, the concept is on the trustee based social authentication in which users select trustees and recover their account via verification mails. The security mails generated by the system gives more secured trustee based authentication system.*

Keywords—Authentication methods, Social Authentication, Backup Authentication Mechanism, Trustee based authentication

1. INTRODUCTION

Authentication has become most important means for an organization to provide accuracy and reliable security against recent events of thefts and terrorism [1]. The authentication methods is classified into three broad categories namely token based (two factor), biometric based (three factor) and knowledge based(single factor) authentication [2].

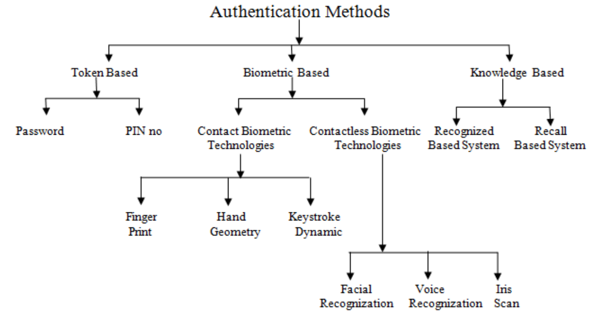

Fig. 1 Classification of Authentication Methods

A. Token Based Authentication

It is based on something you possess, for example Smart Cards, a driver's license, credit card, a university ID card etc. It allows users to enter their username and password in order to obtain a token which allows them to fetch a specific resource - without using their username and password. Once their token has been obtained, the user can offer the token - which offers access to a specific resource for a time period - to the remote site [3]. Many token based authentication systems also use knowledge based techniques to enhance security [2].

B. Biometric Based Authentication

In ancient Greek Biometrics bios="life" and metron ="measure" is the study of automated methods for uniquely recognizing humans, based upon one or more intrinsic physical or behavioral traits [4]. A biometric scanning device takes a user's biometric data, such as an iris pattern or fingerprint scan, and converts it into digital information a computer can interpret and verify. A biometric-based authentication system may deploy one or more of the biometric technologies: voice recognition, fingerprints, face recognition, iris scan, infrared facial and hand vein thermo grams, retinal scan, hand and finger geometry, signature, gait, and keystroke dynamics [6]. Biometric identification depends on computer algorithms to make a yes/no decision. It enhances user service by providing quick and easy identification [7].

C. Knowledge Based Authentication

Knowledge based techniques are the most extensively used authentication techniques and include both text based and picture based passwords [2]. Knowledge-based authentication (KBA) is based on something you know to identify you For example a Personal Identification Number (PIN), password or pass phrase. It is an authentication scheme in which the user is asked to answer at least one "secret" question [8]. KBA is often used as a component in multifactor authentication (MFA) and for self-service password retrieval. Knowledge based authentication (KBA) offers several advantages to traditional (conventional) forms of e-authentication like passwords, PKI and biometrics [9].

2. LITERATURE REVIEW

From last few years, the major problem in the society is to protect the system from malicious attacks. To secure the system is to be reliable for the users. Passwords are the secret between the user and verifier. But these passwords are hacked by the attackers to steal the personal and professional information. There are several different techniques with various algorithm implemented with high feature. Authentication is simple but to protect the system is one of the tough jobs.

Several authentication systems with different techniques and methods that exist in the literature are discussed in this section which helps the user to secure their account from the malicious attacks.

1. Textual password:

The most common method to secure the account is textual authentication method which uses alphanumerical usernames and passwords. The main drawback to use these alphanumeric passwords is that they are hard to remember.

2. Graphical Password:

Graphical password is a technique used to overcome the drawbacks of textual password. Graphical passwords can be used against dictionary attacks, social engineering, eves dropping etc. The main disadvantage of graphical password is that they are vulnerable to shoulder surfing.

3. Session Password:

Textual passwords and graphical passwords are vulnerable to various attacks like shoulder surfing, dictionary attacks, eves dropping etc. Both these techniques have their own drawbacks. Passwords are complicated to remember. The solution to this problem is session password which is a combination of both the textual password and graphical password.

4. Multitouch Gesture Based Authentication:

In addition to authentication methods, one more technique called as multitouch gesture based authentication. This technique provides canonical sets of 22 multi touch gesture of hand and finger movements.

5. Social Authentication

In general, depending on how the friends are involved in the authentication process, social authentications can be classified into two categories, i.e., trustee-based and knowledge based social authentications. In trustee-based social authentications [10], which are studied in this paper, the selected friends (i.e., trustees) aid the user in the authentication process. Knowledge-based social authentication, however, asks the user questions about his or her selected friends. In such systems, friends are not directly involved.

1. Knowledge-based social authentication systems:

Such social authentications are still based on something you know. Yardi et al. [15] proposed a knowledge-based authentication system based on photos to test if a user belongs to the group (e.g., interest groups in Facebook) that he or she tries to access. Facebook recently launched a similar photo-based social authentication system [16], in which Facebook shows a few photos of a friend of a user and asks the user to name the friend. Such system essentially relies on the knowledge that the user knows the person in the shown photos. However, recent work has shown, via theoretical modeling [17] and empirical evaluations [18], that photo-based social authentication are not resilient to various attacks such as automatic face recognition techniques, questioning their use as a backup authentication mechanism.

2. Trustee-based social authentication systems:

Authentication is traditionally based on three factors: something you know (e.g., a password), something you have (e.g., a RSA Secure ID), and something you are (e.g., keystroke dynamics).Brainard et al. [10] proposed to use the fourth factor, i.e., somebody you know, to authenticate users. We call the fourth factor as trustee-based social authentication. Originally, Brainard et al. combined trustee-based social authentication with some other factor as a two-factor authentication mechanism. Later, trustee-based social authentication was adapted to be used as a backup authenticator [11,12, 13]. For instance, Schechter et al. [14] designed and built a prototype of trustee based social authentication system which was integrated into Microsoft's Windows Live ID system. Moreover, Facebook announced its trustee-based social authentication system called Trusted Friends in October, 2011 [12], and it was redesigned and improved to be Trusted Contacts [11] in May, 2013.

3. COMPARISION

In this section, the overall comparisons of all the authentication techniques are discussed. Different authentication methods are discussed from textual to social authentication. Backup authentication involves knowledge based and trustee based authentication. It is represented in the table below

TABLE 1. COMPARISON OF DIFFERENT AUTHENTICATION

	Author	Paper Title	Work Done	Problem Found
1	Lawrence O'Gorman et. al[2003]	Comparing Passwords, Tokens, and Biometrics for User Authentication	In this paper, author examines passwords, security tokens, and biometrics which we collectively call authenticators—and compares these authenticators and their combinations	Deficiencies to identify comprehensive picture of user
2	Ariel Rabkin et. al[2008]	Personal knowledge questions for fallback authentication: Security questions in the era of Facebook	Author describes the password retrieval mechanisms for a number of personal banking websites, and found that many of them rely in part on security questions with serious usability and security weaknesses	Today's personal security questions owe their strength to the hardness of an information-retrieval problem
3	Nick Feamster et. al[2008]	Photo-Based Authentication Using Social Networks	A framework for authenticating members of groups using photographs.	Implementing Lineup in a real-world social network to choose the pictures
4	Stuart Schechter et. al[2009]	It's Not What You Know, But Who You Know	Backup authentication mechanisms help users who have forgotten their passwords regain access to their accounts—or at least	The users must remind of who their trustees are. While email-based attacks

			try	were largely unsuccessful
5	Racha Ajami et. al[2011]	Security Challenges and Approaches in Online Social Networks: A Survey	Paper describes, different research groups highlighted the security threats in social networks and attempted to offer some solutions to these issues	None of the mechanisms provided the users with control over what others can reveal about them; and encryption of images is still not achieved properly
6	Iasonas Polakis et. al.[2012]	All Your Face Are Belong to Us: Breaking Facebook's Social Authentication	Author studied the threat model and how attacker attack on information needed to solve the challenges	Face recognition software and services can be effectively utilized to break social authentication tests with high accuracy
7	Barbara Carminati et. al[2012]	Trust & Share: Trusted Information Sharing in Online Social Networks	OSNs to be one of the most promising paradigms for information sharing on the Web	The problem is that some of the most known social networking sites have not been always honest and transparent with respect to user privacy
8	Neil Zhenqiang Gong et. al[2014]	On the Security of Trustee-based Social Authentications	Trustee-based social authentication, i.e., authenticating users with the help of their friends, has been shown to be a promising backup authentication mechanism	The problem is to apply our framework to extensively evaluate various attack anddefense strategies using three real-world social network datasets

4. PROPOSED SYSTEM

Trustee based social authentication works for a user Alice. The system consists of two phases: Registration phase and Recovery phase. Firstly, a user will provide a friend list to the service provider for registration. The user or service provider can select trustees. When the attacker attacks the system, the service provider sends verification emails to the trustees. Further, the trustees send verified codes to the system as confirmation. At last, user reset his password. The overall framework of the method is shown in Fig. 2

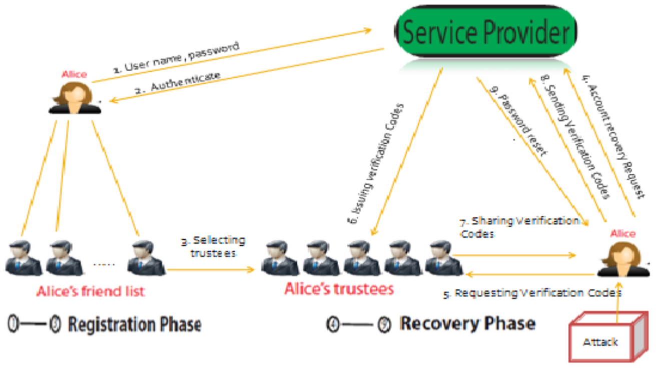

Fig.2: Illustration of a trustee-based social authentication system which consists of Registration Phase and Recovery Phase. In the Registration Phase, Alice is authenticated with the main authenticator, i.e., password, and then several friends are selected by either Alice herself or the service provider from Alice's friend list and are appointed as Alice's trustees. In the 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.

1. Registration Phase. In the Registration Phase, the system prepares trustees for Alice. Specifically, Alice is first authenticated with the 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.

2. Recovery Phase. In the 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. Specifically, Alice first sends an account recovery request with her username to the service provider which then shows Alice an URL. To obtain verification codes from her predefined trustees, Alice is required to share this URL with her trustees via emailing them, calling them, or meeting them in the system and retrieve the 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 number (e.g., 3) of verification codes and presents them to the service provider, then Alice is authenticated and is directed to reset her password. We call the number of verification codes required to be authenticated the recovery threshold. Note that it is important for Alice to know who her trustees are in the Recovery Phase. Schechter et al. [13] 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 trustee based social authentication systems which use the architecture shown in Figure 1 and were implemented by Microsoft [13] and Facebook [11, 12], respectively. Microsoft's trustee-based social authentication: Schechter et. al. [13] designed and built a trustee-based social authentication system and integrated it into Microsoft's Windows Live ID service. In the Registration Phase, users provide four trustees. The recovery threshold is three, i.e., a user is authenticated if he or she obtains verification codes from at least three trustees in the Recovery Phase. Moreover, users will be reminded of their trustees.

Face book's trustee-based social authentication: Facebook announced its first trustee-based social authentication system called Trusted Friends in October, 2011 [12]. In May, 2013, Facebook announced its redesigned and improved Trusted Friends which they renamed as Trusted Contacts [11]. In the Registration Phase of Trusted Contacts, a user needs to select three to five friends from his or her friend list as the trustees. Similar to the Microsoft's trustee-based social authentication, the recovery threshold is set to be three. Differently, Facebook does not remind a user of his or her trustees, but it asks the user to type in the names of his or her trustees instead. However, once the user gets one trustee correctly, Facebook will remind him or her of the remaining trustees. Both trustee-based social authentication systems ask users to select their own trustees without any constraint. In experiments the trustees selected with a constraint imposed by the service provider can achieve better security guarantees. Moreover, none of these work performed rigorous studies to support the choice of three as the recovery threshold. In fact, experimental results show that setting the recovery threshold to be four could better balance between security and usability.

5. ARCHITECTURE OF TRUSTEE BASED AUTHENTICATION SYSTEM

Firstly, a user will provide a friend list to the service provider for registration. The user or service provider can select trustees. When the attacker attacks the system, the service provider sends verification emails to the trustees. Further, the trustees send verified mails to the system as confirmation. At last, user reset his password. The overall framework of the method is shown in Fig. 3

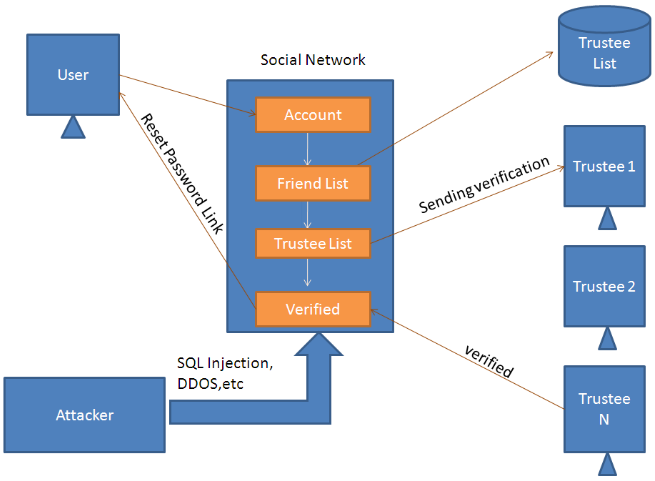

Fig. 3 Workflow for Authentication

1. Registration Phase

User's Login. In user login, user can create account with his/her email id. Email id must be unique. If one user uses the email id to register, he cannot use the same email id to register for another account.

Send/Confirm friends request. User can send the friend request to the other users and also receive the friend requests from other users.

Trustee's Selection. In this step, the user selects trustees from their friends list. If the user wants to select other trustees, they have to reset it to select the other trustees. This will automatically update in the server. The trustee network selection is the more important job in social authentication system

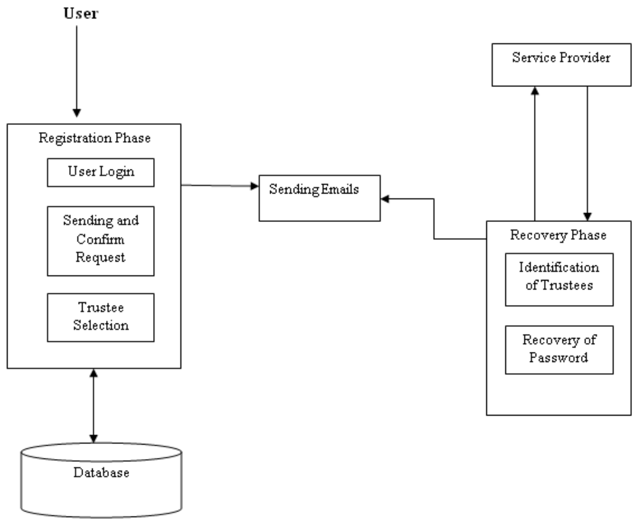

Fig. 4 Architecture of Trustee Based Authentication System

2. Recovery Phase

Identify Trustee's. In this step, the user first selects one correct trustee name for account recovery. If the user selects correct trustee, then the system automatically display trustee name. Otherwise user will not allow accessing the account.

Reset Password. In this step, user allowed to reset their password in the case of password or email id loss. Fig.4. represent the architecture of trustee based authentication and its work flow in Fig.3.

6. RESULTS AND ANALYSIS

The concept of social authentication and requested that participants consider who they would choose as trustees for their account. We asked each participant to list trustees' names and email addresses of the trustees. In experiment we invited 10 of our prior participants to earn a software gratuity by obtaining account-recovery mails from trustees they had previously identified. Emails inviting participants to the study were sent at evenly divided intervals 2 over that time. This distribution ensured that we would not favor a particular time of the day or week that might be better or worse for contacting trustees.

TABLE 2. DISTRIBUTION OF TIME TO COMPLETE EACH STEP OF EXPERIMENT

User	Min time(ms)	Max time(ms)
1	800	1700
2	900	1645
3	1100	2100
4	757	1200
5	895	1000
Avg	890.4	1529

According to Table 2 Trustee based system gives the distribution of time required for the user to select trustees and recovery of password from the email further fig 5 show the graphical representation of maximum and minimum time required for respected user to complete the task.

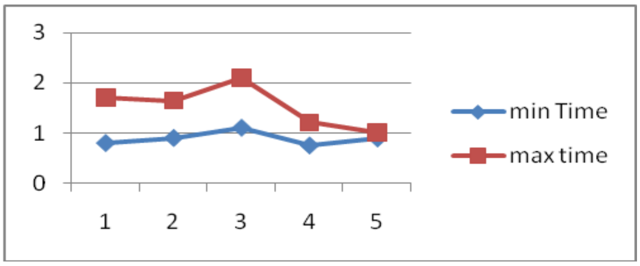

Fig. 5. Distribution of time for selection of trustee

The main purpose of the experiments is to validate hacking possibility of trustee based authentication system. From the experimental result, the compromises probability of user is high. Because trustee based authenticate is depend on the user's friends. So if compromising one user affects many of the friends also.

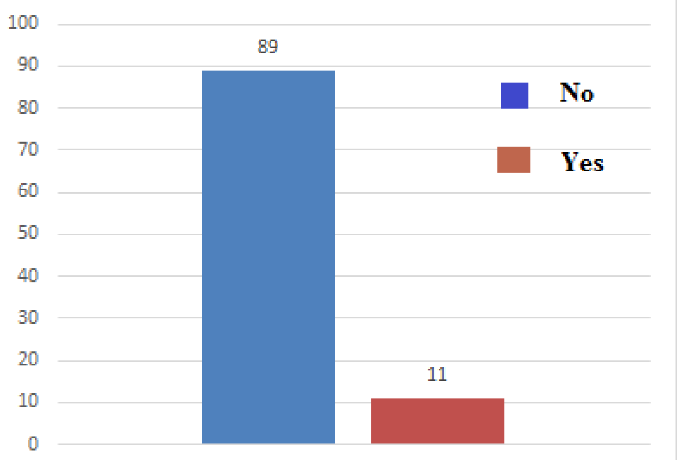

Fig. 6 Compromises probability of user

The attacker compromised the user profile through various ways. Attacker creates the fake account in social network. Then they use this fake account for illegal activity. The fake account in social network is also called as Sybil node. Figure 5 shows the expected number of compromised users. Compromised user percentage is increases bases on number of attackers in their network. Only few of the user's has the strong and secure password. The attacker hack the uncompromised user account through fake (Sybil) profile. In Sybil attack, the attacker send friend request from fake id. If the users accept his friend request then they steal the information from the social network site and use the information for hacking account. Otherwise they attack the user through user friend's networks. Figure 6 shows the percentage of compromised users through friends. The attacking account through neighbor node is also called as mutual friends based attack. The attacker calculate user nearest neighbors then they attack the user through the nearest neighbor node. The cost of the attack is based on the number of iteration used to compromise the particular account.

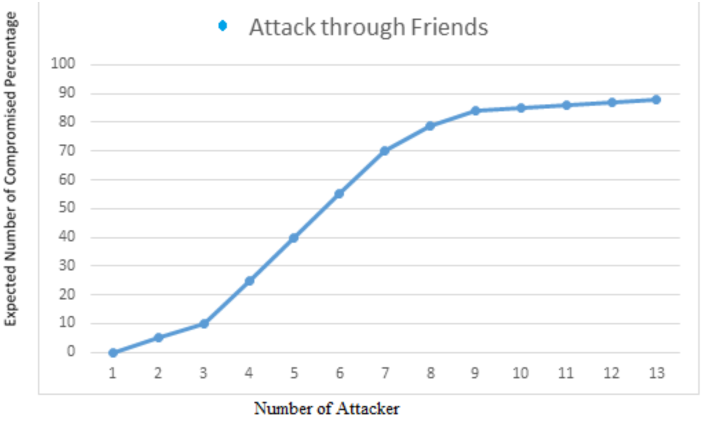

Fig. 7 Percentage of compromised user through friends

7. CONCLUSION

Recently, various authentication techniques and methods are introduced in the market but each one of them has their own advantages and disadvantages. Due to the growing interest in using social networks platform which has created a key factor to attack on the system. Despite of several techniques, very few frameworks are implemented and tested. In view of the above, a system has been proposed in the literature that is called as real social trustee based authentication. Although the social authentication helps to reduce the existing problems but it has some limitation like other two factor methods. To conclude, we need a highly robust authentication system that provides a better reliability and security. Currently, the researchers are working on the trustee based authentication systems that provides highly secured authentication.

The future scope includes the various attacks on the account with the defense strategies and also checking the reliability and security of the social networks.

References

[1] Hafiz Zahid Ullah Khan, "Comparative Study of Authentication Techniques", International Journal of Video & Image Processing and Network Security IJVIPNS Vol: 10 No: 04

[2] Approaches to Authentication: http://www.e.govt.nz/plone/archive/services/see/see-pki-paper-3/chapter6.html?q=archive/services/see/see-pki-paper-3/chapter6.html [Last Visited on 15/05/2011].

[3] Token Based Authentication: http://www.w3.org/2001/sw /Europe/events/foaf galway/papers/fp/token_based_authentication/ [last visited on 02/05/11].

[4] Biometric Authentication: http://www.cs.bham.ac.uk/~mdr/teaching/modules/security/lectures/biometric.html [Last visited on 02/05/11].

[5] Roman V. Y., "User authentication via behavior based passwords," Systems, Applications and Technology Conference. Farmingdale, NY. 2007.

[6] A. Jain, R. Bolle, and S. Pankanti, Eds. "Biometrics: personal identification in networked society", Boston, MA: Kluwer Academic, 1999.

[7] A.R. Hurson, J. Ploskonka, Y. Jiao, and H. Haridas, "Security issues and Solutions in Distributed heterogeneous Mobile Database Systems", Vol. 61, Advances in Computers, 2004, pp. 107-198.

[8] Knowledge based Authentication: http://searchsecurity.techtarget.com/definition/knowledge-based-authentication [Last Visited on 02/05/11].

[9] Knowledge Based Authentication: http://csrc.nist.gov/archive/ kba/index.html [Last Visited on 02/05/11].

[10] J. Brainard, A. Juels, R. L. Rivest, M. Szydlo, and M. Yung. Fourth-factor authentication: Somebody you know. In CCS, 2006.

[11] Facebook's Trusted Contacts. https://www.facebook.com/notes/facebook-security/introducing-trusted contacts/10151362774980766.

[12] Facebook's Trusted Friends. https://www.facebook.com/notes/facebook-security/national-cybersecurity

[13] S. Schechter, S. Egelman, and R. W. Reeder. It's not what youknow, but who you know. In CHI, 2009.

[14] Bad Rank. http://pr.efactory.de/e-pr0.shtml.

[15] S. Yardi, N. Feamster, and A. Bruckman. Photo-based authentication using social networks. In WOSN, 2008.

[16] A. Rice. Facebook's knowledge-based social authentication. http://blog.facebook.com/blog.php?post=486790652130.

[17] H. Kim, J. Tang, and R. Anderson. Social authentication: Harder than it looks. In FC, 2012