iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 6 **Issue:** IV **Month of publication:** April 2018

**DOI:** http://doi.org/10.22214/ijraset.2018.4611

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887*
*Volume 6 Issue IV, April 2018- Available at www.ijraset.com*

# Advanced Security Improvements using Fallback Authentication for Social Networking

S. Arun Pandian[1], W. Rose Varuna[2]
[1] *Student, Information Technology, Bharathiar University, Coimbatore-641 046, India.*
[2]*Assistant Professor, Information Technology, Bharathiar University, Coimbatore-641 046, India.*

***Abstract:*** ***Password authentication is one amongst the only and also the most convenient authentication mechanisms to manage secret data over insecure networks. It's a lot of frequently needed in areas like computer networks, wireless networks, remote login systems, operation systems, and database management. The password retrieval mechanisms for variety of non-public websites. They found that a lot of them rely in part on security queries with serious usability and security weaknesses. The existing systems are vulnerable to various attacks and fail to serve all the purposes an ideal password authentication scheme should. The password securities are used in the input method of user password authentication. It described which is secure even if an intruder can read the system's data, and can tamper with or eavesdrop on the communication between the user and the system.***

***Keywords: Social Networking, Fallback Authentication, Social Security, Password Authentication, Security.***

## I. INTRODUCTION

Online banking is becoming a widely used way of controlling personal finances. Many users find the convenience by electronic access from personal computers irresistible, despite the possible security risks. By the same token, criminals have found online banking an irresistible target. A recent study of online criminal markets has found that stolen bank login credentials are among the most frequently and sought contraband goods. Further, there are large criminal networks organized to turn these compromised credentials into actual crime. To meet this threat, banks have deployed increasingly sophisticated authentication mechanisms. Most banks exhort, or require, users to pick “strong” passwords, not easily guessed by an attacker. Strong passwords, however, are hard for many users to remember. For usability reasons, banks often couple their password authentication mechanism with some sort of “lost password” mechanism, which users can fall back on if they have forgotten their passwords. For the protection technique and worth of passwords in observe has been studied area unit extensively. For the “fallback authentication” mechanisms are a lot of less studied by the educational community.

## II. RELATED WORK

Security aspect of Fallback authentication has been much researched upon. Even though extensive research has been conducted in improving the security of password authentication, and also in introducing novel techniques for fallback authentication, adequate attention has not been paid to improve the usability and security aspects of the most commonly used fallback authentication technique for many webs based accounts which is Security questions based fallback authentication process. The capability to verify the user identity when an account hijacking attempt has occurred is an integral part of the login risk analysis system. Google researchers along with academics have revealed that current security questions are neither secure nor reliable enough to be used as a backup mechanism to reclaim a lost account. Their argument was that security questions suffer from a fundamental flaw of usable security: the security questions and their answers are either somewhat secure or usable, but rarely both. They also stressed that security questions can still be useful when the risk level is considered low. To design a better extra level of security, it is worth understanding the strength of the answers users provided for security questions. This paper attempts to introduce a set of guidelines to design an interface called “secret question meter”. The “secret question meter” interface provides visual feedback on the strength of answers given in security questions to nudge users towards stronger answers. The designed visual feedback to the user supported method tried to nudge the user towards strong answers for their chosen security queries. The visual representation of answers’ strength to security questions is often presented as a coloured bar on screen. Furthermore, our “secret question meter” interface provides suggestions to help users in choosing strong security queries and their answers. We’ve got integrated suggestions supported method for stronger answers if the user decides to go in conjunction with the weak answer regardless of the feedback from the strength indicator. Mnemonics have been tested and proven to improve memorability on stronger passwords rather than

random passwords with digits and special characters to improve strength. All these mechanisms are not enforced on the user and work as suggestions where the user holds the final decision to set the answer they feel best.

## III.METHODOLOGY

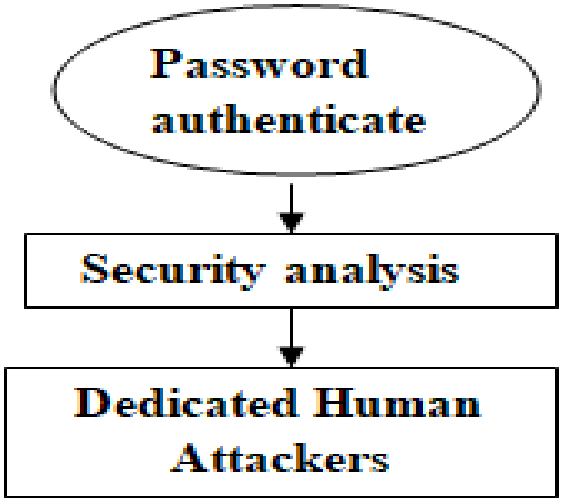



Fig. 1: Proposed Methodology

### A. *Password Authenticate*

As mentioned above, attempted to obtain "forgotten" passwords at social websites. Sample included Gmail sampled included a mix of national, regional, and online-only banks. Four of these sites had know online password-recovery mechanism, and were excluded from further study. It also checked whether the recovery mechanisms changed depending on whether the request originated from a host that had previously been used to access that account. This imposed certain limits on data collection: they did not want to risk the account-holders being locked out of their accounts, and therefore did not attempt to thoroughly explore the mechanisms in use.

1) *Admin Login*: In this Model Admin Person can Access the User Registration Details. The administrator interface allows the administrator to be able to implement editing, inserting, deleting and to check the overall result of all registered users.

### B. *Security Analysis*

To seek only to evaluate the security questions that encountered. They do not purport to do a full security analysis of online banking, or even of the fallback authentication mechanisms in use. Institutions may well adapt the strength of their authentication mechanisms to a variety of cues, such as frequency of access, source address, and so forth, that are difficult for us to control for. Further, such mechanisms change over time, and this study should not be taken to reflect the current state of such mechanisms.

1) *Fallback Authentication:* Fallback authentication is the backup, which approach a user takes to retrieve user account in case of loss of password. Almost all sites, Google, Microsoft, and Facebook that involve user accounts have incorporated fallback authentication methods to facilitate users to regain their accounts in case user lose the password. The other approach utilized for fallback authentication is the security questions based account recovery mechanism. It is commonly argued that fallback authentication should always involve personal information for account recovery, which needs not to be memorized. The fallback authentication to reclaim their account when they have lost the original credentials. Fallback authentication technique for many webs based accounts, which is Security questions, based fallback authentication process. User selected security questions are proven to be most effective in fallback authentication configuration as user defined questions are harder to guess than the predefined questions that are ubiquitous. Google allows users to create their security questions as a part of setting up their fallback authentication method.

### C. *Dedicated Human Attackers*

A still stronger attack is that directed against some specific known user by a fairly dedicated human. an excellent deal of private data is obtainable on-line in unstructured or loosely structured documents. Archival copies of old personal web pages, short newspaper profiles, club membership rosters and the like are all potent sources of personal information to a human attacker, and are all growing in volume and coverage.

Questions such as “what is your home town” are comparatively easy for humans to answer, if the result is indicated by a document in the first few pages of search engine results. Names of pets or family members are not viewed as private, and are often made public via personal web pages and the like. Insidiously, users may have little awareness or control over online information about themselves either published by others, or published and archived, making it difficult for users to assess and minimize their risk. Genealogical in-formation, for instance, is often published without the subjects being informed; old personal WebPages or discussion list emails may be available through archival websites.

## IV. RESULTS


Fig. 1 User login homepage.

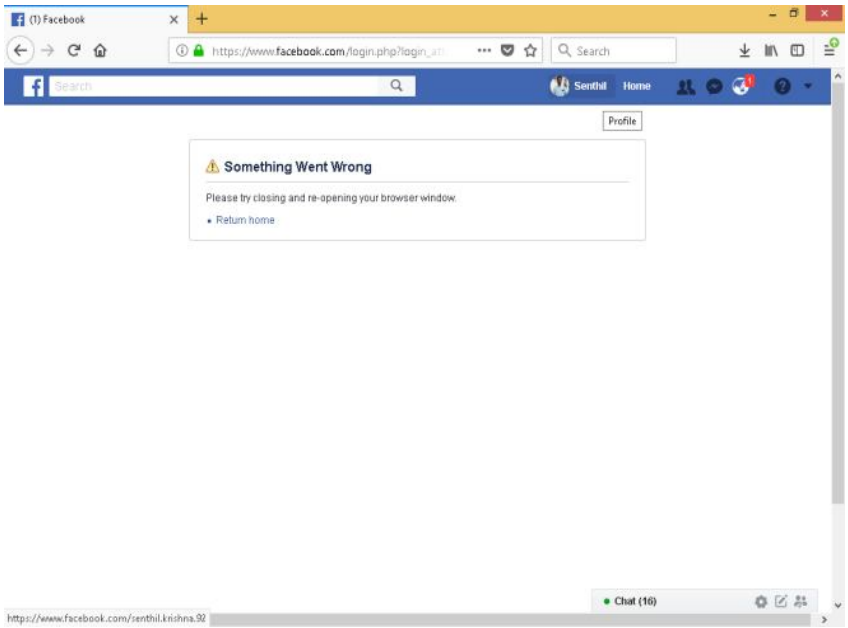



Fig. 2 Blocking anonymous user login

## V. CONCLUSIONS

In early prototype and analysis demonstrates that the usability of privacy settings may be impacting privacy management in online social networking. By providing a higher mental model and improved visual feedback of the result of privacy settings, aim to form utilizing these settings easier for each new and knowledgeable about users. They are currently implementing a more functional audience view interface that includes controls for modifying privacy settings. They plan to evaluate this interface with a more extensive user study to examine the use and impact of this new design.

## VI. FUTURE ENHANCEMENTS

One aspect of this analysis can include what the default settings are appropriate for this new interface. What the current settings should still require additional interfaces, like the controls over the News feed feature on Face book improving the interface, however, will only go therefore far. Long-term analysis agenda is to analyse novel ways in which to manage personal information online as well as methods to better educate users as to the impact of their online behaviours and activities. Enhancement can be done in efficient manner. We can update the following details.

The advanced security improvements in social network web portal providing automatic remainder for password attack.

The advanced security improvements in social network website used send notification through mail or SMS.

## REFERENCES

[1] Acquisti, A. and Gross, R. Imagined communities: awareness, information sharing, and privacy on the Facebook. In the Proceedings of Privacy Enhancing Technology (PET 2006), Cambridge, June 28-30, 2006.

[2] boyd, d. Friendster and publically articulated social networking. In the Extended Abstracts of the Conference on Human Factors and Computing Systems (CHI 2004). Vienna, Austria, 2004, pp1279-1282

[3] boyd, d. and Heer, J. “Profiles as Conversation: Networked Identity Performance on Friendster.” In Proceedings of the Hawai'i International Conference on System Sciences (HICSS-39), Persistent Conversation Track. Kauai, HI: IEEE Computer Society, 2006.

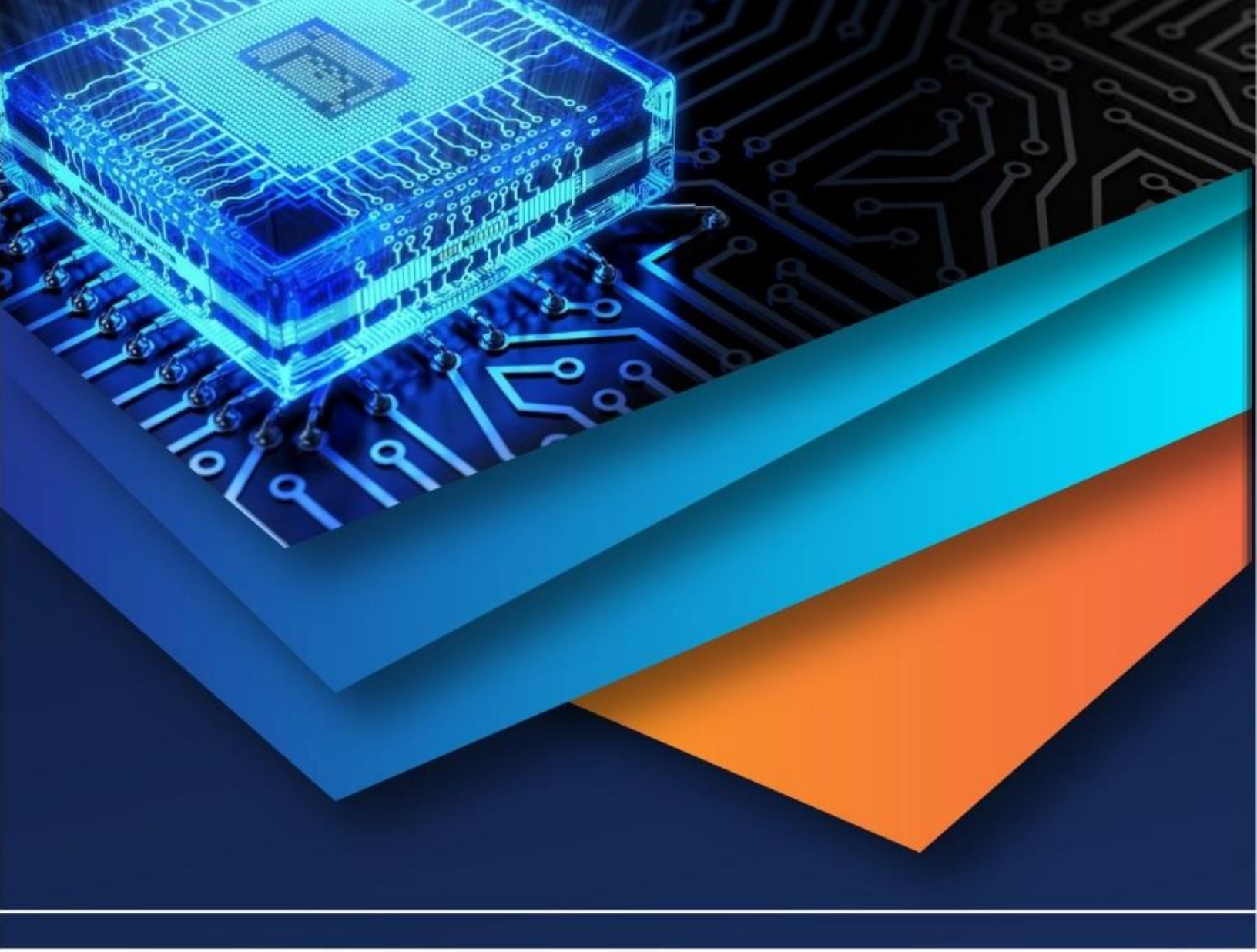
[4] Facebook-Statistics. http://www.facebook.com/press/ info.php?statistics. Accessed January 25, 2008.

[5] Goffman, E. The presentation of self in everyday life. New York: Doubleday, 1959.

[6] Govani, T. and Pashley, H. Student awareness of the privacy implications when using Facebook. Unpublished manuscript retrieved September 2007 from http://lorrie.cranor.org/courses/fa05/tubzhlp.pdf.

[7] Gross, R. and Acquisti, A. Information revelation and privacy in online social networks (the Facebook case). In Proceedings of the 2005 ACM workshop on Privacy in the electronic society, Alexandria, VA, USA, November 7, 2005, pp 71-80.

[8] Strater, Katherine P. and Heather Richter Lipford. Strategies and Struggles with Privacy in an Online Social Networking Community. Unpublished manuscript.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY