Sematral System

Vishal T. Mishra

Computer Engineering, K.J Somaiya Polytechnic

Abstract- Security is the degree of resistance and protection from damage. We set up our password as complex as we can that consist of lowercase and uppercase characters along with special characters to make our profile and various information secure, but what if someone knows this password, are we secure then? To overcome this problem we have come with a solution SEMATRAL SYSTEM. **SE**cure **MA**Trix based **TRA**cing and Login **SYSTEM**, is a central user login control within the browser where we can add up different accounts we want to access securely. SEMATRAL SYSTEM will not only secure the login for the account ID's we add , but will also maintain a log of user activities for the same. This web-app will act as an intermediate layer of security between user and social networking site's traditional login; allowing users to access the account in either of the two way a) Live Login b) Dead login. SEMATRAL SYSTEM's login system will be different from the existing one's i.e Username and Password, it will allow the user to login to system via a unique concept of Matrix based password, eliminating the use of keyboard thus guarding against various key logger viruses. There are many more features in the system. Securing the secured is the main moto of this system.

Index Terms- *Dead Login , Key-Logger, Matrix ,Security, Sematral , Secure login, Web-App.*

I. INTRODUCTION

Security is the degree of resistance and protection from damage. The term security with regards to Social network refers to the security of various user data, user profile, conversations and so on. It has become very important to take necessary steps or follow certain guidelines while setting up username or password to increase the level of security and protect various information data from hackers.

II. CURRENT SECURITY SYSTEM

With Increase in number of cyber crimes taking necessary precautions has become necessary. Most social networking sites as well as other sites make use of login system to secure the user's data. This Login system comprises of username and password, Also various sites forces user to follow certain guidelines while setting up user id and password. Various sites also have their own inbuilt security mechanism to prevent leak of data. The best example of such inbuilt data protection mechanism is Facebook, it allows user to setup various privacy policy giving him/her full control to allow/disallow anyone from sending friend requests, viewing posts or carry out any other activity.

Even after implementation of these security steps, sites are vulnerable to various attacks. Various steps have been undertaken as an effort to increase the security level but still none of the methods implemented achieve higher success.

III. THREATS TO CURRENT LOGIN SYSTEM

Although these high level of security are implemented with the purpose of securing data Attackers still find a way to move over these layers. According to the report released by National Crime Record Bureau (NCRB) there was 18% increase in cyber crime in the year 2014 compared with the cyber crime statistics of 2013.

One of the most common attack to gain login credentials is Phishing. Along with this some of the new techniques includes use of RATS, Key-Logger Viruses, Sql injection, SHELL attack and so on. To overcome all these problems as well as to layer up and level up the security we Introduce to you SEMATRAL SYSTEM.

IV. SEMETRAL SYSTEM

Sematral System stands for SEcure MATrix based TRAcing and Login SYSTEM. It's a Central Login System that acts as an intermediate security layer between user and and sites traditional login system. Once logged in to the Sematral system user can add up different accounts he want to access securely. SEMATRAL SYSTEM will not only secure the login for the account ID's we add , but will also maintain a log of user activities for the same. It will consist of two login feature that can be used i.e. enabled or disabled by the user as per his/her requirement.

a) Dead Login
b) Live Login

The Working of each of the above login control is as follows

A. DEAD LOGIN:

Dead Login will be set as default login control for all the sites added in Sematral System's secure list. This login control will allow the user to login to the site via Face Recognition. As soon as user sets up a new account for sematral system he will be asked to allow his webcam to capture his face to store it as an password. After successfully completion of this step the password will be stored in the database. That's the one part of this login, as discussed above about inbuilt security mechanism Sematral system will also have some. It will allow the user to enable/Disable features of the site for Dead Login. After all this now, when a user logins using his/her face, he will be first logged in as per Dead Login Features i.e. the features he/she has

disabled will remain unavailable to him in this mode until he/she logs in via Live Login Mode.

Now the question arises is what if an user doesn't have an webcam? In this case he will be forced to use Matrix Login system (discussed later in this paper). The Same Matrix login will be used as Sematral System's Main Login Option.

WORKING-ILLUSTRATIONS

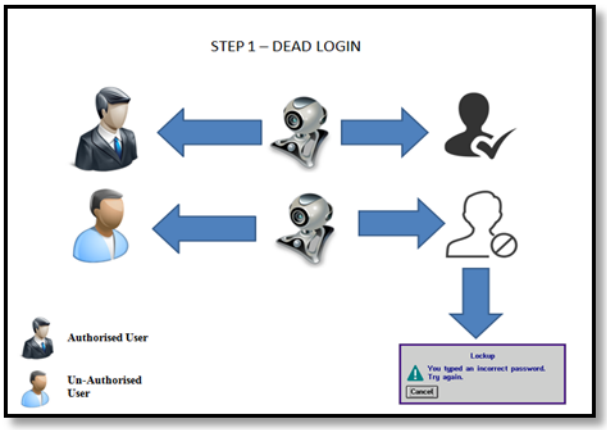

Figure 4.1.1 – Dead Login

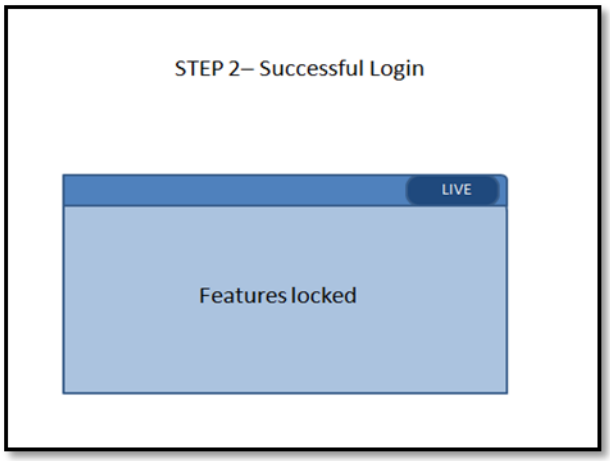

Figure 4.1.2 – Successful Dead Login

B. LIVE LOGIN:

The Dead login will allow the user to login but will have some restrictions on usage of some of the features set up by the user during the time of creation of account. To get the full functional site i.e. unlock the disabled features a user has to login via Live Login from with in the Dead Login mode This Live Login feature will consist of two modes.

i. Simple Live Login
ii. Secure Live Login

The dead login will consist of a small button on the top left side of the screen that will be labelled as Live Login. To enable all the features user have to click on this Live Login button. The function of this button will depend upon the type of security mode set up by the user i.e. Simple Live Login or Secure Live Login.

i. SIMPLE LIVE LOGIN:

If a user has set up simple live login, then when a user clicks on the top left button , it will turn into a simple input box. At the same time user's registered mobile number will receive unlock code. User now has to input this code in the input box to enable all the features of the site.

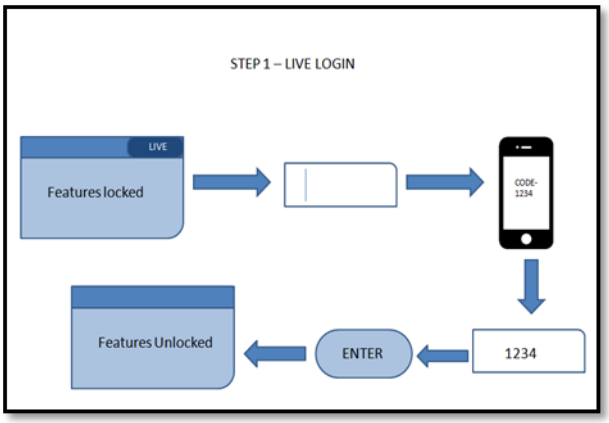

Figure 4.2.1 – Simple Live Login

ii. SECURE LIVE LOGIN:

This mode is almost similar to Simple Live Login mode, it just adds up a layer of security. When user will click on the Live Login Button on the top left corner it will ask for Accepting Clicks (Discussed Later in this paper). Once user enters the right sequence of Accepting Clicks , a code will be sent on the registered number i.e. unlock code to enable all the features. User will also have the option of setting up normal password rather than setting up accepting click.

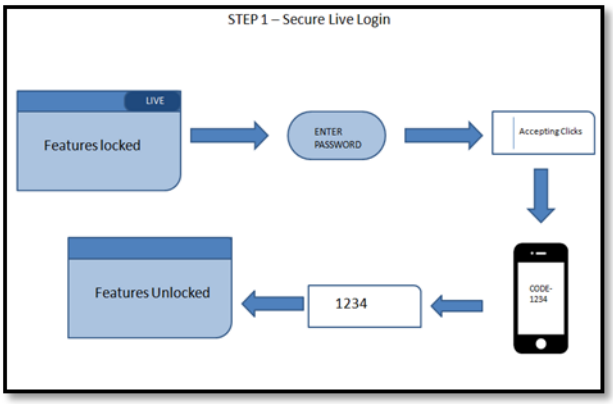

Figure 4.2.2 – Secure Live Login

V. MAIN LOGIN SYSTEM

As stated at the start of this paper most of the site makes use of normal login ie username and password and thats one of the major reason why such sites are easy target for attackers as these passwords can be captured by various key logger viruses and also by other tricks. Taking this into consideration we have made use of Matrix Based Login. In this mode a matrix of specified size will be used allowing the user to set up a password consisting of special characters, numbers or alphabets. During the time of login a matrix of specified size will be displayed to the user

having random letters, numbers or special characters, now user have to accept the matrix if it contains all the characters of user password or else he simply has to reject it. Out of all the matrix displayed by the system for login, only one will contain all the characters of the right password. Even the acceptance and rejection will not be keyboard based as it can be captured, instead mouse clicks will be used. The Acceptance and rejection of right or wrong matrix will be based on the Accepting clicks and Rejecting Clicks. The same Matrix Based Login mode will be used for the dead login in case of absence of a web-camera.

EXAMPLE:

Lets assume user password as "VISHAL" then for the login purpose a matrix will be displayed. In this example Matrix 1 (Case 1) is wrong i.e. it does not contain all the characters of the password defined by user and Matrix 2 (Case 2) is the correct one.

CASE 1:

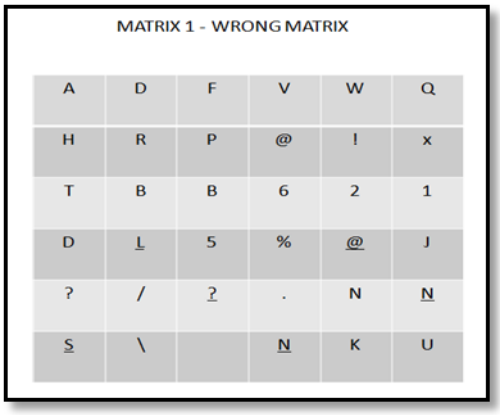

Figure 5.1 – Wrong Matrix

In this case the matrix of 6 X 6 does not contain all the characters of the user defined password, So the user has to reject this one in order to tell the system that this is not the correct one. This rejection will be performed by the user using Rejection Clicks.

CASE 2:

Figure 5.2 – Right Matrix

In this case the matrix displayed is the right one,it consists of all the characters of the user defined password along with some garbage values. The password characters are marked with RED for ease to understand the example. The user has to simply accept this matrix by mean of Accepting Clicks to log in to the system.

A. ACCEPTING CLICKS (AP'S):

This Click pattern will be used to accept the right matrix i.e Selecting the matrix that has all the characters of the user's defined password. Accepting clicks refer to the sequence of mouse clicks. For Instance- Assume user has defined the password for his/her main login as "PASSWORD" and has defined AP as "Left click , Left Click , Right Click". Then at the time of login a matrix will be displayed to the user, if the Matrix consist of all the characters of the password i.e "PASSWORD" the user simply has to click the right sequence of Accepting Click set by him. Wrong sequence will keep the user at the same screen, thus securing the profile.

B. REJECTING CLICKS (RC's):

Unlike Accepting Clicks this click sequence will be used for rejecting a matrix. There's a strong possibility that the matrix shown might not be right i.e. it might not have all characters of the user's defined password in such case user has to reject it, this will be done by Reject Clicks. Rejecting a matrix will display another Matrix that might contain the right set of characters.

The use of Accepting and Rejecting clicks will ensure that any guess attempts to login to the system will not be as easy as compared to a single click for accepting and rejecting a matrix. It will create a large of probabilities for the right sequence along with the right matrix.

VI. HOW IS IT SECURED?

This entire system is very secure as it makes use of all these various security features. It increases the level of security when compared with the existing implemented security steps.The use

of Matrix for entering the right password along with the use of Accepting Clicks and Rejecting Clicks makes it very difficult to guess the password of the user even if the person is looking at the screen while user enters the password. Even if by any mean the password is revealed, the large number of possibility of click sequence will make it difficult for the attacker to get in to the main system easily. The use of Dead And Login mode after successful matrix login also levels up the security.

Not only this Sematral System also provides Track Log feature which will keep a log of all the user activities on the accounts in the secure list. It will capture the screens without user's awareness for the purpose of record keeping. Both of this – Screenshots as well Logs of user activities will be mailed to the user's registered mail id. Thus even in the case of security breach all the activities of the user will be captured.

VII. CONCLUSION

The entire system enables a strict security. Threats from Key-Logger Virues, Rats , Dictionary Attack and many others will not be possible. This System thus accomplishes its moto of providing security to the Security.

ACKNOWLEDGMENT

The contents of the paper fall under the domain of cyber security. The idea put up here are fresh and do not bear any resemblance in term of working and names with any other security concepts.

REFERENCES

[1] Jon Erickson , "The Art of exploitation" ,2nd Edition , No Starch Press , 2008.

[2] Engin Kirda and Christopher Kruegel , "Protecting Users Against Phishing Attacks with AntiPhish"

[3] Sagiroglu, S. ; Dept. of Comput. Eng., Gazi Univ., Ankara, Turkey ; Canbek, G. , "Keyloggers" Published in Technology and Society Magazine, IEEE (Volume:28 , Issue: 3), 2009.

AUTHORS

First Author – Vishal T. Mishra, Currently pursuing Diploma in Computer engineering , K.J. Somaiya Polytechnic, Mumbai , vishal.tm@somaiya.edu