Securing Social Media using Pair based Authentication

Shaikh Huzaif[1], Yadav Swapnali[2], Kale Vaishnavi[3], Hirave Kanifnath[4]

Department of Computer Engineering, H.S.B.P.V.T College of Engineering, Kashti

***Abstract*— Early we use Textual passwords as a security but these passwords are vulnerable to the various attacks like Dictionary attack, Shoulder surfing, eves dropping, etc. Further graphical passwords are coming to the existence but the graphical passwords have their own disadvantages like they require more time to Authenticate and the usability issues. Thus we proposed a session password scheme in which the passwords are used only once for each and when session is terminated the password is no longer in use. The proposed of session password scheme uses Text and colors for generating session password. Two session password schemes are used Hybrid Textual Authentication Scheme and Pair-based Authentication scheme.

Index Terms— Authentication, Password, Pair-based Authentication scheme

I. INTRODUCTION

The most popular user authentication approach is the text-based password scheme in which a user enters a login name and password. Despite of its wide usage, the Textual passwords have a number of short comes. The Simple and straightforward textual passwords are easy to Remember, but they are more vulnerable for attackers to break. Whereas the complex and arbitrary passwords makes the system more secure, resisting the brute force search and dictionary attacks, but the difficulty lies in retaining them. Besides this, textual passwords are liable to the shoulder-surfing, hidden cameras, and spyware attacks.

Consequently, graphical password strategies have been introduced as a substitute for textual passwords schemes, as pictures can be easily remembered when compared with words. Furthermore, it is difficult to formulate automated attacks for graphical passwords. Moreover the password space of the graphical password scheme may extend that of the textual based password schemes and hence probably providing a higher level of security means. On the account of these reasons, there is an intensifying interest in the graphical password methods. However, most of the existing graphical password authentication methods suffer from shoulder surfing, a known hazard where an intruder can scrutinize the password by recording the authentication session or through direct surveillance. In addition, setting up a system that offers the graphical authentication schemes is substantially costlier than the text based password methods. Even though some of the graphical password procedures resistant to the shoulder surfing are proposed, yet they have their own downside like usability issues or consuming additional time for user to login or having tolerance levels. Based on these various reasons pointed out, session passwords are instigated. Session passwords are those that can be used only at that particular instant. As soon as the session expires, the password is no longer valid. As such the user, keys in distinct passwords each time he logs into the session.

In this paper, we have designed a project whose objective is to provide security to the confidential files residing in system. Here, any user who needs to the access those files has to first get registered by the administrator (admin) of that particular organization. The registered user is then allowed to login using session passwords through either of the two authentication techniques that have been proposed in the forthcoming sections. Subsequently, the user is allow for graphical authentication scheme. If the user is ascertained as the genuine person then he is given the rights to access the confidential files or else he is regarded as malefactor.

The rest of the paper is organized as follows.

Section II describes about various existing graphical authentication schemes. Proposed project work is depicted in Section III. Section IV gives conclusion to the paper. Future Scope is pointed out in Section V.

II. RELATED WORK

Graphical password is a type of knowledge based authentication. Thus, graphical passwords consist of images and visual representation which are used in replacement to text or alphanumeric characters. The graphical passwords consist of four sections namely: A) Recognition based technique B) Pure Recall based technique C)Cued-recall based technique D)Hybrid based technique a) Recognition Based Technique: In this technique, users have to choose the image or symbols from a set of images. At the time of registration, the users select images which is set as user's password. Thus, during authentication users have to remember this password from a collection of different images [8].90% of users were able to identify their password images. Also, users were able to remember their passwords after a time span of 45 days[9]. b) Pure recall based technique: In this technique users set as image as a password during registration. Users need to reproduce or remember their own passwords and thus no clues are given to remind the passwords. This scheme is simple, easy but the difficulty in this technique is that passwords are hard to remember. It is more secure compared to recognition based scheme. It is quite similar to DAS (1999) and Qualitative DAS (2007). c) Cued recall based technique: In this technique users generate a password during authentication with the help of a hints or reminders. It is quite similar to recall based scheme but it is recall with cueing. d) Hybrid based technique: In this technique authentication happens through the combination of two or more schemes. Thus, it overcomes the drawback of a single scheme. For e.g.: spyware, shoulder surfing etc...

A. Recognition based Technique

In this technique users set as image as a password during registration. Users need to reproduce or remember their own passwords and thus no clues are given to remind the passwords. This scheme is simple, easy but the difficulty in this technique is that passwords are hard to remember. It is more secure compared to recognition based scheme. It is quite similar to DAS (1999) and Qualitative DAS (2007) recognition based scheme is also known as cognometric scheme or search scheme.

a)Dhamija and Perrig:

Proposed a scheme in the year 2000. In this scheme, users have to choose a random image from a set of images. The set of images are generated by the program executed in a system. During the authentication phase, the system provides the user with a set of images which consist of both decoy as well as password images. The user has to select the right set of images from a set of password and decoy images. The initial seeds are used to generate these images thus it becomes to store up but it is difficult to share or record these images. Deja vu scheme has its shortcomings such as ambiguous images are difficult to remember and the password space is less as compared to the textual password.

b) Passface scheme:

This was proposed by Brostoff. In this scheme, users have to choose four faces as a password. So, during the authentication phase, user is provided with a grid of size 3x3 shown in Fig 1, the user has to recognize one face from a set of nine face and click on it. This process continues until four faces have been selected by the user as a valid password. There are limitations such that it can be easily guessed and processing time is quiet longer than that of textual passwords.

c) Jensen: proposed a scheme in the year 2003.This scheme was mainly focused on PDAs. It is also known as picture password scheme. The user has to select image of size 40x40 from a 5x5 matrix. Thus, order of selection of image is also verified during the authentication phase i.e. It should be the same sequence of order as in registration phase. The disadvantage of this method is the memorability is more complex and difficult.

d) Story: is quite similar passfaces scheme was proposed by Davis. In this scheme, users have to select a sequence of images to form a portfolio. During login, users have to choose the images and their portfolio images. It is also required for the user to choose the image in the correct order to remember their passwords, user mentally construct a story by connecting the set of images.

e) Sobardo and Birget: proposed a scheme which focuses mainly on the shoulder surfing problem. In first method, the system displays a number of objects. During the authentication user chooses these pass-objects and click inside of a convex hull formed by the pass-objects. In order to show the password is difficult to guess. Sobardo and Birget formed a scheme, in which 1000 objects are used to make the display crowded and making it indistinguishable.

f) Man et al: proposed a method which is resistant to shoulder surfing attack. In Fig 2,The users have to select a number of images as a password object or pass-objects. Each pass-object has variants and each variant is assigned a unique code. Thus, during authentication user has to choose the pass-object from several scenes. Thus, user has to type a unique code along with a string along with a code indicating the relative location of the pass-objects.

Graphical Password with Icons[GPI]: was designed to solve the problem of hotspot. In GPI users have to select 6 icons from 150 icons to set as a password. In this scheme, the GPIs system generate a password which is authenticated by the user and if the user is not satisfied with the password, the user can request to generate a new password. The drawback of this scheme is the icon size is very small and unacceptable login time.

B. Pure Recall Based Technique:

Pure recall based scheme is also known as drawmetric scheme, where the users have to recall drawing on grid, that they selected registration phase. In this scheme, users have to draw password either onto a grid or a blank canvas.

a) Jermyn: proposed a method called "Draw-A - Secret"(DAS). Users have to draw a password on a 2D grid using stylus or mouse. The drawing may consist of a single stroke or multiple strokes. Thus, for the user to successfully login, users redraw the same path, passing through the grid cells as shown in Fig 3. The system database stores the password in the same sequence of coordinate of the grid encoded during the DAS password. The length of the password depends on the number of coordinate pairs. There is no need for user to remember any alphanumeric characters. The difficulty with this technique the user has to redraw at the exact position of the grid line.

b) Thorpe and Van Oorschot: proposed a graphical password scheme based on Jermyn. They introduced graphical dictionaries and using these dictionaries, they studied the brute force attack. They set a length parameter for DAS password and proved that DAS password of length 8 is less susceptible to dictionary attack. They also proved that space of mirror symmetric graphical password is smaller than DAS password space. People tend to recall symmetric images better than asymmetric images. Therefore, users tend to choose mirror symmetric passwords.

c) Varenhorst: proposed a graphical password scheme called passdoodle which allows user to create a free hand drawing as a password as shown in Fig 4. There is no visible grid. It consists of two pen strokes which drawn on the screen using a number of colors. Matching of passdoodle is more complex. In this system, doodle is stretched and scaled and then compared with stored user password.

d) Weiss: proposed the graphical password scheme passhapes. In the system, geometric shapes are generated on basis of the combination of eight strokes. During login, there is no grid and password can be drawn on any position. Thus, passshapes offer memorability.

e) Syukri algorithm: is based on pure recall based system, thus user is authenticated by drawing their signature with the help of a mouse or stylus. This method has two stages registration & verification. During registration, the user draws the signature with a mouse and system extracts area under signature and saves the information to the database. The verification stage involves the user to place signature and then extracts the parameter of the signature. Thus, verification involves using a geometric average and thus update a database. The biggest advantage there is no need to memorize one's signature and also signature are hard to fake.

There are two commercial products based on pure recall based graphical password scheme. First, there is an unlock scheme which is similar to a mini pass-go that unlocks screen of an android smart phones. In this user chooses his unlocking pattern by dragging with finger over points in 3x3 grid. Second, in Windows 8 system, Microsoft has introduced a new graphical password. Users are provided with an image and have to draw gestures on the image provided. Gestures could include: top, circle and straight line or combination of these gestures. Thus, these two products show that simple to operate easy to remember and can be applied to a system where there is no need for a high security level

III. SECURITY ATTACKS ON GRAPHICAL PASSWORD SYSTEMS

a) Dictionary Attack:

In this type of attack, an attacker tries to guess the password from a dictionary which is a collection of list of words. Dictionary consists of all passwords based on the previous selections and all the **passwords** have high probability. Thus, if a user chooses a password, which is present in the dictionary, then the attack is successful. This attack is based password brute forcing.

b) Guessing Attack:

Many a times, user prefer to **choose** their passwords based on their personal information such as house name, phone number, etc... In most of these cases, the attacker tries to guess the password by accessing the user's personal information. Guessing attacks can be categorized into two: online password guessing and offline password guessing attacks. In online password guessing, the attack guesses a password by manipulating inputs of one or more than one oracles. In offline, password guessing attacker searches for the password through manipulation of inputs of one or more than one oracles.

c)Shoulder Surfing Attack: In shoulder surfing attack, the attacker watches over the behaviour of the user based on the direct observation technique.one of the direct observation technique, is looking over the persons shoulder to trace the password. It usually occurs in public places.

d)Spyware Attack: Spyware is kind of a malicious software installed onto user's computers with aim to steal information of users. The method to execute a spyware attack is either through key logger or key listener. This malware collects the information about the user without his/her knowledge and thus leak this information to an outsider.

e) Social Engineering Attack: Social engineering attack takes place through human interaction which causes users to give out sensitive information. In this type of attack, the attacker fakes himself to be an employee of an organisation and tries to interact with user to collect information related to the organisation. The attacker does not use any kind of electronic gadget but with his/her own intelligence and tricky conversation to get information he/she want.

IV. Proposed System

Authentication technique consists of four phases:

1. Registration phase
2. Login phase
3. Verification phase
4. Recovery phase

During registration, user rates the colors in the first method or enters his password in the second method. During login phase, the user has to put the password based on the interface displayed on the screen. The entered password verifies by the system by comparing with content of the password generated during registration. During recovery phase, if user forgets his password, he may recover the password by answering security questions which user had selected during registration phase

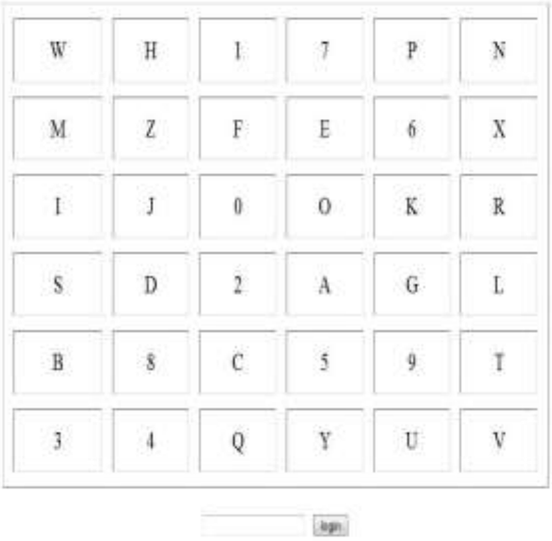
1. Admin Phase In admin phase administrator can see the on line users and can see the user's information. Only has authority to see the information. He enter the user name and password to see the user information

2. Registration Phase In this phase if the user is not registered then first he can register his information as shown in fig. 8 As shown in fig.8 user can enter user name, mobile number, first name, last name, email-id and choose the color code as secret password used for Hybrid based technique and submit the information.

3. Login Phase After registration user can login; user got his password on his email-id and his mobile number. In login user enter his user name and user id After login two technologies displayed on the screen for user. User can select any technique for login. There are two techniques, one Pair based technique and another Hybrid based technique

4. Pair-Based authentication scheme

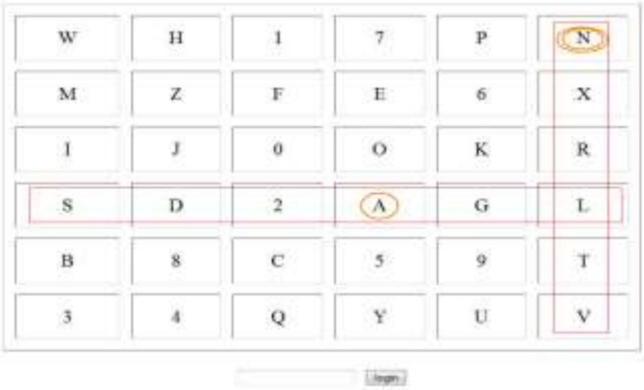
During registration user submits his password. Minimum length of the password is 8 and it can be called as secret pass. The secret pass should contain even number of characters. Session passwords are generated based on this secret pass. During the login phase, when the user enters his username an interface consisting of a grid is displayed. The grid is of size 6 x 6 and it consists of alphabets and numbers. These are randomly placed on the grid and the interface changeseverytime



W	H	1	7	P	N
M	Z	F	E	6	X
I	J	0	O	K	R
S	D	2	A	G	L
B	8	C	5	9	T
3	4	Q	Y	U	V

Fig 1. Pair-Based authentication scheme

User has to enter the password depending upon the secret pass. User has to consider his secret pass in terms of pairs. The session password consists of alphabets and digits



W	H	1	7	P	N
M	Z	F	E	6	X
I	J	0	O	K	R
S	D	2	A	G	L
B	8	C	5	9	T
3	4	Q	Y	U	V

The first letter in the pair is used to select the row and the second letter is used to select the column. The intersection letter is part of the session password. This is repeated for all pairs of secret pass. Fig 8 shows that L is the intersection symbol for the pair “AN”. The password entered by the user is verified by the server to authenticate the user. If the password is correct, the user is allowed to enter in to the system. The grid size can be increased to include special characters in the password.

V. IMPLEMENTATION DETAILS

1. Module Descriptions

A module description provides detailed information about the module and its supported components, which is accessible in different manners. The included description is available by reading directly, by generating a short html-description, or by making an environment check for supported components to check if all needed types and services are available in the environment where they will be used. This environment check could take place during registration/installation or during a separate consistency check for a component.

1.1 Overall System Overview

The proposed system using new Authentication technique consists of 3 phases: registration phase, login phase and verification phase. During registration, user enters his password in first method or rates the colors in the second method. During login phase, the user has to enter the password based on the interface displayed on the screen. The system verifies the password entered by comparing with content of the password generated during registration.

1.1.1 Registration Phase:

In this phase if the user is not registered then first he can register his information. User can enter name, user name, mobile number, and email-id and choose the secret password used for Pair based technique and submit the information.

1.1.2 Login Phase

After registration user can login, using his username. It will check entered username is an existing or not if username is valid, it will process, else it gives error message.

1.1.3 Pair Based Authentication scheme

During registration user submits his password. Minimum length of the password is 8 and it can be called as secret pass. The secret pass should contain even number of characters. Session passwords are generated based on this secret pass. During the login phase, when the user enters his username an interface consisting of a grid is displayed. The grid is of size

6 x 6 and it consists of alphabets and numbers. These are randomly placed on the grid and the interface changes every time User has to enter the password depending upon the secret pass. User has to consider his secret pass in terms of pairs. The session password consists of alphabets and digits.

1.1.4 Profile Phase

Once successfully Logged in the user will enter to his profile where he/she can perform following things:

Send friend request.
Rate friends which is depending on how much he/she is active on the site.
Can update his/her status.

1.1.5 OTP Phase
For rating friend the user should be the friend of the rater. The user will receive an OTP on the mobile number register during the registration process. This OTP is supposed to enter for verification of the user and to enter the rate friend.

1.1.6 Rating Friend
Rating friend is a person who can rate his/her friends. He/she can rate according to some criteria on which the friend can know about his friend being active or not i.e. the no. of status been uploaded by the friend, no. of photos been uploaded by the friend.

1.2 Algorithms:
Algorithm:
Algorithm means set of rules to be followed and the steps are as follows:
1 The new user will register on the site which will include important details as :
- Name
- Username
- Password

The password to be used in pair based authentication will be even length.
- E-mail ID of the user
- Phone number of user

2 After the user has registered successfully then he can proceed to Login.
- Enter username.
- Enter the Password (Even alphabets only).

3 When successfully Logged in the user will enter to his profile. where he/she can perform following things:
- Send friend request.
- Rate friends which is depending on how much he/she is active on the site.

Can update his/her status.
For rating his/her friend the user should be the friend of the rater. The user will receive an OTP on the mobile number register during the registration process. This OTP is supposed to enter for verification of the user and to enter the rate friend.

VI. CONCLUSION

In this paper, two authentication techniques based on text and colors are proposed for PDAs. These techniques session passwords and are resistant to dictionary attack, brute force attack and shoulder-surfing. Both the techniques use grid for session passwords generation. Pair based technique requires no special type of registration; during login time based on the grid displayed a session password is generated. For hybrid textual scheme, ratings should be given to colors, based on these ratings and the grid displayed during login, session passwords are generated. However these schemes are completely new to the users and the proposed authentication techniques should be verified extensively for usability and effectiveness.

VII. FUTURE SCOPE

Future scope of this technique is that , as it provides more security than the others existed systems more secure login of users is possible .so this technique is not just limited for PDA

i.e. personal digital Assistant but also it is very useful for providing protection against Hacking, Dictionary attacks, etc.

In future it will be used for Banking Applications, Mobile phones applications where the security is more important. It also use with the 3D password technique for providing more and more security.

VII. REFERENCES

[1] R. Dhamija, and A. Perrig. “Déjà Vu: A User Study Using Images for Authentication”. In 9th USENIX Security Symposium, 2000.

[2] Jermyn, I., Mayer A., Monrose, F., Reiter, M., and Rubin., “The design and analysis of graphical passwords” in Proceedings of USENIX Security Symposium, August 1999.

[3] A. F. Syukri, E. Okamoto, and M. Mambo, "A User Identification System Using Signature Written with Mouse," in Third Australasian Conference on Information

Security and Privacy (ACISP): Springer-Verlag Lecture Notes in Computer Science (1438), 1998, pp. 403-441.

[5] G. E. Blonder, "Graphical passwords," in Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent,Ed. United States, 1996.

[6] Passlogix, site http://www.passlogix.com.

[7] Haichang Gao, Zhongjie Ren, Xiuling Chang, Xiyang Liu Uwe Aickelin, "A New Graphical Password Scheme Resistant to Shoulder-Surfing [8] S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, N. Memon, "Design and longitudinal evaluation of a graphical password system". International J. of Human-Computer Studies 63 (2005) 102-127.