Session Password Authentication Schemes-A Review

Aashutosh Gawali
maxaashu@gmail.com

Deepika Bhatia
deepika.18850@gmail.com

ABSTRACT

Textual passwords are the most common method used for authentication. But textual passwords are vulnerable to eves dropping, dictionary attacks, social engineering and shoulder surfing. Graphical passwords are introduced as alternative techniques to textual passwords. Most of the graphical schemes are vulnerable to shoulder surfing. To address this problem, text can be combined with images or colors to generate session passwords for authentication. Session passwords can be used only once and every time a new password is generated. In this paper, two techniques are proposed to generate session passwords using text and colors which are resistant to shoulder surfing. These methods are suitable for Personal Digital Assistants.A new technique called session password is introduced on the combination of text and images to solve the problem of security. Session password can be used every time the password is created for authentication. Two techniques are used to generate session password which overcomes the attacks like shoulder surfing, Dictionary attacks.

Keywords:-Security, Shoulder Surfing, Dictionary attacks, Authentication,

I. INTRODUCTION

Recently there has been a great emphasis to provide more security for passwords. The 21st century is the more advancing age of internet and related contents, highly exposing data which innovated before a minute or say as to some seconds. The most traditional method for authentication is textual Password. Users first choice for authentication is textual passwords. Mostly users choose short and simple password so that they can be easily memorised and can be recalled at the login-time. In common it has been surveyed that an average users has to memoriseatleast 3 passwords. Again in addition to this the user has to remember password for banking, e-commerce, social networking sites and also email accounts. Short and simple textual passwords are easy to remember, but can be easily hacked while random and lengthy passwords are secured but hard to remember. To overcome this problem graphical authentication schemes were proposed. Authentication is the first step in information security. It requires the user to memorize their password and remember at login time. Textual passwords are the most traditional schemes that are used for providing security.

The most traditional method for authentication is textual Password. Mostly users choose short and simple password so that they can be easily memorised and can be recalled at the login-time. The user is authenticated using session password. Session passwords are the password that is provided to authenticate the user for a session. Session passwords are used only once. Every time the users enters a session he has to input different password. Once the session is over that password becomes is of no use for next session and the current session gets terminated. Session password provide more security as every time the session start a new password is created and they are not prone to dictionary attacks ,brute force attacks and shoulder surfing attacks. This paper is organized into four sections. & findings to dictionary attacks , brute force attacks and shoulder surfing attacks.

II. RELATED WORK

Recently there has been a great emphasis to provide more security for passwords. The 21st century is the more advancing age of internet and related contents, highly exposing data which innovated before a minute or say as to some seconds.

Various comprehensive investigations on the existing authentication schemes have been accomplished. And it has been discerned that none of the recent authentication schemes can resist all sorts of attacks. With this outcome, this paper proposes an authentication schemes which overcomes all the existing authentication schemes. Related work reveals all the studies that are done in past. Some of the authentication schemes are discussed as follows:

COMPARISON OF VARIOUS AUTHENTICATION METHODS:-

Authentication schemes	**Textual password**	**Graphical password**	**Token password**	**Biometric password**
Usability	very high	High	Less	very less
Implementation	Easy	difficult	more difficult	highly difficult
Attacks	Bruteforce dictionary guessing	shoulder surfing, guessing	Forgery	Forgery
Password space	quite less	Less	no matter	no matter
Cost of attacks	Low	Moderate	High	Very High
Time to login	Low	Moderate	Moderate	High
Flexibility	Moderate	High	Low	very low
Recovery	Easy	Easy	Hard	Difficult

A. AUTHENTICATION SCHEME RESISTANT TO SHOULDER SURFING ATTACK USING IMAGE RETRIEVAL[1]:

Thorawade M.B. and Patil S.M. (2012) described a secured authentication system should be incorporated in order to protect secret information from sensitive and various applications. The vulnerabilities of textual passwords are well known, such as short passwords are easy to remember, which makes the pass-words vulnerable for attackers to break and some passwords which cannot be easily guessed are often difficult to remember. Shoulder surfing attack refers to using direct observation techniques, such as looking over someone’s shoulder to get some information such as password, etc. Hence an alternative solution to text based authentication is image based authentication. However image based authentication is more vulnerable to shoulder surfing attack.

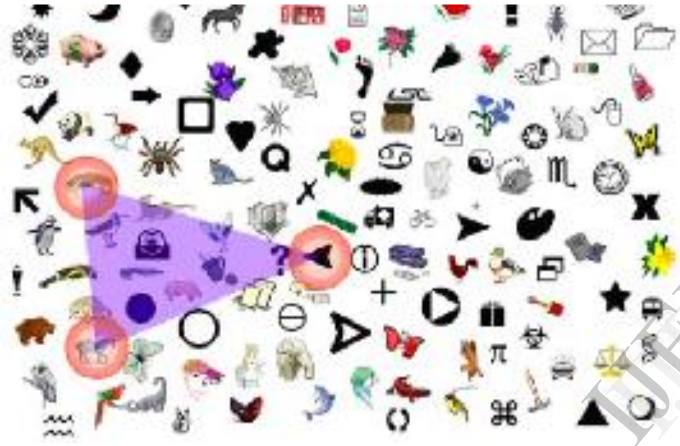


Fig. 1 A shoulder surfing resistant graphical password scheme

The system comprises of 9 steps out of which steps 1-3 are registration steps and steps 4-9 are the authentication steps.

Step 1

The first step is to type the user name and a textual password which is stored in the database. During authentication the user has to give that specific user name and textual password in order to log in.

Step 2

In this second step objects are displayed to the user and he/she selects minimum of three objects from the set and there is no limit for maximum number of objects. This is done by using one of the recognition based schemes. The selected objects are then drawn by the user, which are stored in the database with the specific username. Objects may be symbols, characters, auto shapes, simple daily seen objects etc. Examples are shown in Figure 4.

Step 3

During authentication, the user draws pre-selected objects as his password on a touch sensitive screen (or according to the environment) with a mouse or a stylus. This will be done using the pure recall based methods.

Step 4

In this step, the system performs pre-processing

Step 5

In the fifth step, the system gets the input from the user and merges the strokes in the user drawn sketch.

Step 6

After stroke merging, the system constructs the hierarchy.

Step 7

Seventh step is the sketch simplification.

Step 8

In the eighth step three types of features are extracted from the sketch drawn by the user.

Step 9

The last step is called hierarchical matching.

B. A GRAPHICAL PASSWORD BASED SYSTEM FOR SMALL MOBILE DEVICES [2]:

Greg Blonder in 1996 discribed A graphical based password is one promising alternative of textual passwords. According to human psychology, humans are able to remember pictures easily. In this paper, we have proposed a new hybrid graphical password based system, which is a combination of recognition and recall based techniques that offers many advantages over the existing systems and may be more convenient for the user. Our scheme is resistant to shoulder surfing attack and many other attacks on graphical passwords. This scheme is proposed for smart mobile devices (like smart phones i.e. ipod, iphone, PDAs etc) which are more handy and convenient to use than traditional desktop computer systems.

C. Graphical Password Authentication Using Cued Click Points ⋆:

Users click on one point per image for a sequence of images. The next image is based on the previous click-point. present the results of an initial user study which revealed positive results. Performance was very good in terms of speed, accuracy, and number of errors. Users preferred CCP to Pass Points (Wiedenbeck et al., 2005), saying that selecting and remembering only one point per image was easier, and that seeing each image triggered their memory of where the corresponding point was located. We also suggest that CCP provides greater security than Pass Points because the number of images increases the workload for attackers.

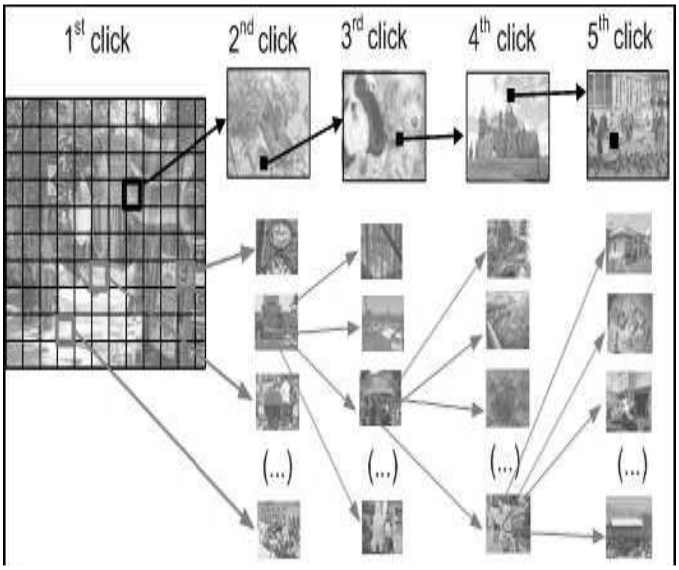


Fig. 2. CCP passwords can be regarded as a choice-dependent path of images

III.PROPOSED SYSTEM

Authentication technique consists of 3 phases

1) Registration phase
2) Login phase and
3) 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.

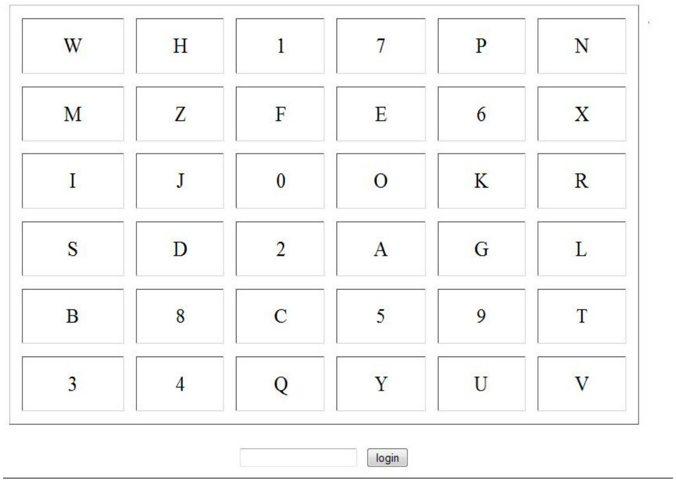
3.1 Registration Phase:

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.

3.2 Login Phase:

Pair-based Authentication scheme:

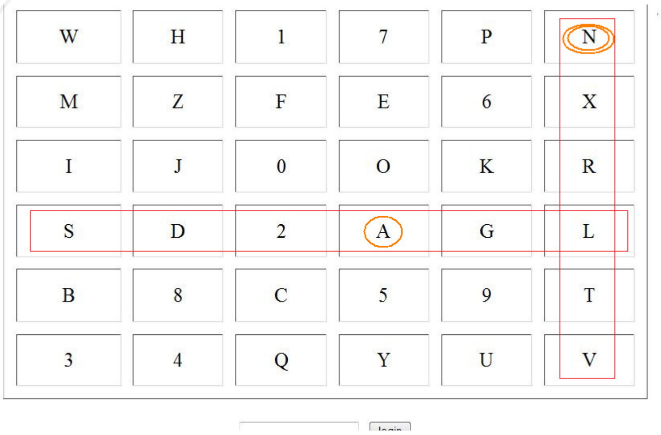
During registration user submits his password. Minimum length of the password is 8 and it can be called as secret pass. The secret pass should contain even number of characters. Session passwords are generated based on this secret pass. During the login phase, when the user enters his username an interface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



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

Figure 3: Login interface

Figure 3shows the login interface. 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. 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.



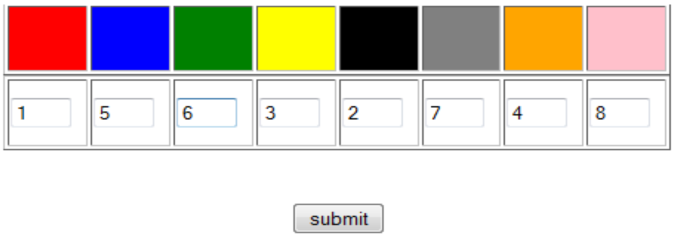
W	H	1	7	P	N
M	Z	F	E	6	X
I	J	0	O	K	R
S	D	2	A	G	L
B	8	C	5	9	T
3	4	Q	Y	U	V

Figure 4: Intersection letter for the pair AN

3.3 Verification Phase:

Hybrid Textual Authentication Scheme

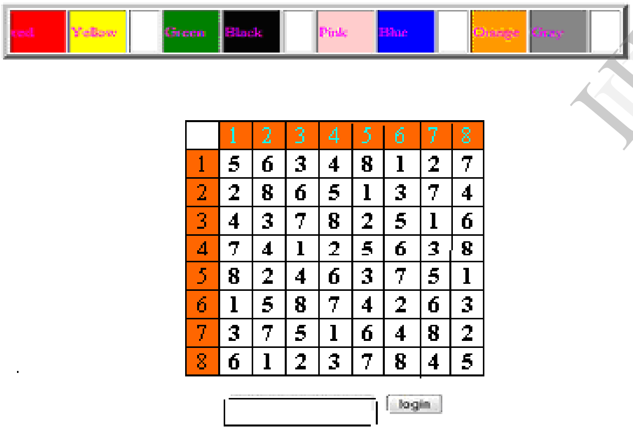
During registration, user should rate colors as shown in figure 5. The User should rate colors from 1 to 8 and he can remember it as "RLYOBGIP". Same rating can be given to different colors. During the login phase, when the user enters his username an interface is displayed based on the colors selected by the user. The login interface consists of grid of size 8×8. This grid contains digits 1-8 placed randomly in grid cells. The interface also contains strips of colors as shown in figure 10. The color grid consists of 4 pairs of colors. Each pair of color represents the row and the column of the grid.



1	5	6	3	2	7	4	8

Figure 5: Rating of colors by the user

Figure 6 shows the login interface having the color grid and number grid of 8 x 8 having numbers 1 to 8 randomly placed in the grid. Depending on the ratings given to colors, we get the session password. As discussed above, the first color of every pair in color grid represents row and second represents column of the number grid. The number in the intersection of the row and column of the grid is part of the session password. Consider the figure 5 ratings and figure 6 login interface for demonstration. The first pair has red and yellow colors. The red color rating is 1 and yellow color rating is 3. So the first letter of session password is 1st row and 3rd column intersecting element i.e **3**. The same method is followed for other pairs of colors. For figure 10 the password is " **3573** ". Instead of digits, alphabets can be used. For every login, both the number grid and the color grid get randomizes so the session password changes for every session.



	1	2	3	4	5	6	7	8
1	5	6	3	4	8	1	2	7
2	2	8	6	5	1	3	7	4
3	4	3	7	8	2	5	1	6
4	7	4	1	2	5	6	3	8
5	8	2	4	6	3	7	5	1
6	1	5	8	7	4	2	6	3
7	3	7	5	1	6	4	8	2
8	6	1	2	3	7	8	4	5

Figure 6: Login interface

IV. ADVANTAGES

- As the interface changes every time, the session password changes. This technique is resistant to shoulder surfing.
- Due to dynamic passwords, dictionary attack is not applicable.
- Hidden camera attacks are not applicable to PDAs because it is difficult to capture the interface in the PDAs.

V. FUTURE SCOPE

- In this paper, Two authentication techniques based on text and colours are proposed for PDAs. These techniques generate session passwords and are resistant to dictionary attack, brute force attack and shoulder-surfing.
- Both the techniques use grid for session passwords generation. However these schemes are completely new to the users and the proposed authentication techniques should be verified extensively for usability and effectiveness.
- These techniques can also be developed a windows application such as a folder locker or an external gateway authentication to connect the application to a database or an external embedded device.

VI. SUMMARY

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.
As the interface changes every time, the session password changes. This technique is resistant to shoulder surfing. Due to dynamic passwords, dictionary attack is not applicable. Hidden camera attacks are not applicable to PDAs because it is difficult to capture the interface in the PDAs.

REFERENCES

[1] Thorawade M.B. and Patil S.M. (2012) Authentication Scheme Resistant to Shoulder Surfing Attack using Image Retrieval. International Journal of Knowledge Engineering, ISSN: 0976-5816 & E-ISSN: 0976-5824, Volume 3, Issue 2, pp.-197-201.

[2] chnologies, Inc. (Murray Hill, NJ), August 1996.

[3] Y. Zhang, L. Wu, Rigid Image Registration by PSOSQP Algorithm, Advances in Digital Multimedia, vol.1, no.1, pp.4-8, 2012

[4] Tejaswi Lalitha Surepeddi, K. Gowtham, A. Ramakrishna, D. Aruna Kumari, Design, Implementation of Network Based Authentication Mechanisms, Advances in Information Technology and Management, vol.1, no.2, pp.44-48, 2012

[5] P. Vikram Varma, Siva Pillalamarri Prasad, R. Leela Kumari, Virtual laboratory through internet, Advances in Information Technology and Management, vol.1, no.2, pp.60-65, 2012

[6] W. Jansen, "Authenticating Mobile Device User through Image Selection," in Data Security, 2004.

[7] W. Jansen, "Authenticating Users on Handheld Devices "in Proceedings of Canadian Information Technology Security Symposium,2003.