THE INTERNATIONAL JOURNAL OF SCIENCE & TECHNOLEDGE

Color Scheme Authentication for Session Passwords with OTP Protection

Avinash Pandey
Student, Vartak College Engineering, Maharashtra, India
Vishal Bedi
Student, L. R. Tiwari College of Engineering, Maharashtra, India
Sumesh Valanju
Student, Vartak College of Engineering, Maharashtra, India

Abstract:
All companies that use commercial applications on the internet are vulnerable to security threats. Numerous applications have been designed to secure these systems with only a handful of them, unfortunately succeeding in being able to provide good security to these applications and insulate them against threats. Internet Banking is under more threat than any other application and if one has to counter the threats, then some of the aspects like application, networks access control, etc. have to be worked on together and simultaneously to secure the systems, rather than focusing on securing them individually. Even in today's security-conscious world, most of the applications use traditional textual passwords which are vulnerable to shoulder-surfing, dictionary attacks etc. Therefore, new ways to secure various systems have been designed: graphical password scheme is one such instance. Unfortunately, this scheme also has a drawback as it is susceptible to shoulder-surfing attacks. To overcome this problem, a new age security system has evolved which uses a combination of text and graphics to generate passwords thus providing higher security. To strengthen this password scheme, a new technique called session password is introduced in combination with text and images. Session password can be used every time the password is created for authentication. A strong password is a good first step, but our proposed system suggests setting up two-factor authentication, which adds another layer between other people and your data. This restricts access to your account to people who have your password; also access to the secured level of authentication uses OTP method which not only secures authentication process but also provides a holistic and comprehensive security approach.

Keywords: *Graphical Passwords, OTP, Security, Session Password, Two-Factor Authentication*

1. Introduction

1.1. Problem Definition

Textual passwords have proven to be of effective means for securing applications until they were exposed to vulnerabilities. In context to the known range of vulnerabilities shoulder surfing has proven to be inevitable. To enhance the security and avoid shoulder surfing the prerequisites are long and random passwords, but with a proven disadvantage of being hard to remember. According to researchers, users tend to create passwords that are short and easy to recollect and for this very reason they are prone to brute force attacks and dictionary attacks. Apart from these issues there is no denying of the fact that textual passwords can fall prey to eavesdrop and social engineering attacks. On account of making the security concrete, alternate techniques exist, such as biometrics and graphical passwords. A known vulnerability of shoulder surfing is redundant in graphical password schemes. Biometrics also come with their own set of drawbacks in terms of infrastructure and usability issues.

1.2. Related Work

As we know graphical images are more easily recalled then text. In this selection so graphical password system based on recognition and recall based are discussed.

1) Recognition-Based Technique: In this type of technique, users will select pictures, logos or any symbols from pre-stored image. For authentication process user needs to recognize the image, which he choose as a password.

2) Recall-Based Technique: Again, recall-based, password authentication are categorize in two parts:

i) Pure Recall Based Technique, ii) Cued Recall Based Technique.

1.2.1. Dhamija and Perrig [1]

Dhamija and Perrig proposed a scheme called "Déjà vu" based on human ability to remember previously seen images. User has to select few images from a set of images. User has to perform same at login time. All abstract Images were generated using Andrej Bauer's Random Art. They showed 90 % success rate using "Déjà vu" while only 70% using text-based password and pins.

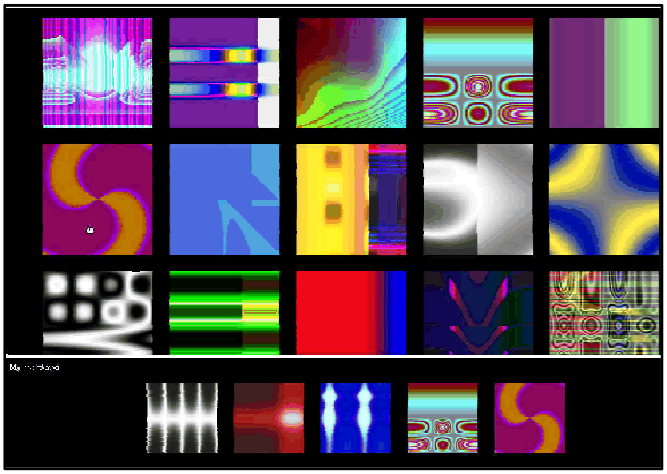

Figure 1: Random images used by Dhamija and Perrig

1.2.2. Passfaces [2]

Graphical password technique has been proposed as an alternative to text based techniques. Graphical password techniques can be categorized into two schemes which are Recognition based and Recall-based graphical techniques. The pass face technique fall into recognition based technique in this technique user is given a face database and user has to click on given faces to get authenticated. The pass face technique was developed by Real User Corporation in this technique user has to select faces from a given face database to get authenticated. Here, User has to select four faces from a given face database to set his password.

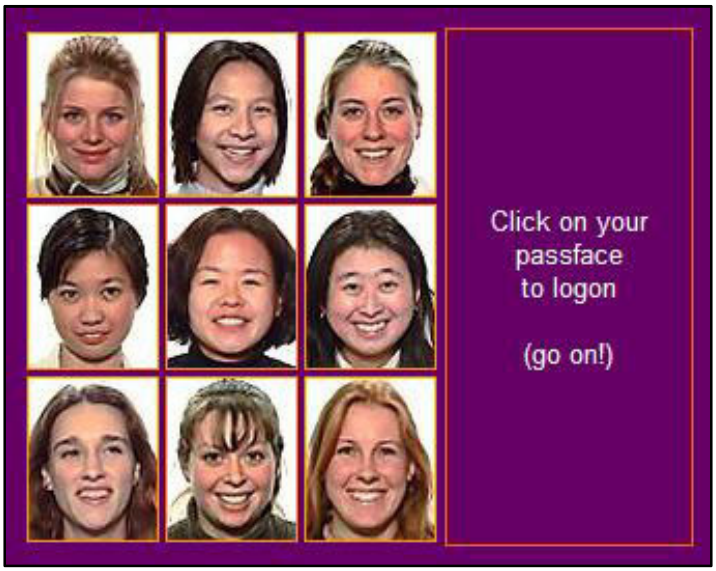

Figure 2: Example of Passfaces

1.2.3. Draw –A-Secret [4]

Similar to this a similar scheme was introduced by Syukri.In this scheme, the password is a simple picture drawn on a grid. This approach is alphabet independent, thus making it equally accessible for speakers of any language. Users are freed from having to remember any kind of alphanumeric string. This authentication scheme was based on the principle that the user has to draw his signature by using mouse. This scheme had two stages of implementation -the registration phase,-the verification phase. At the time of registration the user draws a signature that is extracted by the system. The signature is taken as an input and normalization is done and then the parameters are extracted and cheking is done and the user is authenticated if the parameters get matched. But drawing with a mouse is not so easy and actual parameters cannot be matched with the signature that was drawn at the registration time. This scheme is prone to forgery of signature.

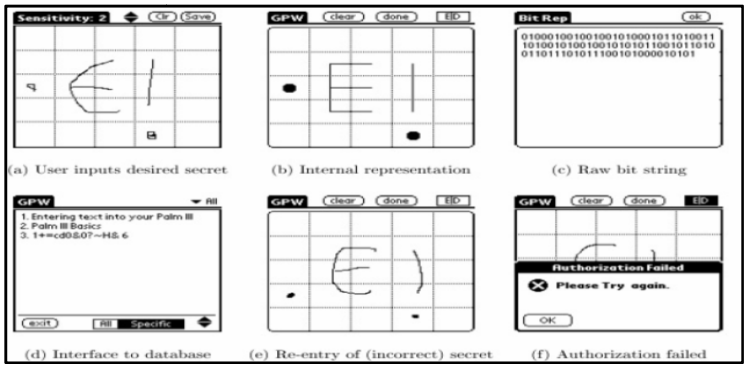

Figure 3: DAS technique by Jermyn

1.2.4. Blonder Scheme

G.E blonder designed a scheme in which an image is presented to user with tap regions, for authentication user has to click within those tap regions and in a sequence. The major drawbacks of this scheme was memorable password space, moreover, user cannot click where, he wants because of predetermined tap regions.

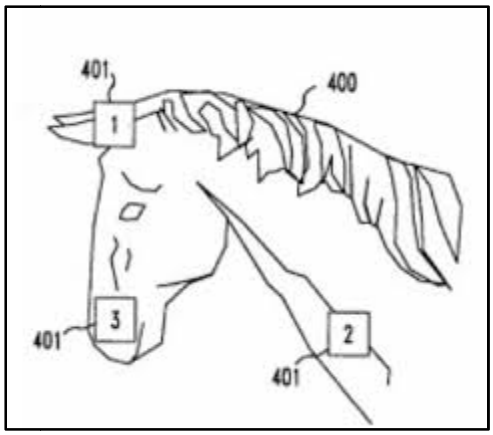

Figure 4: Blonder Scheme

1.2.5. Story-Scheme [5]

To overcome this shoulder surfing attacks a scheme was proposed by Haichang. This scheme is the combination of DAS and Story schemes. The user has to draw a curve along the images to prove their authenticity.

Figure 5: Haichang's shoulder-surfing technique

1.3. Purpose

The proposed system will add a layer to security superimposing the drawbacks of existing security schemes. The user will have a new password for every session, eradicating the need to remember a common password. The system being resistant to shoulder surfing and eavesdropping user can rely on the system for crucial transactions. The main aim is to provide an easy to use, reliable and cost-efficient system that would carry out the process of authentication.

1.3.1. Contribution of the Paper

The proposed system has 8 colors and asks user to rate each color from 1-7. Each color gets a distinct value and on the login phase all the 8 colors are randomly populated on the screen. Eight colors appear in 4 pairs. While registering, users should rate the colors. The range is from 1 to 7. Different colors can be rated the same. An interface will be displayed during the login phase when the username is entered, based on the colors selected by the user. The login interface consists of grid of size 8×8. This grid contains digits 1-7 placed randomly in grid cells. Depending on the ratings given to colors, we get the session password. Row is represented by the first color of every pair in the color grid and column is represented by the second color. We will get a number where the row and column of the grid intersect. That number is a part of the session password. For example: In the first pair of colors, Red is the first color and green as the second color. Let's suppose the rating given by user for red color is '1' and green as '2'. So '1' becomes the row number and '2' becomes the column number. At the intersection of Row 1 and Column 2, we get the number '3'. So '3' becomes the first character of our password. Similarly, 3 characters are derived from the other 3 pairs of colors. For every login, both the number grid and the color grid randomizes, so the session password changes for every session.

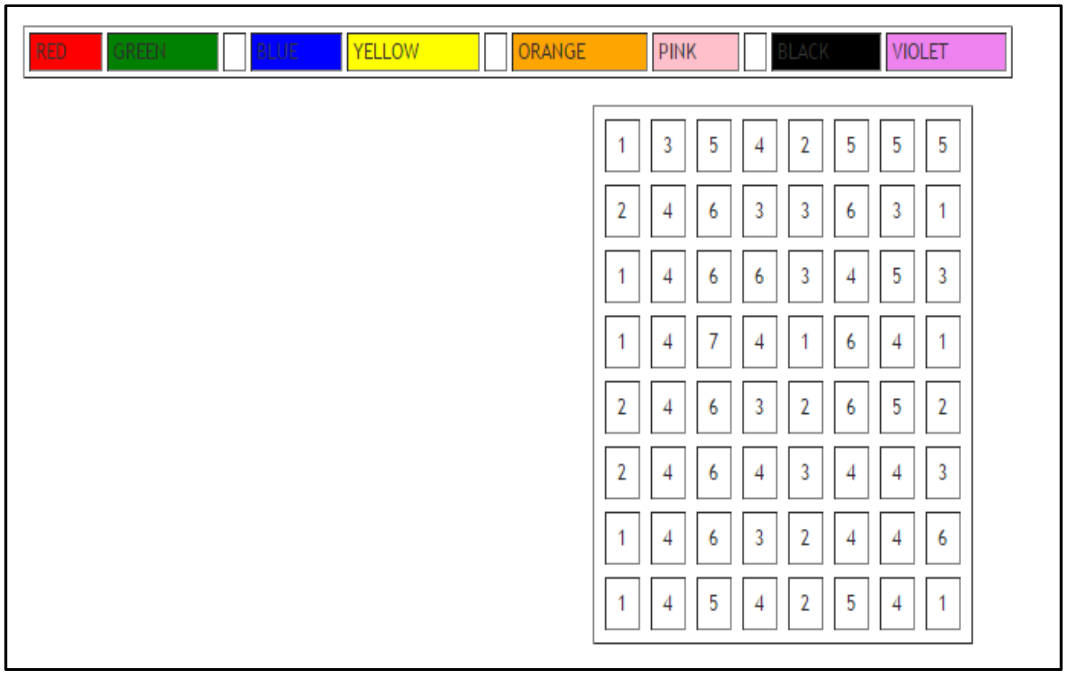

Figure 6

The verification of this password is done when the one user enters the OTP. If the password is correct, authentication takes place.

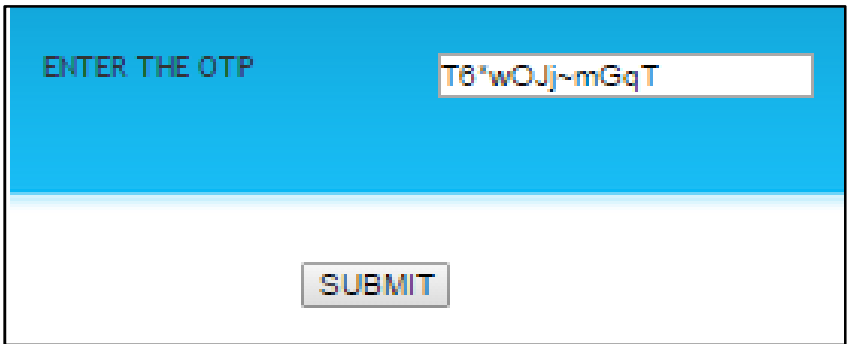

Figure 7

For authentication purpose our algorithm uses a pseudo random OTP which is redirected to users cell phone. The user enters the received OTP and comparison is done for a match. If match is found, user is granted access to the site.

2. Conclusion

There has been growing interest in picture passwords; recently one of Microsoft's operating system windows 8 has used this for authentication. We believe that the main reason for using graphical password is they can be easily recalled. Furthermore, graphical passwords are more secure than text based passwords. The proposed system provides a new concept for implementation of security through the use of color scheme authentication for session password. These techniques generate session password and are resistant to dictionary attack, brute force attack, session fixation and shoulder surfing. This technique uses a totally new implementation of grid matching for generating session password with a corresponding color rating methodology. For hybrid textual scheme, ratings should be given to colors, based on these ratings and grid displayed during login which extensively secures the process. Security is achieved because only legal user is known that what kind of color image block selected and in what sequence. However, this scheme is completely new to the users and to achieve an appropriate outcome, the scheme needs to be validated through mutation testing, which involves a number of test case inputs to be trialed to bring in more accuracy in results.

3. References

i. R. Dhamija, and A. Perrig. "Déjà Vu: A User Study Using Images for Authentication". In 9th USENIX Security Symposium, 2000.
ii. Real User Corporation: Passfaces. www.passfaces.com
iii. 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.
iv. 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.
v. Haichang Gao, ZhongjieRen, Xiuling Chang, Xiyang Liu Uwe Aickelin, "A New Graphical Password Scheme Resistant to Shoulder-Surfing
vi. 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.
vii. W. Jansen, "Authenticating Mobile Device User through Image Selection," in Data Security, 2004.
viii. W. Jansen, "Authenticating Users on Handheld Devices "in Proceedings of Canadian Information Technology Security Symposium, 2003.
ix. Graphical Password Authentication Schemes: Current Status and Key Issues Harsh Kumar Sarohi , FarhatUllah Khan
x. H. Zhao and X. Li, "S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme," in 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW 07), vol. 2. Canada, 2007, pp. 467-472.
xi. X. Suo, Y. Zhu and G. Owen, "Graphical Passwords: A Survey". In Proc. ACSAC'05.