INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 5)
Available online at: www.ijariit.com

Password authentication using symbols

Priyanka Nath
nath.priyanka51@gmail.com
SRM Institute of Science and Technology, Chennai, Tamil Nadu

Sahaya Sakila
Shyla1992lipna@gmail.com
SRM Institute of Science and Technology, Chennai, Tamil Nadu

Ananya Tamuli Saikia
ananyatsaikia@gmail.com
SRM Institute of Science and Technology, Chennai, Tamil Nadu

P. Geeta
geetap2101@gmail.com
SRM Institute of Science and Technology, Chennai, Tamil Nadu

ABSTRACT

Password authentication is one of the most important components for security and confidentiality of data that is stored on various workstations and servers. There are various kinds of ways to authenticate passwords, for example, textual passwords, graphical passwords, session passwords etc. Biometric authentication is also one of the trending ways these days but has several physiological issues. Though textual password is very common among people, it is still susceptible to various attacks like brute force attacks, dictionary attack, glossary attack, shoulder surfing, keylogger attack or eavesdropping. Graphical passwords were the new solution but had drawbacks like taking more time to authenticate and slow processing issues. Thus we introduce a new session password system, which is a one-time use password. This system uses only symbols for authentication. The generation of the password each time depends on an algorithm.

Keywords— *Authentication, Session password, Symbol, Shoulder surfing*

1. INTRODUCTION

The present era has brought along with it a new deluge of technical advancements, obviously with its pros and cons. The highest rated factor which still worries most people is Cyber Security. It is a term which is common to almost all generations, thus indicating its vitality in all fields. The most essential part of cybersecurity is password authentication. Authentication is basically the process of allowing only authorized individuals to access data. The typical way is by using textual passwords. But in the recent past, cybercrimes have increased at an alarming rate through brute force attacks, dictionary attack, glossary attack, shoulder surfing, keylogger attack or eavesdropping. The new innovative idea was to use graphical passwords as images are better memorized by humans. Though removing the attacks from shoulder surfing, this method was slow to authenticate and was quite expensive.

Session passwords these days are a new thing and is becoming popular gradually amongst people. Session passwords are generally better than normal passwords as they keep expiring with the end of each session. A new password is generated with the commencement of each new session. This secures data in a way far better than the conventional methods. Session passwords using text and colors are in use currently.

We propose a new scheme wherein session passwords use symbols. Here, in the login page user must rate the given symbols as per wish. This rating must be remembered while logging in. The login page generates a new session and remains until the user stays logged in. Each time user logs in a new session are generated and terminate as soon as it is logged out. This would aid people who have issues differentiating between colors. Also, symbols are convenient to use and provide simplicity to the application.

2. LITERATURE SURVEY

Dhamija and Perrig [1], proposed a graphical authentication scheme which is used to prove the user's authenticity. The user, here, selects some images from a pool of random pre-defined images during the registration process. Later the user has to identify the selected images for verification. This system is vulnerable to shoulder-surfing.

Passfaces [2], as suggested by Real User Corporation, uses a system where the user is given a grid of nine faces and has to select a particular face. This process is repeated four times as four such images are chosen as the password. Later on, during authentication, the pass images are chosen from eight other decoy images.

Jermyn [3], describes a paper, "The design and analysis of graphical passwords", where a new technique is proposed called "Draw-a-Secret". Here, the user is required to draw a pre-defined picture on a 2D grid during registration. The same image has to be drawn during authentication. If the drawn image touches the grid in exactly the same sequence then the user is authenticated. The process is time-taking and vulnerable to shoulder-surfing.

Syukri [4], describes in the paper, "A user identification system using signature is written with a mouse", an authentication method where the user draws his/her signature with a mouse. This technique requires two steps, i.e: registration and verification. The user initially draws his signature with a mouse during registration. This system is extracted by the system. Later, during verification user is supposed to re-draw the signature. The system here takes in the signature as input, normalizes it and extracts the parameters of the signature. Authentication of a password depends on the congruency of the two signatures. The disadvantage of this method is the forgery of signatures. Also, it is difficult to draw signature with a mouse as most people aren't accustomed to it.

Haichang Gao [5], in the paper, "A new graphical password scheme resistant to shoulder surfing", came up with a new shoulder-surfing resistant scheme. The user here draws a curve around the password images, instead of clicking on them directly. This graphical scheme combines DAS and Story schemes to provide authenticity.

Wiendenbeck [6], employs a graphical password entry scheme which uses the convex hull method to narrow down shoulder surfing problems. The user here selects from a pool of random pass objects which form a convex hull and selects on the inside of the objects. For complex passwords, a large number of objects are used, making the display crowded and objects highly obscure. Fewer objects lead to smaller passwords which are easy to hack.

Jansen [7], describes in the paper, "Authenticating users on handheld devices", a graphical password scheme for mobile devices. The user selects a sequence of thumbnail size pictures as a password. During authentication, the same order must be followed. Each thumbnail has a numerical value assigned to it. The sequence thus generates a numerical password. Image limit is 30.

Zheng [8], in the paper, “A Hybrid password authentication scheme based on shape and text”, uses the basic concept of mapping shape to text with strokes of shape and grid with text.
Takada and Koike [9], in their paper, "Awase-E: Image-based authentication for mobile phones using the user's favorite images", suggested a method where the user chooses his/her own images. The user then recognizes these images among decoy images during verification. There multiple stages of verification and each time a user has to select pass-images. Authentication succeeds if all stages are passed successfully.

S.Tidke, N.Khan and S.Balpande [10], in their paper, "Password using text and colors", suggested a system where user rates colors during registration. This rating must be remembered. During login, a 10 x 10 number grid is provided, where ratings are to be input in accordance with the colors. The position of the numbers in the grid are set with respect to an algorithm. The position of numbers in the grid changes with every new session, thus generating a different numerical password each time. Session passwords are this harder to hack.

3. EXISTING SYSTEM

Passwords are the most common way to prove our identities on social media accounts, various websites, email accounts, or for accessing bank accounts via net banking etc. Authentication is an important part, which permits access to personal and at times confidential details of an individual.

Usually, textual passwords are used by people. This kind of passwords suffers from various attacks such as brute force attacks, dictionary attack, glossary attack, shoulder surfing, keylogger attack or eavesdropping. To avoid such attacks, people usually keep long and complex passwords but as humans to remember such passwords becomes a rather rigid process. But on the other hand, keeping short and easy to memorize passwords can cause it to fall prey to such attacks easily.

An alternative was to use Graphical passwords. This would somehow overcome attacks like shoulder surfing and was also suggested as supported by psychological studies that humans can memorize images better than texts. But also has disadvantages like slow authentication and is also quite expensive.

Biometric authentication consists of human body characteristic verification. For example, retina scan or fingerprint detection. But this technique has various physiological issues and is also very expensive. Session passwords are in trend nowadays as it is one-time use password and has fewer risks of any kinds of attacks. There are session passwords using text and color, but on a deeper level, this might pose some kind of inconvenience for the visually impaired individuals or else people diagnosed with color blindness (it is hard to differentiate between certain colors).

We thus propose a new system using Symbols.

4. PROBLEM STATEMENT

As per the survey, most of the people still use the traditional way of authenticating the password, ie. Textual passwords. Graphical passwords too, though less in use, is still seen as a better option, sometimes, as it avoids shoulder surfing. Every system has flaws of their own. As we have already seen, Textual passwords suffer from brute force attacks, dictionary attack, glossary attack, shoulder surfing, keylogger attack or eavesdropping. Likewise, Graphical passwords too have cons like taking more time to authenticate and slow processing. Biometrics are way too expensive.

To improvise on such problems, we have introduced session passwords using symbols. In such a case user will rate the pre-defined symbols and session password would be generated based on the algorithm and rating together.

5. PROPOSED SYSTEM

The problems generated by textual and graphical passwords are now well known. We thus provide a system wherein the user is asked to give ratings to various pre-defined symbols during the registration process as shown in figure 1. The ratings must be memorized. The symbols which are pre-defined, are in pairs in

the registration form. During each login process, a 10x10 grid having numbers from 0-9 would be provided as shown in figure 2. The numbering of the grid varies each time in accordance with the algorithm provided. Here, the first symbol of every pair represents the row and the second symbol acts as the column of every grid. So the rating of the first symbol has to be searched for, in the row and likewise, the rating for the second symbol has to search for in the column. The intersection of the two gives the first digit of your session password. For example, if we choose symbols (!,@), the rating for (!) is 2 and for (@) is 7. So we search for the number at the intersection of a 2nd row and 7th column in the grid, that is 7. The session password remains until the user logs out of the current session. For the next time user logs in a separate session, a password is created and is valid only for that particular session. After termination of every session, the session used for that particular session becomes invalid. Session passwords are far more secure than any kind of textual or graphical password authentication. These are very tough to hack as each time a new password is generated. Using symbols also adds on as a beneficial factor.

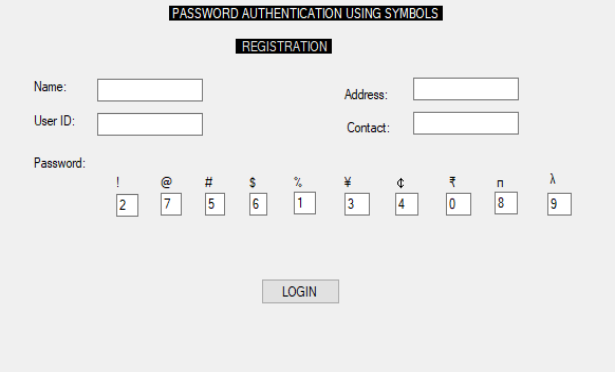

Fig. 1: Symbol rating

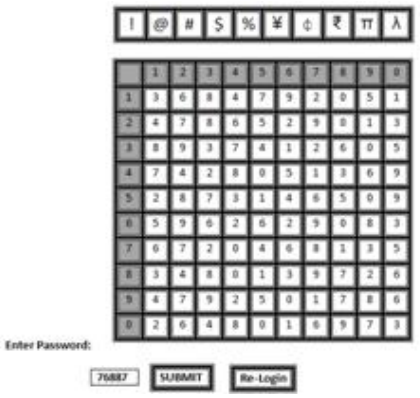

Fig. 2: Login interface

6. CONCLUSION

The technique implemented in the paper serves its purpose by making it user-friendly. The scheme aims at avoiding attacks like shoulder surfing, dictionary attack and brute force attack without implementation of color or text anywhere. Here, a grid is provided to generate new session passwords every time. The scheme fits in well for people who are diagnosed with color-blindness. It is also a new concept for people who would normally view it as a new variety of password authentication. The process is highly secured and is difficult for anybody to hack easily.

7. REFERENCES

[1] Dhamija, Perrig, "Déjà vu: A User Study Using Images for Authentication". In 9th USENIX Security Symposium, 2000.

[2] Real User Corporation: Passfaces. www.passfaces.com

[3] Jermyn, "The design and analysis of graphical passwords" in Proceedings of USENIX Security Symposium, August 1999.

[4] 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] Haichang Gao, Zhongjie Ren, Xiuling Chang, Xiyang Liu Uwe Aickelin, "A new Graphical Password Scheme Resistant to Shoulder-Surfing".

[6] S. Wiendenbeck, 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.

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

[8] Z. Zheng, X. Liu, L.Yin, Z.Liu, "A Hybrid password authentication scheme based on shape and text " Journal of Computers, vol.5, no.5 May 2010.

[9] Takada Tetsuji, Koike Hideki, "Awase-E: Image-based authentication for mobile phones using user's favorite images ".

[10] Swati Tidke, Nagama Khan and Swati Balpande, "Password using text and colors ". International Journal of Scientific Research Engineering and Technology (IJSRET), ISSN 2278-0882, vol.4, Issue 3, March 2015.

[11] S. Man, D. Hong, and M. Mathews, "A shoulder-surfing resistant graphical password scheme," in Proceedings of International conference on security and management. Las Vegas, NV, 2003.

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

[13] M Shashi, M Anirudh, MD Sultan Ahamer, V Manoj Kumar, "Authentication Schemes for Session Password using colors and Images", International Journal of Network Security and Its Applications (IJNSA), Vol.3, No.3, May 2011.

[14] PritiJadhao, Lalit Dole, "Survey of Authentication Password Techniques", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-2, May 2013.

[15] L.D.Paulson, "Taking a Graphical Approach to the Password, "Computer, vol. 35, pp. 19, 2002.

