International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 02 | Feb-2018 www.irjet.net p-ISSN: 2395-0072

Survey on Graphical Password Authentication Techniques

Aishwarya N. Sonar[1], Purva D. Suryavanshi[2], Pratiksha R. Navarkle[3], Prof. Vijay N. Kukre [4]

[1,2,3]Diploma Students of Computer Engineering, All India Shri Shivaji Memorial Society's Polytechnic, Kennedy Road, Near RTO, Pune-411001, India.
[4]Professor Vijay N. Kukre, Department of Computer Engineering, All India Shri Shivaji Memorial Society's Polytechnic, Kennedy Road, Near RTO, Pune-411001, India.

Abstract - *In a current time, the greatest prominent user authentication system which is extensively uses the out-dated method. It comprises of "username" and "password", which is usually through text. This system has definitely revealed disadvantages which cannot be ignored. However, Strong text passwords are hard to remember, thus the users incline to write them down or attempt to save them on as files on digital means. Now, several computer systems, networks and internet-based condition are demanding the use of graphical authentication method. Therefore, base of an authentication system is to stimulate users to pick healthier password, which increases security, usability and also refining the password space. In this study paper, we complete an inclusive survey of the current graphical password systems into recognition based, pure-recall based, cued-recall based and multifactor methods. We also studied strength and drawback of graphical password schemes.*

Key Words: **Graphical password, Authentication systems, Text passwords, Shoulder Surfing.**

1. INTRODUCTION

Systems like conventional password systems such as word-based password system, graphical system are commonly used for authentication. But these systems are susceptible to dictionary attack, shoulder surfing attack, accidental login. Hence the word-based Shoulder surfing resistant graphical password schemes have been proposed. The shoulder surfing attack is an attack where illegal user can get authorized user's password by observing over his shoulder when he enters his password. Though, as most handlers are more aware with word-based passwords than graphical passwords. The existing word-based shoulder surfing resistant graphical password systems are not secured and effective enough Another vulnerability attack regarding textual password is keyloggers. In Keyloggers any key pressed by the user is monitored by unauthorized users. A keylogger can be either software or hardware. By using Keylogger a person can steal the victim's personal information, transmission can be interrupted by hackers, it can prove very dangerous for people who are using online cash sites, or when they are typing their passwords. In various proposed system, the user can simply and efficiently login to the system without using any keyboard. It is very relaxed for the user to login. It has become very hard to guess the password because of text and color combination. The systems provide extra security.

Most of the authentication system now-a-days uses a combination of username and password for authentication. Due to the restriction of human memory, most users incline to select short or simple passwords which are easy to recall. Graphical passwords use images rather than word-based passwords and are comparatively inspired by the fact that users can recall pictures more simply than a string of characters. A graphical password is an validation method where the user have to pick from images, in a certain order, accessible in a graphical user interface. Graphical passwords may provide improved security than word-based passwords because various individuals, in an attempt to remember word-based passwords, use basic words. In various proposed systems one time passwords are used for security purpose. An OTP is a set of characters that can act as a form identity for one time only. Once the password is used, it cannot be used for any extra authentication. Even if the hacker gets the password, it is possible that it was previously used once, as it was being conveyed, therefore unusable to the hacker. Another way used for providing increased security is session passwords. Session passwords are passwords that are used only once. When the session is completed, the session password is no more useful. For every single login procedure, users input dissimilar passwords. The session passwords provide better security against dictionary and brute force attacks as password changes for every session. The planned authentication systems use text and colors for producing session passwords.

2. LITERATURE SURVEY:

[1] In Dec 2009 author H. Gao proposed graphical password scheme using color login. In this color login uses background color which decrease login time. Possibility of accidental login is high and password is too short. The system developed by Sobrado is improved by combining text 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. The advantages of this system is that it reduces the login time, session passwords are also generated to improve security. The disadvantage of this system is that it the possibility of accidental login is high and password is too short.

[2] In this paper M. Sreelatha proposed Hybrid Textual Authentication Scheme. This scheme uses colors and user has to rate the colors in registration phase. During login phase four pairs of colors and 8*8 matrix will be displayed.

As the color rating given by the user, the password will generate. First color shows row number and second shows column number of the grid. The drawback of this system is intersecting element is the first letter of the password. The user has to memorize the rating and order of the colors. So it becomes very hectic to user. The benefit of this system is that it is flexible and simple to use.

[3] A hybrid graphical password based method is advised, which is a mixture of recognition and recall based methods having many advantages as compare to existing systems and more suitable for the user. In this system the user draws the selected object which is then stored in the database with the specific username. Objects may be symbols, characters, auto shapes, simple daily seen objects etc. Then the user draws pre-selected objects as his password on a touch sensitive screen with a mouse. Then the system performs pre-processing. Then after stroke merging, the system constructs the hierarchy then the next step is sketch simplification, then the three types of features are extracted from the sketch drawn by the user. The last step is called hierarchical matching. The plus point of this system is it's a combination of recognition and recall based technique, hence provides flexibility. This system performs some complex actions like pre-processing, stroke merging. So it can be a weakness of this system.

[4] Authors proposed a system in which password scheme uses colors and text for generating session password. They have introduced a session password scheme in which the passwords are used only once for each session and when session is completed the password is no longer in use. In this system two session password schemes pair-based textual authentication scheme and color code-based authentication scheme are introduced In the pair based textual authentication scheme the user submits his password during the registration. The password should contain number of characters. When the user enters login an interface containing of a grid is showed during the login phase. The grid is of size 6 x 6 and it contains of alphabets and numbers. These are randomly placed on the grid and the interface changes every time. Depending upon the password which is submitted during the registration phase, user has to enter the password. Users have to consider his password in terms of pairs. In the color code based scheme, the user has to get his password with the help of colors. During registration phase, user should fill up all his information and also rate colors. The merit of this system is it provides much better security. Demerit of the system is sometimes users may consider wrong password as they are supposed to consider the password in terms of pair.

[5] In Graphical password as an OTP proposed by authors, she used the scheme of OTP. As there are many drawbacks of using alphanumerical passwords, people tend to forget the password, or they may write the password somewhere. Hence they have developed authentication methods that use pictures as passwords known as graphical password to solve this problem. They have provided an additional layer of security by generating one-time password(OTP) which is send to the users mobile. Using the instant messaging service available on internet, user will obtain the One Time Password (OTP). The OTP will be the information of the items present in the image to be clicked by the user. The users will authenticate themselves by clicking on various items in the image based on the information sent to them. The main aim of this system is to avoid Shoulder surfing attack. It also aims to avoid other attacks like dictionary attack, brute force attack and guessing attack. The OTP is sent on the user's mobile number from the database. The positive point of this system is it provides better security as it avoids shoulder surfing by using OTP. Negative point of this system is user must click within the tolerance of their chosen pixels and also in correct sequence.

[6] Authors proposed four systems which mainly focuses on graphical password. The textual-based password system is a popular authentication system since ancient times. It has many advantages but at the same time it has a few drawbacks too. Hence, the current graphical password techniques, is classify into four techniques as recognition-based, pure recall-based, cued-recall based and hybrid based. [A]In the recognition based algorithm the user must memorize the portfolio of images during the password creation. When the user logs in, the user must recognize the images form decoys. Various images like faces, icons, everyday objects, random arts etc. can be used. In the pure recall-based system the user recalls the outline drawing on the grid which they have created or selected during registration phase. In this system the user usually draws their password either on grid or on blank canvas. The cued-recall based system is similar to recall system but it is recalled with cueing. In this system remainders are send to the user to reproduce the password accurately. The Hybrid system is a combination of two or more password schemes. It is used to overcome the limitation of single system, such as hotspot problem. The advantage of this system is it provide high authentication process as it is categorized in four techniques. Disadvantage of this system is it's a complex and long term process.

[7] Authors proposed a scheme which mainly focuses on shoulder surfing. In this system, they proposed a new click-based color password scheme called Color Click Points (CCP). It can be viewed as a combination of Pass-Points, Pass faces, and Story. A password consists of one click-point per Color for a sequence of Colors. The next Color displayed is built on the previous click-point. In this proposed scheme, we propose an improved text-based shoulder surfing resistant graphical password scheme by using colors. In the proposed scheme, the user can easily and efficiently login system. Afterward, we examine the security and usability of the proposed system, and show the resistance of the proposed system to shoulder surfing and accidental login. The benefit of this system is that it reduces the login time & it is an efficient system.

3. CONCLUSION

Hence the various methods from recognition based, cued recall based and hybrid systems of graphical password methods are studied. Although the main feature about graphical password is that users are able to memorize the graphical password than text-based passwords. Based on the survey, according to us the best one was "Graphical Password Based on OTP" because it provides extra security as it uses One Time Password (OTP). This system has one more advantage i.e. this not only avoids shoulder surfing but also avoids dictionary attack, brute force attack, guessing attack, etc. Therefore, it is more useful for visually impaired people.

REFERENCES

[1] Dec 2009, H. Gao proposed paper on "graphical password scheme using color login".

[2] In May 2011, M. Sreelatha proposed Hybrid Textual Authentication Scheme.

[3] Er. Aman Kumar, Er. Naveen Bilandi, Department of Computer Science and Engineering, DAV University, Jalandhar, Punjab, India "Graphical Password Based Authentication Based System for Mobile Systems".

[4] Miss.Swati Tidke, Miss Nagama Khan, Miss.Swati Balpande Computer Engineering, RTM nagpur university, M.I.E.T Bhandara, "Password Authentication Using Text and Colors".

[5] Veena Rathanavel, Swati Mali, Student M. Tech, Department of Computer Engineering, K J Somaiya, College of Engineering Mumbai, "Graphical Password as an OTP".

[6] Veena Rathanavel, Swati Mali, Student M. Tech, Department of Computer Engineering, K J Somaiya, College of Engineering Mumbai, "Graphical Password as an OTP".

[7] In 2017 Aayush Dilipkumar Jain, Ramkrishna Khetan Krishnakant Dubey, Prof. Harshali Rambade K. Elissa, Department of Information Technology Vidyalankar Institute of Technology, Mumbai, "Color Shuffling Password Based Authentication".