Human Resource Management by using Graphical Password

D. Kanyakumari[1], Mr. S Munikumar[2]
[1] *Student, Dept. of MCA, KMM Institute of Post Graduate Studies*
[2] *Assistant Professor, Dept. of MCA, KMM Institute of Post Graduate Studies, Tirupati,A.P*

***Abstract*- Passwords provide security mechanism for protection services against unwanted access to resources. A graphical based password is one promising alternatives of textual passwords. According to human psychology, humans are able to remember pictures easily. In existing, a new hybrid graphical password based system, which is a combination of recognition and recall based techniques that offers many advantages. In proposed system is new graphical passwords based hybrid system which is a combination of recognition and recall based techniques and consists of two phases. During the first phase called Registration phase, the user has to first select his username and a textual password. Then objects are shown to the user to select from them as his graphical password. After selecting the user has to draw those selected objects on a touch sensitive screen using styles. During the second phase called Authentication phase, the user has to give his username and textual password and then give his graphical password by drawing it in the same way as done during the registration phase.**

***Index Terms*- Password, Registration phase, Human resource**

I. INTRODUCTION

One of the major functions of any security system is the control of people in or out of protected areas, such as physical buildings, information systems, and our national borders. Computer systems and the information they store and process are valuable resources which need to be protected. Computer security systems must also consider the human factors such as ease of a use and accessibility. Current secure systems suffer because they mostly ignore the importance of human factors in security. An ideal security system considers security, reliability, usability, and human factors. All current security systems have flaws which make them specific for well trained and skilled users only. A password is a secret that is shared by the verifier and the customer. Passwords are simply secrets that are provided by the user upon request by a recipient." They are often stored on a server in an encrypted form so that a penetration of the file system does not reveal password lists. Passwords are the most common means of authentication because they do not require any special hardware. Typically passwords are strings of letters and digits, i.e. they are alphanumeric. Graphical passwords (GP) use pictures instead of textual passwords and are partially motivated by the fact that humans can remember pictures more easily than a string of characters. The idea of graphical passwords was originally described by Greg Blonder in 1996. An important advantage of GP is that they are easier to remember than textual passwords. Human beings have the ability to remember faces of people, places they visit and things they have seen for a longer duration. Thus, graphical passwords provide a means for making more user friendly passwords while increasing the level of security. Besides these advantages, the most common problem with graphical passwords is the shoulder surfing problem: an onlooker can steal user's graphical password by watching in the user's vicinity. In proposed system is new graphical passwords based hybrid system which is a combination of recognition and recall based techniques and consists of two phases. During the first phase called Registration phase, the user has to first select his username and a textual password. Then objects are shown to the user to select from them as his graphical password. After selecting the user has to draw those selected objects on a touch sensitive screen using a stylus. During the second phase called Authentication phase, the user has to give his username and textual password and then give his graphical password by drawing it in the same way as done during the registration phase.

II. RELATED WORK

In 2002, Sobrado and Birget planned 3 capture attacks resistant graphical password methods, the Movable Frame method, the Intersection section method, and therefore the Triangle method. within the Triangle method, the user should notice 3 of the pass-icons designated at the registration time and click on within the invisible triangle developed by those 3 pass-icons to complete a challenge. within the Movable Frame method, the user should search the 3 displayed pass-objects, then move the frame till the pass-icons on the frame lines up with the opposite 2 pass-icons within the given fame. The Intersection method uses the intersection of the invisible lines shaped by four displayed pass-icons. The user should click close to the intersection of the 2 invisible lines within the convexo-convex quadrilateral shaped by those four pass-icons. In 2005, Sobrado associated Birget projected the convex Hull Click scheme (CHC) as an improved version of the Triangle method with high security and value. Since then, several capture attacks resistant graphical Arcanum method with totally different degrees of resistance to capture attacks are projected, and every has its execs and cons. As most current users area unit additional acquainted with matter passwords than graphical passwords, Zhao in 2007 projected a capture attacks resistant textual graphical password method, S3PAS, during which the user has got to notice his matter password then follow a special rule to combine his matter password to urge a session password to login the system. However, the login method of Zhao.'s method is advanced and difficult. In 2011, Sreelatha . projected a capture attacks resistant graphical password method depend on text, the Pair-Based method. However, its resistance to accidental login is deficient and its resistance to capture attacks is unsatisfactory . within the same year, Kim et al. planned a capture attacks resistant graphical password method depend on textual password, associated utilized an analysis technique for accidental login resistance and capture attacks resistance to investigate the security of their method. sadly, its resistance to accidental sign in is deficient and its resistance to capture attacks is unsatisfactory . In 2011, Imran. additionally projected a capture attacks resistant text-based graphical password scheme, the Advance Secure Sign in method, within which the user needs to consecutive notice every pass-character of his textual password so respond the corresponding range higher than it to sign in the system. However, the resistance of the Advance Secure Login method to accidental login is deficient and therefore the resistance of the Advance Secure Login theme to capture attacks is unsatisfactory. In 2012,Rao. projected a capture attacks resistant text-based graphical password method. To login the system, the user needs to combine his matter password to provide many pass-pairs, so follow four library rules to urge his session password on the sign in screen. However, the login method of PPC is simply too satisfied and tedious. supported squares rather than triangles. However, 3LAS continues to be too complicated to use and its resistance to accidental sign in is weak.

III. CLASSIFICATION OF GRAPHICAL PASSWORD BASEDSYSTEM

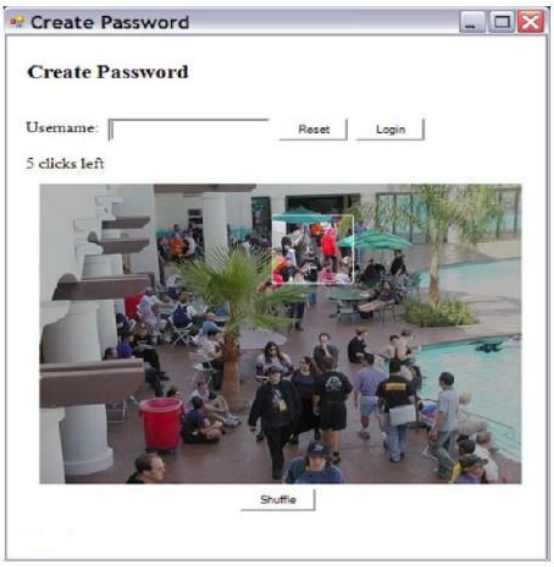
Graphical based passwords schemes can be broadly classified into four main categories: First is Recognition based Systems which are also known as Congo metric Systems or Search metric Systems. Recognition based techniques involve identifying whether one has seen an image before. The user must only be able to recognize previously seen images, not generate them unaided from memory. Second is Pure Recall based systems which are also known as drawn metric Systems. In pure recall based methods the user has to reproduce something that he or she created or selected earlier during the registration stage. Third is Cued Recall based systems which are also called Icon metric Systems. In cued recall-based methods, a user is provided with a hint so that he or she can recall his his/her password. Fourth is Hybrid systems which are typically the combination of two or more schemes. Like recognition and recall based or textual with graphical password schemes.

IV. LITERATURE REVIEW

Here we are mentioning the literature review the works which have already done in the field of image password-

- Persuasive cued click point PCCP encourages and guides users in selecting more random click-based graphical passwords. A key feature in PCCP is that

creating a secure password is the ―path-of-least-resistance‖, making it likely to be more effective than schemes where behaving securely adds an extra



In this technique we are creating a password in particular hotpot area of an image, where we are selecting a particular portion to create a password, whereas in CCP we are going to create a password in whole image which give us less success rate in order to get into login process. Still the problem into this scheme was to get good success rate while login into the system but effective in case of attack than textual password, so further enhancement moving to another graphical scheme.

 Taking the number of different images or set of images and selecting or more as a password, which is easy to remember and giving a good success rate than Previous demonstrated .

V. CONCLUSION

In this system, there is a growing interest in using pictures as passwords rather than text passwords but very little research has been done on graphical based passwords so far. In view of the above, we have proposed authentication system which is based on graphical password schemes. Although our system aims to reduce the problems with existing graphical based password schemes but it has also some limitations and issues like all the other graphical based password techniques. To conclude, we need our authentication systems to be more secure, reliable and robust as there is always a place for improvement. Currently we are working on the System Implementation and Evaluation.

REFERENCES

[1] A.Perrig and D.Song, “Hash Visualization: A New Technique to improve Real-World Security”. In International Workshop on Cryptographic Techniques and E-Commerce, pages 131--138, 1999.

[2] D.Davis, F.Monrose and M.K.Reiter, “On User Choice in Graphical Password Schemes”. In 13th USENIX Security Symposium, 2004.

[3] Wing Ho Leung and Tsuhan Chen, “Hierarchical Matching For Retrieval of Hand Drawn Sketches”, In Proceeding of International Conference on Multimedia and Expo - Volume 2 (ICME '03), 2003.

[4] Hafiz Zahid Ullah Khan, “Comparative Study of Authentication Techniques”, International Journal of Video & Image Processing and Network Security IJVIPNS Vol: 10 No: 04

[5] Token Based Authentication: http://www.w3.org/2001/sw /Europe/events/foaf galway/papers/fp/token_based_authentication/ [last visited on 02/05/11].

[6] Knowledge Based Authentication: http://csrc.nist.gov/archive/ kba/index.html [Last Visited on 02/05/11].

[7] Knowledge based Authentication: http://searchsecurity.techtarget.com/definition/knowledge-basedauthentication [Last Visited on 02/05/11].

[8] A Survey on Recognition based Graphical User Authentication Algorithms: http://www.scribd.com/doc/23730953/A-Survey-onRecognition-Based-Graphical-User-Authentication-Algorithms [Last Visited on 02/05/11].

[9] X. Suo, “A design and analysis of graphical password”, Master's thesis, College of Arts and Science, Georgia State University, August 2006.

[10] S. Chiasson, P. C. van Oorschot, and R. Biddle, “Graphical password authentication using Cued Click Points”, In European Symposium On Research In Computer Security (ESORICS), LNCS 4734, pages 359{374, September 2007. .

[11] A.Stubblefield and D. Simon, "Inkblot Authentication", MSRTR-2004-85, Technical report, Microsoft Research, 2004.

[12] F. Alsulaiman and A. El Saddik, "A novel 3D graphical password schema", In IEEE Int. Conf. on Virtual Environments HumanComputer Interfaces and Measurement Systems, July 2006.

[13] Arash Habibi Lashkari, Dr. Rosli Saleh, Samaneh Farmand, Dr. Omar Bin Zakria, "A wide-range survey on Recall-Based Graphical User Authentications algorithms based on ISO and Attack Patterns", (IJCSIS) International Journal of Computer Science and Information Security,Vol. 6, No. 3, 2009.

[14] Farnaz Towhidi, Maslin Masrom, "A Survey on RecognitionBased Graphical User Authentication Algorithms", (IJCSIS) International Journal of Computer Science and Information Security, Vol. 6, No. 2, 2009.

[15] N. Govindarajulu and S. Madhvanath, "Password management using doodles", In 9th International Conference on Multimodal Interfaces (ICMI), November 2007.

[16] Michael Kimwele, Waweru Mwangi, Stephen Kimani, "Strengths of a Colored Graphical Password Scheme", International Journal of Reviews in Computing, 2009-2010 IJRIC& LLS.

[17] Ahmad Almulhem, "A Graphical Password Authentication System", World Congress on Internet Security (WorldCIS-2011), London, UK, February 21-23, 2011.

[18] P.C. van Oorschot Tao Wan "TwoStep: An Authentication Method Combining Text and Graphical Passwords" 4th International Conference, MCETECH 2009, Ottawa, Canada, May 4-6, 2009.