Study on Recognition based Graphical Password Techniques

[1]Shritha Bharadwaj, [2]Dr Devaraj Verma C
[1]Student, [2]Associate Professor
1Department of Computer Science and technology, Jain (Deemed to be University), Bengaluru, India

Abstract: This paper investigates and analyzes the graphical password scheme, relying on recognition. Few graphical password schemes focused on recognition are being researched and evaluated with respect to their security risks. Preventative measures and recommendations for avoiding and reducing the threats are provided. The results include a comparative description of the chosen recognition-based graphical password scheme.

***Key words*–Authentication, Graphical Password, Information Security.**

I. INTRODUCTION

The urge for potent computer security is growing with the accelerated advancement of technologies and applications [1]. Most computer systems and applications are reconstructed with user identification & authentication. However, due to ready to accept nature of consumer, many of the authentication techniques have faults. Although there are many ways to authenticate a person, using the password method is the most commonly used means of authentication.

Passwords always comply with two basic contradictory requirements in which they must be secure and easy to remember[2]. However, using alphanumeric passwords is hard to achieve this, because a long and random password is secure, but it is difficult to recall for users. Users commonly have a tendency to use poor password[3]. Graphical password was then implemented as an alternative authentication system to solve the memorability concern for alphanumeric-text passwords[3].

Greg Blonder first clarified the idea of graphical passwords back in 1996 [4]. It is easier to remember graphical password than alphanumeric password which is a significant benefit of it [4]. Graphical passwords use images instead of alphanumeric passwords as people can quickly identify images than a number of characters [6]. Human beings are capable of recognizing places they frequent, the faces of other people and things [7]. Hence, the graphical password system paves a path by presenting passwords much easier to use while improving the security level. The most applauded problem with graphical passwords, except for those enhancements, is the shoulder-surfing attack [3].Head-surfing refers to the use of methods of direct observation, for example eyeballing over someone's head, to gain information[3]. The changing passphrase generation method for encrypting the information exchanged between the two nodes is implemented by TOTP algorithm to attenuate the attackers [5]. Numerous researchers have tried to overcome this challenge by having separate procedures. Therefore, we begin this research to find out the algorithmic level issue of different recognition-based graphical password schemes how they implemented these schemes and why the shoulder-surfing issue and other attacks occur in the field of recognition-based graphical passwords.

II. METHODOLOGY

The work begins with collecting knowledge about current graphical password schemes based on recognition. For example, the information is accumulated from various sources – journals, conference papers, and legitimate sites. To discover the virtues and inadequacies, the perceived structures are dissected. Reports from the review allow for a prevalent understanding of the latest issues and problems surrounding existing graphical password schemes. Such knowledge is used as a part of the way the research goals are rendered and defined.

III. RESEARCH BACKGROUND

A graphical password system is a program that performs authentication using artifacts (images / icons / symbols) [9]. In a graphical password scheme there are two key procedures-the registration procedure and the authentication procedure. Users are expected to register such items as their password from a database during the enrollment procedure [10]. The users will be given a task set in the authentication protocol to perform authentication. Users are expected to recognize the proper objects before being able to access a safe network.

Graphical passwords can be divided into three categories — recognition-based, pure recall-based, and cue recall-based [11]. Graphical password schemes based on identification usually allow users to register and memorize objects during the authentication process. During the authentication process users are required to click the correct objects. In each challenge set, the correct objects can be the registered objects, part of the registered objects, or pass-objects that identify using some method. Users are expected to remember and represent a covert drawing within a given grid or blank canvas in recall based graphical password systems, based on the registered objects. On the other hand, cued recall-based graphical password systems needed users to remember and pinpoint target on specific locations within a picture.

In this paper, we only focus on the study of recognition-based graphical password systems because based on our reviewed, majority of the articles were found belongs to this category. The selected recognition-based graphical password systems are reviewed as below.

IV. RECOGNITION BASED GRAPHICAL PASSWORD TECHNIQUES

PassfacesTM is a commercial product, and is one of PassfacesTM Corporation's earliest recognition-based graphical password systems [12]. Users are required to register photos of human faces during the enrollment process. Users are asked to click on the registered pictures to sign in to the authentication process. This system is easy to use and is simple [13]. However, it is vulnerable to shoulder-surfing attack. In fact, people with a prosopagnosia condition (face blindness) would find this device hard to use.

Users are required in Déjà Vu framework to register several "random art" images during the enrollment process [1]. The users are expected to click on the registered images to sign in to the authentication procedure. This system is user friendly and simple. The proper choice of the pictures during authentication, however, makes it vulnerable for shoulder-surfing attack.

The Picture Password scheme, suggested by [14], is for mobile devices such as the PDA. Users may either pick images from one of three predefined themes or include their own images during the process of enrollment. Users are expected to click on the registered images to sign in to the authentication process. This program attempts to increase the password space by allowing for the selection of two images as one file. The careful collection of the images during authentication, however, allows for easy observation of shoulder-surfing attacks.

Users are required in Triangle framework to register and remember three icons during the enrollment process [1]. The users are required to digitally shape a polygon using the three registered icons in the authentication procedure. To complete a challenge package, the users need to click one of the icons (pass-icon) within the polygon area (convex hall). Upon logging in, users are expected to pass several challenge sets. In addition to the approved icons this program uses other icons to sign in. Therefore, the device can withstand direct shoulder-surfing assault through observation.

Enrollment process requires user to select and remember 3 icons in Moving Frame System [9]. Authentication process includes the movement of frames in rotational format such that 2 icons registered by user should be placed inside the frame in a straight line. Before logging in, users are expected to pass multiple challenge sets. This system does not require registered users to click on the icons. Hence, it can withstand direct shoulder-surfing assault by observation. However, the users only have four ways to rotate the frame. So chances are very high for attackers to guess the right rotation.

In the Special Geometric Configuration (SGC) system [9], Users are expected to register four icons during the enrolment process. Users need to find the identified icons inside the authentication process. The users then should use two of the registered icons to virtually create a line. To login, users have to click on the intersection icon that the two virtual lines made. This program also doesn't allow users to click on the registered icons. The system is thus able to resist direct shoulder-surfing attack by observation.

Version one and version two are Visual Identification Protocol (VIP) systems that predefined a set of registered images to users, rather than allowing users to register during the registration process[17]. The users are required to identify the correct images in sequence in the authentication procedure before they can log in. The difference between VIP1 and VIP2 is how the images are arranged, and how many images are used. VIP1 uses 10 images, and the arrangement of the image is similar to the arrangement of the keypad numbers in an ATM. In contrast, VIP2 uses 3 x 4 grid cell interfaces to authenticate users. These systems are user friendly and simple. Nevertheless, the recorded photos selected by the users can also be easily shoulder-surfed. Both systems are therefore susceptible to direct shoulder-surfing attack by observation. In VIP version 3[17], users are expected to register eight images during the registration process. Just four of the registered images will be displayed in a 4 x 4 grid cell during the authentication procedure. The rest of the cells on the grid are filled with decoy images. To log in, the uses are required to sequentially click on the registered images. This program will that direct watching surfing attack on the shoulder as the attackers will shoulder-surf the recorded photos clicked by the users each time they login. The main reason this system can reduce shoulder-surfing direct observation attack is because only part of the registered pictures are shown in each challenge set. It will therefore take the attackers time and extra effort to evaluate the right registered images used by the users.

In ColorLogin system [19], Users have to select a color and a set of icons in the enrollment process. Users can use the registered color to help them find their registered icons as background. Users are required to click on the rows which contain the registered icons in a N x N grid cell during the authentication procedure. When clicked; it locks the entire sequence. All of the affected icons are changing to a "lock" icon. The users have to ensure all the registered icons are locked to complete a challenge package. To log in, the users must perform several challenge sets. ColorLogin system can reduce shoulder-surfing attacks by direct observation because the recorded icons are not selected directly during the login process. Even, attackers will shoulder-surf the row that users clicked on. In addition, due to the small password space this system is vulnerable to guessing attacks

The What You See Is What You Join (WYSWYE) device has two variations [21]. Users are expected to register four images in both variations during the enrolment process. During the authentication procedure, users are presented with a 7x4 grid for the first variation, called the Horizontal Reduce Scheme (HRS). Users will identify the columns and mentally delete columns that don't have their photos recorded. The result would be a Nx4 grid with a 4x4 grid as its maximum dimension. The users then have to key for the password in the corresponding position of the registered images in the input grid. The second variation, called the Dual Reduce Scheme (DRS), will feature a 5x5 grid for users. Users must delete a row and a column which does not have their registered photos. The result would be a M x N grid, again a 4x4 grid of the maximum dimension. As with the first variation, users are needed for key in the defined image position in the input grid of the password. WYSWYE-HRS and WYSWYE-DRS will minimize direct-observation shoulder surfing attacks because the captured images are not selected during the authentication process. Attackers can however still shoulder-surf the interest keyed in by the users and map the location of the registered photos.

In a system proposed by Haque [24], registration of username and selection of few images by user formed the enrollment process. After that the users will be given a set of questions. The users need three registered images to pair each question. The users are required to recognize the correct images based on the question being asked in the authentication procedure. This system is user friendly and simple. However, this system cannot prevent direct shoulder-surfing attack as the direct selection of the recorded images can be easily observed and shoulder-surfed during an authentication process.

User has to record six photographs of animals during the registration process in CuedR system [26]. The users are required to key in sequence in the character associated with the registered images during the authentication procedure. This system is vulnerable to direct shoulder-surfing attack, since attackers can decompose the password string and then connect each character in a challenge set with the specific animal image.

Users are required to register a username in Digraph Substitution Rules (DSR) system [3] and register two images in the enrollment process. Users need to click on a pass-image based on the registered images and the three rules of digraph substitution in the authentication procedure. Before they can login the users must complete multiple task sets. This method will prevent direct shoulder-surfing attack from being detected, as users would never click on the captured images.

In WordPassTile [27] method, users are expected to register five Tiles (a specific word) as part of the enrollment procedure. Users should click on the Tiles given in a particular sequence in the authentication procedure. WordPassTile system is vulnerable to direct shoulder-surfing attack, because the direct selection of the tiles during an authentication process is easy to observe and shoulder-surf.

V. COMMON VULNERABILITIES OF RECOGNITION BASED GRAPHICAL PASSWORD

The common attacks which expose the vulnerability of recognition-based graphical password are-

Guessing Attack – An attack which includes guessing or finding a user's [1, 29]. Small password space is exposed to a security challenge in many of the graphical passwords which is based on recognition. Usage of partial registered objects or pass-objects to login can resolve or can be countermeasure for guessing attack.

Shoulder surfing – It is a form of social engineering attack. It includes attacker to peep through someone entering something to gain information or password [3]. Some of the recognition-based graphical password schemes, which use explicitly registered objects, would face such a challenge to security. Indirect objects for example pass-objects may be used to login to resolve or reduce this attack.

Frequency of Occurrence Analysis (FOA) attack – It's a possibility only in recognition based systems that use uniform randomization algorithm to perform selection [22]. Because the sampling size of the registered objects is relatively smaller than the sampling size of the decoy objects, when using a uniform randomization algorithm, the probability that the registered objects will always appear in a challenge set while the same distracting image will appear only occasionally in each challenge set[22]. To overcome or reduce this attack, an authentication system can either use fix objects or prevent the use of large quantities of decoy objects in any set of challenges.

VI. RESULTS AND DISCUSSION

Table1.Recognition-based graphical password and its security threats

Graphical Password Technique	Guess Attack	Shoulder Surfing	FOA
Passfaces	No	No	No
Déjà Vu	No	No	No
Picture Password system	No	No	No
Triangle system	Yes	Yes	N/A
Moving Frame system	No	Yes	N/A
SGC	Yes	Yes	N/A
VIP1	No	No	N/A
VIP2	No	No	N/A
VIP3	yes	Can reduce	No
Color Login	No	Yes	No
WYSWYE-HRS	Yes	Can reduce	N/A
WYSWYE-DRS	Yes	Can reduce	N/A
Haque's system	Yes	No	N/A
CuedR	Yes	No	N/A
DSR	Yes	Yes	Yes
WordPass Tile	Yes	No	Yes

Note-

No- not secure, vulnerable for attack.
Yes- yes secure, cannot attack
N/A- not applicable

Table 1 depicts the comparison of reviewed system. Considering the table, the existing system are exposed to many vulnerabilities such as shoulder surfing and guessing attacks. The systems which use partial objects in login can reduce shoulder surfing attack like VIP3, WYSWYE-HRS and WYSWYE-DRS.Systems that use indirect input or pass-objects to log in instead of registered objects can prevent this attack. Triangle system, Moving Frame system, SGC, ColorLogin and DSR are examples of these systems.

As far as FOA attack is concerned, there are few systems that get affected as these systems used uniform randomization to perform selection. PassfacesTM, Déjà Vu, Picture Password program, VIP3, and ColorLogin, for example. There are few systems that are able to withstand such an attack since they use fixed number of objects to log in through time. Examples of these systems include – DSR and WordPassTile. Other systems are not applicable, since they do not use uniform selection randomization.

VII. CONCLUSION

In this paper, many different security threats were highlighted, such as guessing attack, direct observation and FOA, which were experienced via recognition-based graphical password system. The countermeasures were discussed for each of the security threats. The paper enriched the detailed study that supports the researchers to do the research on graphical password, particularly on graphical password based on recognition. In future, in addition to the security issues, the research will concentrate on the usability aspects such as user login time and methods that may help users to remember their passwords.

REFERENCES

[1] Por L. Y. and Lim X. T.: Issues, threats and future trend for GSP. in Proceedings of The 7th WSEAS International Conference on Applied Computer & Applied Computational Science, Hangzhou, China, 627–633 (2008).

[2] Ho, P. F., Kam, Y. H. S., Wee, M. C., Chong, Y. N., Por, L. Y.: Preventing Shoulder-Surfing Attack with the Concept of Concealing the Password Objects' Information. The Scientific World Journal, (2014)

[3] Por, L.Y., Ku, C.S., Islam, A., Ang, T.F.: Graphical password: Prevent shouldersurfing at-tack using digraph substitution rules. The Frontiers of Computer Science,Accepted (2016).

[4] Blonder, G. E.: ``Graphical Passwords", United States Patent 5559961, Lucent Technologies, Inc. (Murray Hill, NJ), (1996).

[5] Devaraj Verma C., and Naveen K R.,: Secure Data Protection in Insecure Networks using One Time Password based Encryption, published in International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 4 Issue 06, June-2015, Pg No: 541 – 544, IF = 1.76. http://dx.doi.org/10.17577/IJERTV4IS060406

[6] Biddle, R., Chiasson, S., Van Oorschot, P. C.: Graphical passwords: Learning from the first twelve years. ACM Computing Surveys (CSUR), 44(4), 19 (2012)

[7] Por, L. Y., Wong, K., Chee, K. O. :UniSpaCh: a text-based data hiding method using Unicode space characters. Journal of Systems and Software, 85(5), 1075–1082 (2012)

[8] Por, L. Y., Delina, B.:Information hiding a new approach in text steganography. In Proceedings of the 7th WSEAS International Conference on Applied Computerand Applied Computational Science, 2008, 689–695.

[9]Por, L. Y., Delina, B., Ang, T. F., Ong, S. Y.: An enchanced mechanism for image steganog-raphy using sequential colour cycle algorithm. The International
Arab Journal of Information Technology, 10(1), 51–60 (2013)

[10]Por L. Y., Lai W. K., Alireza Z., Delina B.: StegCure: an amalgamation of different steganographic methods in GIF image. In Proceedings of the 12th WSEASInternational Conference on Computers, Heraklion, Greece, 420–425 (2008)

[11] De-Angeli, A., Coventry, L., Johnson, G., and Renaud, K.: Is a picture really worth a thou-sand words? Exploring the feasibility of graphical authentication systems. International Journal of Human-Computer Studies, 63, 128-152 (2005)

[12]PassfacesTM: The Science behind Passfaces, White paper. http://www.passfaces.com/enterprise/resources/white_papers.htm. Accessed 10 July 2017 (2000)

[13] Brostoff, S., Sasse, M. A.: Are Passfaces more usable than passwords: a field trial investigation. In People and Computers XIV—Usability or Else! , 405-424: Springer London (2000)

[14] Jansen, W., Gavrila, S., Korolev, V., Ayers, R., Swanstrom, R.: Picture password A visual login technique for mobile devices. (2003)

[15] Davis, D., Monrose, F., Reiter, M. K.: On user choice in graphical password schemes. In USENIX Security Symposium, 13, 1-14 (2004)

[16] Zhao, H., Li, X.: S3PAS: A Scalable Shoulder-Surfing Resistant Textual- Graphical Password Authentication Scheme. Proceedings of the International Conference on Advanced In-formation Networking and Applications Workshops, 2, 467-472 (2007)

[17] De-Angeli A., Coutts M., Coventry L., Johnson G.: VIP: A Visual Approach to User Authentication. Proceedings of the Working Conference on Advance VisualInterfaces, 316-323 (2002)

[18] Hayashi, E., Dhamija, R., Christin, N., Perrig, A.: Use Your Illusion: secure authentication usable anywhere. Proceedings of the 4th Symposium on Usable Privacyand Security, 35-45 (2008)

[19]Gao, H., Liu, X., Wang, S., Liu, H., Dai, R.: Design and Analysis of a Graphical Pass-word Scheme. The 4th International Conference on Innovative Computing,Information and Control, 675-678 (2009)

[20]Khot, R. A., Kumaraguru, P., Srinathan, K.: WYSWYE: shoulder surfing defense for recognition based graphical passwords. Paper presented at the Proceedings ofthe 24th Australian Computer-Human Interaction Conference, Melbourne, Australia (2012).

[21]Perkovic, T., Cagalj, M., Rakic, N.: SSSL: Shoulder Surfing Safe Login. 17th International Conference on Software, Telecommunications & Computer Networks,2009.SoftCOM (2009)

[22]Por, L.Y.: Frequency of occurrence analysis attack and its countermeasure. The International Arab Journal of Information Technology, 10(2), 189-197 (2013)

[23]Manjunath, G., Satheesh, K., Saranyadevi, C., Nithya, M.: Text-based shouldersurfing resistant graphical password scheme. International Journal of ComputerScience and Information Technologies, 5(2), 2277-2280 (2014)

[24]Haque, M.A., Imam, B.: A New Graphical Password: Combination of Recall & Recognition Based Approach. World Academy of Science, Engineering andTechnology, International Journal of Computer, Electrical, Automation, Control and Information Engineering, 8(2), 320-324 (2014)

[25]Pooja K. S., Prajna V. D., Prathvi, Ashwini N.: Shoulder Surfing Resistance UsingGraphical Password Authentication in ATM Systems. International Journal of Information Technology & Management Information System (IJITMIS), 6(1), 1-10 (2015)

[26] Al-Ameen M. N., Wright M., and Scielzo S.: Towards making random passwords mem-orable: leveraging users' cognitive ability through multiple cues. CHI `15Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, pp.2315-2324 (2015)

[27]Assal, H., Imran, A., Chiasson, S.: An Exploration of Graphical Password Authentication for Children. https://arxiv.org/abs/1610.09743. Accessed Date: 16June 2017 (2016)

[28] Agrawal, S., Ansari, A. Z., Umar, M. S.: Multimedia graphical grid based text password authentication: For advanced users, 2016 Thirteenth International Conferenceon Wireless and Optical Communications Networks (WOCN), 1-5 (2016)

[29] Por L. Y., Kiah M. L. M.: Shoulder surfing resistance using penup event and neighbouring connectivity manipulation. Malaysian Journal of Computer Science, 23(2), 121–140 (2010)