A Symbol Based Graphical Schema Resistant to Peeping Attack

T.Srinivasa Ravi Kiran[1], Dr.K.V.Samabasiva Rao[2], Dr.M.Kameswara Rao[3],A.Srisaila[4]

[1] Lecturer, Department of Computer Science
P.G.Centre, P.B.Siddhartha College of Arts & Science,
Vijayawada, Andhra Pradesh, 520010, India

[2] Principal, M.V.R College of Engineering, Paritala, 521180, Andhra Pradesh, India

[3] Associate Professor, Department Of Electronics and Computer Engineering, KL Univeristy,Vaddeswaram, 520 002,India

[4] Assistant Professor, Department of Information Technology, V.R.Siddhartha Engineering College,Kanur,Vijayawada,520006Andhra Pradesh,India

Abstract

Alphanumeric passwords are the most commonly used way of authenticating users in computer systems. One of the disadvantages of alphanumeric passwords is that they are hard to remember. Image passwords have been proposed to aim to make passwords more memorable and easier for users to use and, for this reason, it is more secure. Furthermore, most of the existing graphical password schemes are susceptible to spyware and shoulder surfing. This paper proposes a new graphical password authentication scheme resistant to peeping attack. In this schema We also try to answer two important questions: "Are graphical passwords as secure as text-based passwords?"; "What are the major design and implementation issues for graphical passwords?". This survey will be useful for information security researchers and practitioners who are interested in finding an alternative to text-based authentication. methods. An analysis of security and usability aspects of the proposed scheme is presented.

Keywords: Graphical password; Authentication, Peeping attack, Security, Spyware

I. INTRODUCTION

Traditionally, alphanumeric passwords have been used for authentication, but they are known to have security and usability problems. The main problem with the alphanumeric passwords is that once a password has been chosen and learned the user must be able to recall it to log in. But, people regularly forget their passwords. If a password is not frequently used it will be even more susceptible to forgetting. To resist bruteforce search and dictionary attacks, users are required to use long and random passwords. Unfortunately, such passwords are hard to remember[1]. Furthermore, textual password is vulnerable to shoulder-surfing, hidden-camera and spyware attacks. Graphical password schemes have been proposed as a possible alternative to text-based schemes, motivated partially by the fact that humans can remember pictures better than text [2]. If the number of possible pictures is sufficiently large, the possible password space of a graphical password scheme may exceed that of text based schemes and thus presumably offer better resistance to dictionary attacks. Because of these advantages, there is a growing interest in graphical password. In addition, the possible password space of a graphical password scheme may exceed that of text based schemes and thus most probably offer higher level of security. It is also difficult to devise automated attacks for graphical passwords. As a result, graphical password schemes provide a way of making more human-friendly passwords while increasing the level of security. Due to these advantages, there is a growing interest in graphical password. However, existing graphical passwords are far from perfect. Typically, system requirements and cost of communication for graphical passwords are significantly higher than text-based passwords. In addition, few graphical systems support keyboard inputs. More importantly, most current graphical passwords are more vulnerable to shoulder-surfing attacks than textual passwords. In this paper we propose a textual graphical password system resistant to peeping attack. User study is conducted to explore the usability of the

proposed scheme in terms of accuracy, efficiency and memorize ability. The rest of this paper is organized as follows. Section 2 briefly discusses related works on Graphical password schemes. Section 3 presents our proposed scheme. Section 4 examines usability issues and Section 5 deals with conclusion and future directions.

II. Related Work

In general, the graphical password techniques can be classified into in to three main categories: Locimetric, Drawmetric and Cognometric [6]. Locimetric authentication is an approach that exploits memorization and cued recall. This approach requires the user to use a background image to locate a series of predefined points. In 1996, Blonder [7] patented an innovative graphical authentication scheme called Graphical Password which is based on cued recall. In his design, the system first picks an image with many simple distinguishable locations, and these locations are stored on the system database. Wiedenbeck et al. [8] proposed and implemented an improved graphical authentication system called PassPoints.PassPoints is based on Blonder's idea of representing the password by multiple clicks on a single image. Drawmetric authentication is an approach that requires the user to draw a simple outline of the password during registration, and the user must redraw the similar drawing to be authenticated. Jermyn et al. [9] proposed and implemented a graphical authentication technique called Draw-a-Secret (DAS), which is primarily intended for devices with stylus input, such as Personal DigitalAssistants (PDAs). The main idea of DAS is that the user draws secret drawing (password) on a grid and the system verifies the drawing by checking the directions and the positions of the drawn strokes on the grid. Cognometric authentication is an approach that requires the user to identify a series of recognized images amongst a larger set of decoy images. Real User Corporation [10] developed a graphical authentication technique called Passfaces. The motivation behind Passfaces is based on humans' proficient ability to recognize human faces. Dhamija [11] has mentioned a major problem in authentication that users tend to have difficulties memorizing secure passwords.To overcome such problem, Dhamija et al. [12] suggested a solution called Déjà Vu, which improves the security of the system by replacing the precise recall of a text password with the recognition of seen images. Graphical authentication suffers a major drawback from Shouldersurfing. Shoulder-surfing refers to someone observing the user's action as the user enters a password. With graphical authentication, the user must select the recognized pictures from the displayed screen during login. Due to this, the user's action can be monitored by the attacker or it can be captured using recording devices such as camera. Wiedenbeck et al. [13] suggested a graphical password scheme for user authentication on computer called Convex Hull Click (CHC); and it was design to prevent shoulder surfing. Pierce et al. [14,15] proposed a technique that improves password security without additional hardware. Their technique exploits the ability of people being proficient to recognize visual information. Their proposed graphical authentication is called Authentigraph. The system first presents an image of randomly allocated artifacts on screen. Users are required to locate and select the recognized artifacts in sequence as their graphical password. De Angeli et al. [16,17] proposed a graphical authentication concept called Visual Identification Protocol (VIP) that aimed at improving user authentication in self-service technology. The notion of VIP is to replace the precise recalling of numerical code with the recognition of previously seen images for authentication. De Angeli et al. have suggested three prototypes of VIP, named VIP1, VIP2, and VIP3. Jansen et al. [18-20] proposed a visual login technique called Picture Password, which is designed for mobile devices with stylus input such as Personal Digital Assistants (PDAs).Hinds el al. [21] proposed a graphical password system called ToonPasswords. It requires users to select individual images from screens, which is similar to Passfaces [22] and Déjà Vu [23]. However, most of the current graphical password schemes do not have a balance between usability and security aspects. For example, if the system is too simple then the system may not be secure enough. If the algorithm is too complex then the system may not be user friendly, e.g.: difficult to learn and takes too long to log in.

III. Proposed Scheme

In this proposed scheme we use 5 x 5 grid formed using 25 blocks. Each block consists of a symbol. The symbol contains a set of four characters. The characters may numbers between 0 to 9, A to Z(Uppercase), a to z (Lowercase), Spaces and some special characters totally 95 character and 5 blank spaces are represented as shown in the Fig1. Passwords are input by typing or by mouse clicks.

Rules to write straight line on the interface

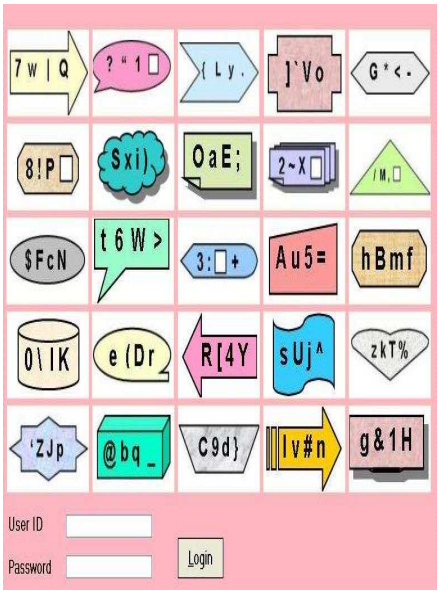

Fig 1 Proposed Schema

Rule 1: If user draws a line between two adjacent blocks, the password contains at least one character from each set of four characters depicted on the symbol of each block.

E.g. User draws a line between the top leftmost two blocks (row 1, column 1 and row 2, column 2), then the user would click on at least one character from each of the two sets [7,w,|,Q] and [8,!,P,blank-space] depicted on the blocks.

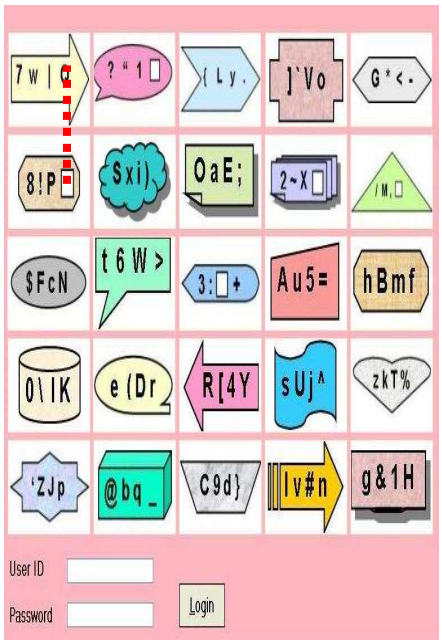

Fig 2 Line between adjacent blocks

Rule2: If user draws a line between two non-adjacent blocks, the character sets to be considered are taken from the symbol of the individual blocks in between if the line touches the symbol of the block. Then the password contains at least one character from each set of four characters depicted on the symbol of each block.

E.g. User draws a line between the two blocks row 2, column 4 and row 4, column 1, the drawn line touches only the symbols of three blocks (row 2, column 4 and row 3, column 3 and row 4, column 1) Then the password comprises of at least one character from each of the three sets [2, ~, X,blank-space] and [3,;,blank-space,+] and [0,\,|,K] depicted on the blocks.

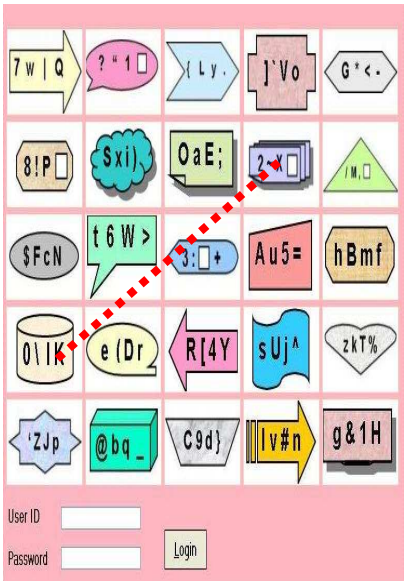

Fig 3 Line between non-adjacent blocks

Rule 3: If user draws a line on a single block, then the password contains at least one character on which the line passes.

E.g. If we draw a line on the characters ‘t ‘, ‘6 ‘,’ w ‘ of block at row 3, column 2 then the password contains at least one character from the set [t,6,w].

Fig 4 Line on a single block

Rule 4: If the user draws the line on a single character of the symbol on a block then the password contains only that character.

E.g. If we draw a line on the character C of block at row 5, column 3 then the password is that character.

Fig 5 Line on single character of the symbol

IV. USABILITY STUDY &SECURITY ANALYSIS

We conducted a lab study with 23 participants out of which 15 were male and 8 were female. All the participants were post graduate students with their ages ranging from 22 to 26 years. A learning phase was conducted for practicing proposed graphical password scheme. They are given training initially explaining the concept of how to identify their password based on the rules proposed through the interface .The result was encouraging that novice users were able to identify the quadruplets formed with their password accurately. It took about 42 seconds on average to log in. Peeping attack is the attack where an attacker gets the secret information through direct observation when the user is entering his or her password. Alphanumeric systems are susceptible to peeping attack. In these attacks, typically the attacker gets a chance to observe the password entry for a short duration of time. As alphanumeric passwords are typically small, the attacker may see the secret by looking just for a while. On the other hand, peeping attack is not feasible against our proposed scheme as the user types or clicks on non password characters

V. CONCLUSION

Text-based authentication schemes are inherently insecure as they are subject to a tradeoff between usability and security, however they remain popular as their concept corresponds to an existing common model worldview making them an easy to understand concept. Graphical password has been designed to overcome the text-based password problems. Graphical passwords are more memorable compared to text-based passwords. In this paper, we proposed a new graphical password system resistant to peeping attack with promising usability features. The scheme provides a potential solution for the current problems faced by the other graphical password schemes. The proposed scheme provides larger password space than traditional text based passwords. This work can be extended by increasing the password space using more than three color character sets based upon user choice. The extension of the proposed schemes to hand-held mobile devices can be explored as future work.

REFERENCES

[1] 1. Abdullah et al (2008), Graphical Passwords: *Users' Affinity of Choice, AnAnalysis of Picture Attributes Selection*,IEEE 2008.

[2] R. N. Shepard. Recognition memory for words, sentences and pictures. *Journal of Verbal Learning and Verbal Behavior*, 6:156–163, 1967.

[3] R. U. Corporation. How the passface system works, 2005.

[4] D. Hong, S. Man, B. Hawes, and M. Mathews. A password scheme strongly resistant to spyware. In *in Proceedings ofInternational conference on security and management*, LasVergas, NV, 2002.

[5] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin. in proceedings of the design and analysis of graphicalpasswords. In *the 8th USENIX Security Symposium*, 1999.

[6] Renaud, K and De Angeli, A.My password is here! An investigation into visuo-spatial authentication mechanisms. 2004, Interacting with Computers, Vol. 16, pp. 1017-1041.

[7] Blonder, G E. Graphical Password. 5559961 United States, 1996.

[8] Wiedenbeck, S, et al. Authentication using graphical passwords:effect of tolerance and image choice. Pittsburgh, PA : ACM Press,2005. Proceedings of the 2005 symposium on Usable privacy and security (SOUPS). pp. 1-12.

[9] Jermyn, I, et al The Design and Analysis of Graphical Passwords.. Washington, D.C. USENIX Association, 1999. Proceedings of the 8th USENIX Security Symposium. pp. 1-14.

[10] Passfaces. [Online] Passfaces Coporation. [Cited: November 7, 2007.] http://www.passfaces.com.

[11] Dhamija, R., Hash visualization in user authentication The Hague,Netherlands : ACM Press, 2000. Conference on Human Factors in Computing System (CHI '00). pp. 279-280.

[12] Dhamija, R and Perrig, A. Déjà Vu: A user study using images for authentication. Denver, CO : USENIX Association, 2000. Proceedings of the 9th Conference on USENIX Security Symposium.

[13] Wiedenbeck, S, et al PassPoints: Design and longitudinal evaluation of a graphical password system.. 2005, 2005, International Journal of Human-Computer Studies, Vol. 63, pp. 102-127.

[14] Pierce, J D, et al Graphical Authentication: Justifications andObjectives Perth : Edith Cowan University, Western Australia, 2004. Proceedings of the 2nd Australian Information Security Management Conference. pp. 49-55.

[15] Pierce, J D, et al A conceptual model for graphical authentication Perth, Western Australia : Edith Cowan University, Western Australia, 2003. Proceedings of the 1st Australian Information Security Management Conference.

[16] De Angeli, A, et al Usability and user authentication: Pictorial passwords vs. PIN.. [ed.] P T McCabe. London : Taylor & Francis, 2003. Contemporary Ergonomics 2003. pp. 253-258.

[17] De Angeli, A, et al Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems. 1-2, 2005, International Journal of Human-Computer Studies, Vol. 63, pp. 128-152.

[18] Jansen, W, et al. Picture password: a visual login technique for mobile devices. Department of Commerce, National Institute of Standard and Technology. Gaithersburg, MD : NISTIR, 2003.

[19] Jansen, W. [ed.] K Morgn and J M Spector ,"Authenticating mobile device users through image selection" 2004, In The Internet Society.[20] Authenticating Users on Handheld Devices. Jansen, W. 2003.Proceedings of the Canadian Information Technology Security Symposium.

[20] Hinds, C and Ekwueme, C. Winston-Salem, Increasing security and usability of computer systems with graphical passwords. NC : ACM Press, 2007. Proceedings of the 45th Annual Southeast Regional Conference. pp. 529-530.

[21] M. Shahid and M.A. Qadeer. Novel scheme for securing passwords. In Digital Ecosys-tems and Technologies, 2009. DEST'09. 3rd IEEE International Conference on, pages 223{227. IEEE, 2009.

[22] R. Jhawar, P. Inglesant, N. Courtois, and M.A. Sasse. Make mine a quadruple: Strengthening the security of graphical one-time pin authentication. In Network and System Security (NSS), 2011 5th International Conference on, pages 81{88. IEEE, 2011.

[23] Dictionary.com. Password | at dictionary.com, 2012. [Online; accessed 03-March-2012].