ISSN:0975-9646

T.Srinivasa Ravi Kiran et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (5) , 2012,5051-5054

A Novel Graphical Password Scheme Resistant To Peeping Attack

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

[1,3]*Lecturer, Department of Computer Science*
P.G.Centre, P.B.Siddhartha College of Arts & Science,
Vijayawada, Andhra Pradesh ,India

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

Abstract **- The conventional text-based password authentication scheme faces some drawbacks with usability and security issues that bring troubles to users. Graphical password schemes act as a possible alternative to text-based schemes which are proposed mainly by the fact that humans can remember pictures better than text. Beside that, the possible password space of a graphical password scheme may exceed that of text based schemes and thus presumably offer better resistance to brute force search and dictionary attacks. However, graphical password is vulnerable to peeping attack. This paper proposes a new graphical password authentication scheme resistant to peeping attack. An analysis of security and usability aspects of the proposed scheme is presented.**

Keywords **- Graphical password; Authentication, Peeping attack, Security**

I. INTRODUCTION

A key area in security research is authentication, the determination of whether a user should be allowed to access to a given system or resource. Traditionally, alphanumeric passwords have been used for authentication, but they are known to have security and usability problems. Today other methods, including graphical passwords, are possible alternatives [1], [2]. Graphical password has a lot of benefits when compared to alphanumeric passwords. It is more safe and easy to remember. In addition it is also resistant towards most of the attacks. A number of graphical authentication systems have emerged and survey on existing graphical password techniques illustrates that it is more difficult to break graphical passwords using the traditional attack methods such as brute force search, dictionary attack [3], [4]. However, it is important to have a graphical password scheme which is resistant to peeping attack where a third party can observe and record the legitimate user's password by peeping over the victim's shoulder [5].

To overcome this issue, an anti-peeping mechanism has to be integrated into the said graphical 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 memorisation 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 Digital Assistants (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 Shoulder-surfing. Shoulder-surfing refers to someone observing the user's action as the user enters a password. With graphical authentication, the user must select the recognised 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 artefacts on screen. Users are required to locate and select the recognized artefacts 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 the proposed scheme, we use a 10x10 grid formed using the single color 94 printable character set added with spaces as shown in Fig 1. Passwords are input by typing or by mouse clicks.

Fig 1 Proposed Schema

The proposed scheme starts with identifying quadruplets formed from the user password starting with the first character and sliding to the right one character at a time wrapping around if necessary until the last character in the password appears as the first character in a quadruplet. For example, if the password selected at registration time is “T2D8h” then the quadruplets formed are “T2D8”,”2D8h”,”D8hT”,”8hT2” and “hT2D”.

Rule1: If the four characters in the quadruplet are different and form a quadrilateral in any order then the characters inside the quadrilateral can be typed in or alternatively the user would click on any of the cells inside the quadrilateral.

Rule 2: If the four characters of the quadruplet are equal (ex: QQQQ) then any character that surrounds the character (Q) of the quadruplet can be typed in or alternatively the user would click on any of the cells surrounding it.

Rule 3: If in the four characters on the quadruplet three characters are equal and one character is different (ex:AuAA) then user can type or click any of the characters that lie on the line formed between the quadruplet characters (‘A’ and ‘u’).

Rule 4: If in the four characters on the quadruplet two characters are equal and the other two characters are different (ex: 7B7U) then the user can type or click the cells that lie inside the triangle formed by quadruplet characters. If the quadruplet characters form a straight line (ex: THT3) then the user can click on any of the cells that lie on the line formed between the quadruplet characters.

Rule 5: If in the four characters on the quadruplet two characters are equal and other two characters are also equal to one another (ex:8M8M) then user can type or click any of the characters that lie on the line formed between the quadruplet characters

A. Illustration

To illustrate the login process, let us follow an example where the user ‘A’ original password is "T2D8h". The quadruplets formed with this password are “T2D8”,”2D8h”,”D8hT”,”8hT2” and “hT2D”.

The login procedure consists of the following steps and is also shown below.

1) *Step 1*: User ‘A’ identifies his characters in the quadruplet “T2D8" and then clicks on any of the cells that lies within the quadrilateral formed by the quadruplet characters in any order.

Fig 2 represents the clickable area for quadruplet “T2D8"

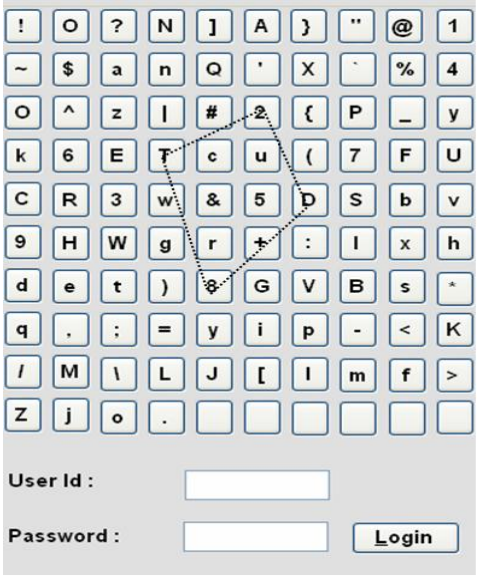

Fig2. Clickable area of quadruplet T2D8

2) *Step 2:* User 'A' identifies his characters in the quadruplet "2D8h" and then clicks on any of the cells that lies within the quadrilateral formed by the quadruplet characters in any order.

Fig 3 represents the clickable area for quadruplet "2D8h"

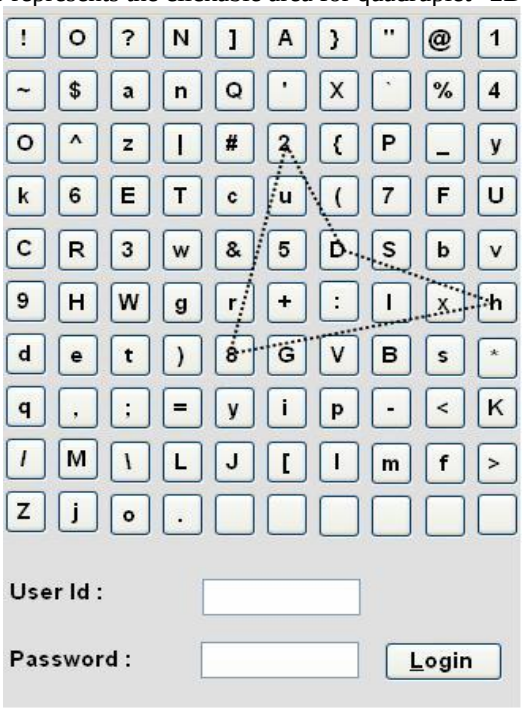

Fig3. Clickable area of quadruplet 2D8h

3) *Step 3:* User 'A' identifies his characters in the quadruplet "D8hT" and then clicks on any of the cells that lies within the quadrilateral formed by the quadruplet characters in any order.

Fig 4 represents the clickable area for quadruplet "D8hT"

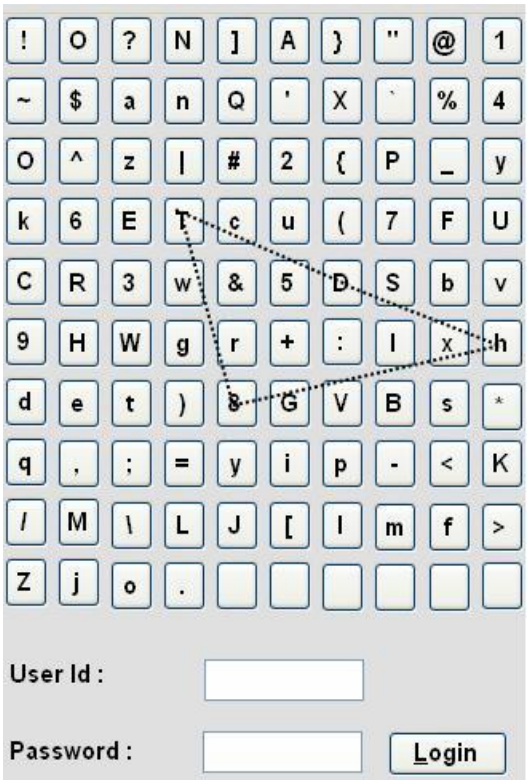

Fig 4. Clickable area of quadruplet D8hT

4) *Step 4:* User 'A' identifies his characters in the quadruplet "8hT2" and then clicks on any of the cells that lies within the quadrilateral formed by the quadruplet characters in any order.

Fig 5 represents the clickable area for quadruplet "8hT2"

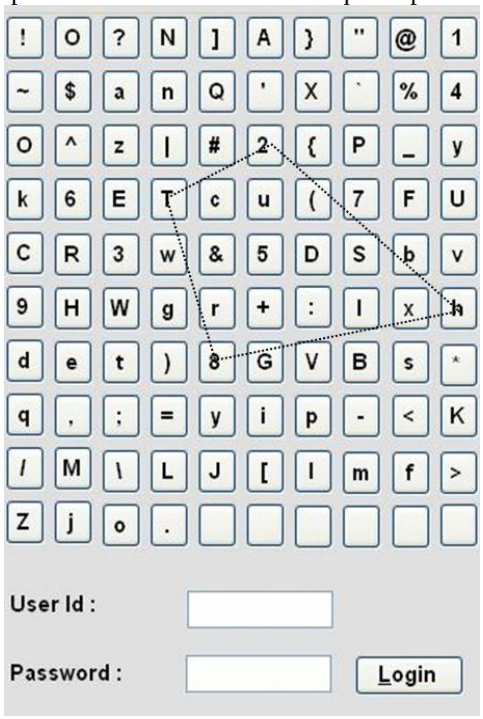

Fig 5. Clickable area of quadruplet 8hT2

5) *Step 5:* User 'A' identifies his characters in the quadruplet "hT2D" and then clicks on any of the cells that lies within the quadrilateral formed by the quadruplet characters in any order.

Fig 6 represents the clickable area for quadruplet "hT2D"

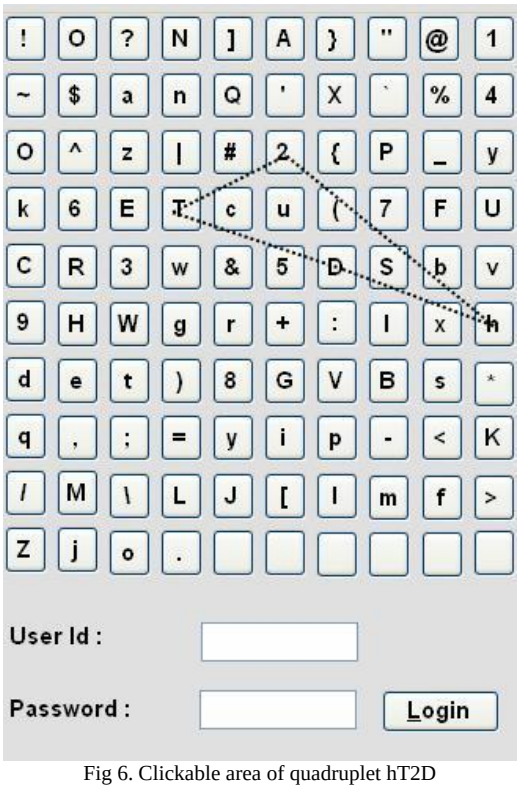

Fig 6. Clickable area of quadruplet hT2D

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

The password problem has made it clear that there are problems with the usability and security of traditional text-based passwords. These problems exist due to the limitation of human's Long Term Memory. Throughout the last decade, several alternative mechanisms have been developed. However, due to the cost of hardware, security and usability reasons, traditional text-based password remain dominant. 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] Standing, L.P., "Learning 10,000 pictures. Quarterly" Journal of Experimental Psychology vol. 25, pp. 207–222, 1973.

[2] Paivio, A., Rogers, T.B., Smythe, P.C., Why are pictures easier to recall then words? Psychonomic Science 11 (4),137–138, 1968.

[3] S. Madigan. Picture memory. In Imagery, Memory, and Cognition, pages 65–86, Lawrence Erlbaum Associates,1983.

[4] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords:Basic results," in Human-Computer Interaction International (HCII 2005). Las Vegas, NV, 2005.

[5] X. Suo, Y. Zhu, and G. S. Owen, "Graphical pass-words: A survey," 21st Annual Computer Security Applications Conference (ACSAC), pp. 463–472,Dec. 5-9, 2005.

[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 authenticationThe 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 and Objectives 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.

[21] 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.

[22] 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.

[23] 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.

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