ISSN: 2321-7782 (Online)

Volume 2, Issue 11, November 2014

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

A Safe and Powerful Technique for Visual Based (Secret Word) Password Confirmation

J.Kanagaraj[1]
M.Phil Research Scholar
Department of Computer Science
Kovai Kalaimagal College of Arts and Science
Coimbatore, India

K.Noel Binny[2]
Assistant Professor and Head of the Department
Department of Computer Applications
Kovai Kalaimagal College of Arts and Science
Coimbatore, India

Abstract: This Paper Shows a Co-ordinated assessment of the Persuasive Cued click-Points graphical secret code method, including simplicity of use and security assessments, and execution reviews. An imperative convenience objective for learning based confirmation frameworks is to help clients in selecting secret codes of higher security, in the feeling of being from a stretched compelling security space, We utilize influence to impact client decision in click based graphical secret codes, urging clients to choose more arbitrary, and consequently more hard to figure, click-focuses.

Keywords: Verification, graphical secret codes, guessing attacks, computer security.

I. INTRODUCTION

There has been a great deal of hype for graphical secret codes since two decade due to the fact that primitive's methods suffered from an innumerable number of attacks which could be forced easily. Here we will improve down the taxonomy of confirmation methods.

To start with we focus on the most common computer verification method that makes use of text secret codes. Despite the vulnerabilities, it's the user natural tendency of the users that they will always prefer to go for short secret codes for ease of remembrance [10] and also lack of awareness about how attackers tend to attacks. Unfortunately, these secret codes are broken mercilessly by intruders by several simple means such as concealed, Eaves dropping and the other offensive means say the dictionary attack, shoulder surfing attack, social engineering attack[10][1].

To mitigate the problems with the traditional methods, advanced methods have been proposed using a graphical as secret codes. The idea of graphical secret codes first described by Greg Blonder (1996). For Blonder, graphical secret codes have a predetermined image that the sequence and the tap regions selected are interpreted as the graphical secret code. Since then, many other graphical secret code schemes have been projected. The pleasing quality related with graphical secret codes is that psychologically humans can remember graphical far better than text and hence is the best alternative being proposed. There is a fast and increasing interest in graphical secret codes for they are more or infinite in numbers thus providing more resistance.

The main objective of this work is to reduce the guessing attacks as well as encouraging users to select more random, and difficult secret codes to guess.

II. TAXONOMY OF VERIFICATION

The following Figure.1 is the representation of current verification methods Biometric based verification systems techniques are proved to be costly, deliberate and unpredictable and hence not preferred by many. Token based verification system is high security and usability and convenience evaluate then others. But this organization employ knowledge based techniques to enhance security. But the current knowledge based techniques are still immature. For instance, ATM cards always go hand in hand with PIN number. So the knowledge based techniques are the most wanted techniques to improve real high security. Recognition & recalls based are the two names by which graphical techniques could be classified based.

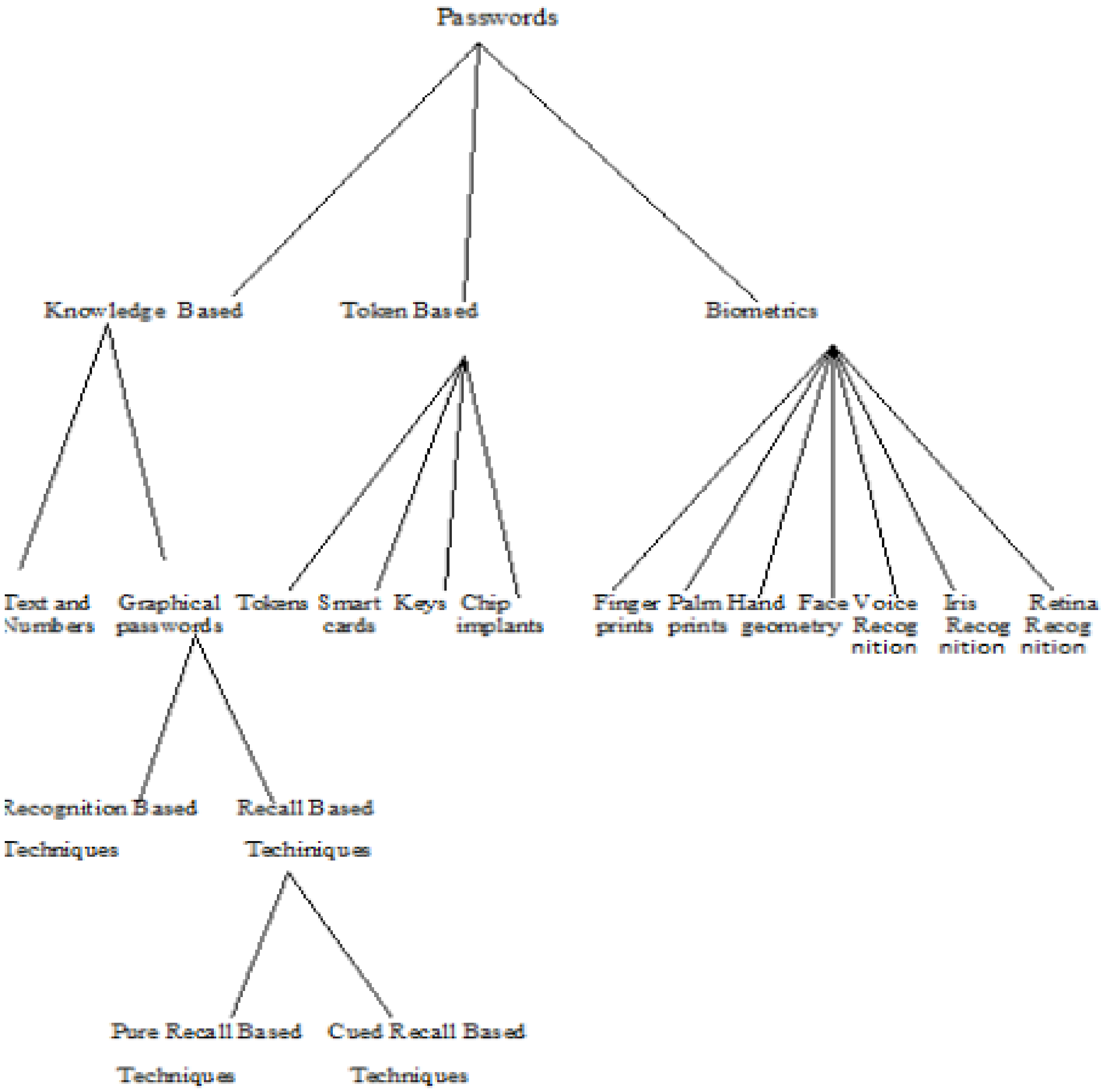


Figure 1: Taxonomy of Secret code Verification Techniques

III. Background on Graphical Secret Code Systems

Graphical secret codes were first described by Blonder. Since then, many other graphical secret code schemes have been proposed. Graphical secret code systems can be classified as either recognition-based (image based scheme, cued recall-based (image based scheme) or pure recall-based (grid based scheme).

A. *Recognition Based Techniques*

1. Dhamija and Perrig

Dhamija and Perrig [4] proposed a graphical verification scheme based on the Hash Visualization technique. In their system Figure. 2 the user is asked to select a certain number of images from a set of random pictures generated by a program later the user will be required to identify the pre selected images in order to be authenticated. A weakness of this system is that the server needs to store the seeds of the portfolio images of each user in plain text. Also, the process of selecting a set of pictures from the picture database can be tedious and time consuming for the user.

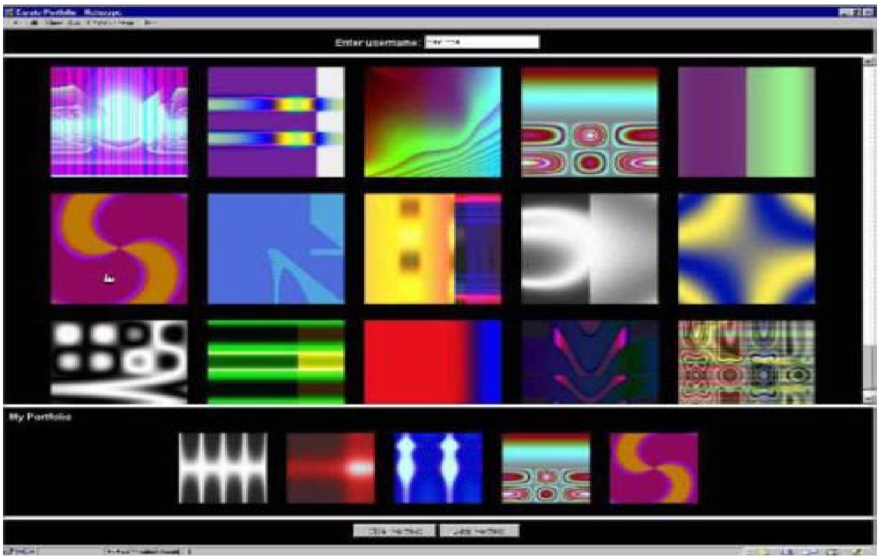


Figure 2: Random images used by Dhamija and Perrig

Akula and Devisetty’s algorithm [5] is similar to the technique proposed by Dhamija and Perrig .the images will be converted into hashing code using SHA-1 techniques to give more secure and less memory. In this Technique produces a 20 byte output. Both the above algorithms are prone to shoulder surfing attacks.

2. Hong’s Methods

Hong, et al. [7] proposed another shoulder-surfing resistant algorithm. In this approach to allow the user to assign their own codes to pass-object variants. Figure. 3 shows the log-in screen of this graphical secret code scheme. However, this method still forces the user to memorize many text strings and therefore suffer from the many drawbacks of text-based secret codes.

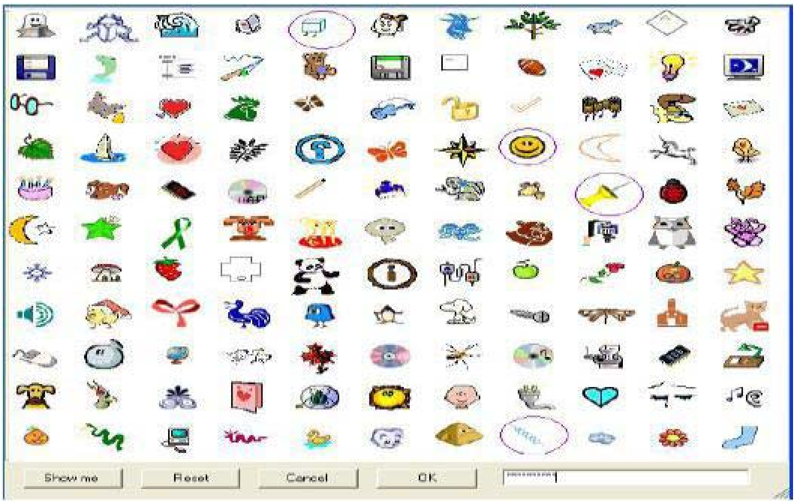


Figure 3: Hong’s al ’s Shoulder surfing resistant

B. Recall based technique

In this section we discuss recent there types of click based graphical secret code techniques:

1. Pass Points (PP)

2. Cued Click Points (CCP)

3. Persuasive Cued Click- Points (PCCP)

1. Pass point (PP)

Based on Blonder's original idea [7], Pass Points (PP) [7] is a click-based graphical secret code system where a secret code consists of an ordered sequence of five click-points 4 on a pixel-based image as shown inFigure.4

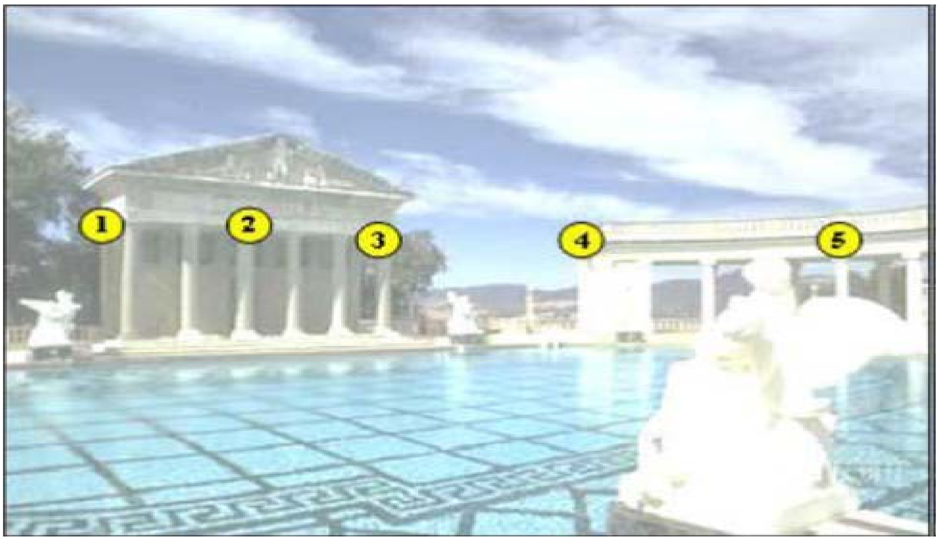


Figure: 4 Pass Points

To log in, a user must click within some system-defined tolerance region for each click-point. The image acts as a cue to help users remember their secret code click-points.

2. Cued Click Points (CCP)

CCP [1] was developed as an alternative click based graphical secret code scheme where users select one point per image for five images Figure.5: The interface displays only one image at a time; the image is replaced by the next image as soon as a user selects a click point. The system determines the next image to display based on the user's click-point on the current image. The next image displayed to users is based on a deterministic function of the point which is currently selected. It now presents a one to-one cued recall scenario where each image triggers the user's memory of the one click-point on that image. Secondly, if a user enters an incorrect click-point during login, the next image displayed will also be incorrect. Legitimate users who see an unrecognized image know that they made an error with their previous click-point. Conversely, this implicit feedback is not helpful to an attacker who does not know the expected sequence of images.

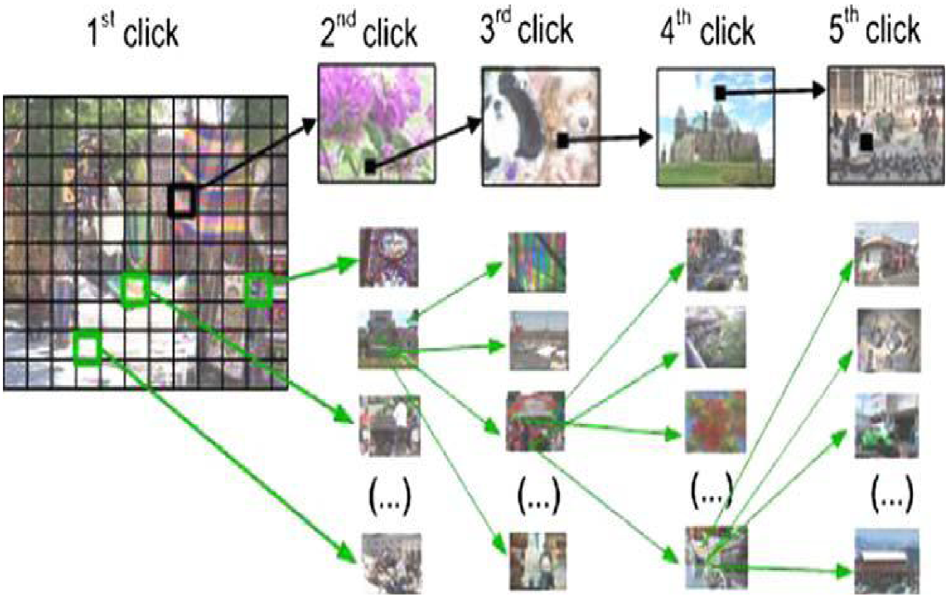
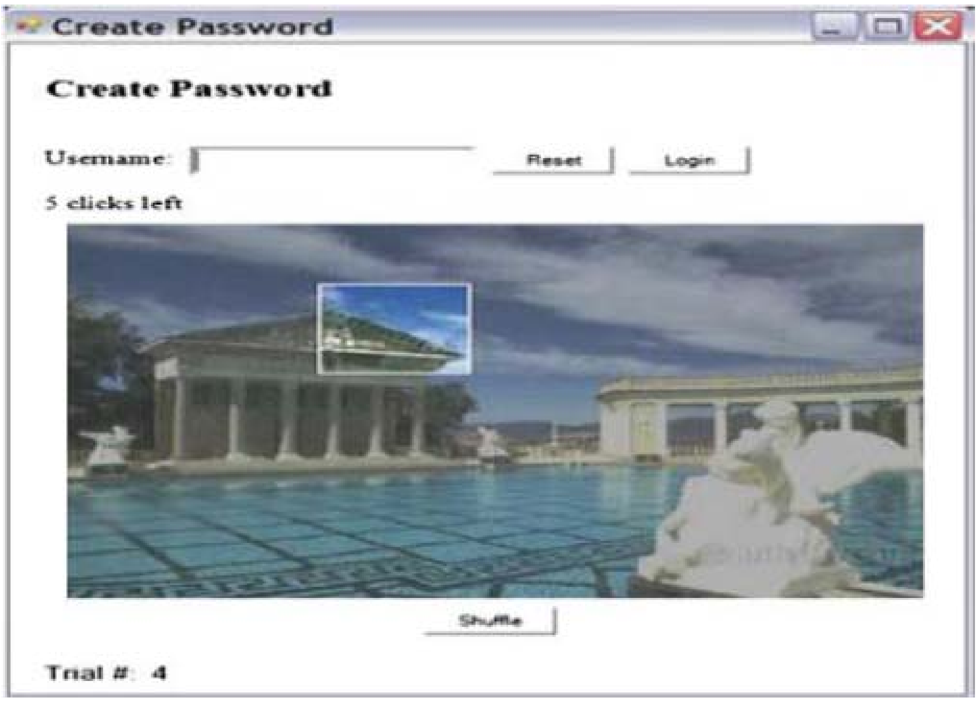


Figure 5: Cued Click point.

3. Persuasive Cued Click- Points (PCCP)

To address the issue of hotspots, PCCP was proposed [7]. As with CCP, a secret code consists of five click points, one on each of five images. During secret code creation, most of the image is dimmed except for a small view port area that is randomly positioned on the image as shown in Figure.6. Users must select a click-point within the view port. If they are unable or unwilling to select a point in the current view port, they may press the Shuffle button to randomly reposition the view port. The view port guides users to select more random secret codes that are less likely to include hotspots. A user who is determined to reach a certain click-point may still shuffle until the view port moves to the specific location, but this is a time consuming and more tedious process.



5 clicks left

Trial #: 4

Figure 6: the PCCP secret code creation interface

IV. Discussion

"Will Graphical secret codes circumvent Text based secret codes?" Here we briefly exam some of the possible techniques for breaking graphical secret codes and try to do a comparison with text-based secret codes.

A. Dictionary Attacks

Since recognition based graphical secret codes involve mouse input instead of keyboard input, it will be impractical to carry out dictionary attacks against this type of graphical secret codes. For some recall based graphical secret codes [11], it is possible to use a dictionary attack but an automated dictionary attack will be much more complex than a text based dictionary attack. More research is needed in this area Overall; we believe graphical secret codes are less vulnerable to dictionary attacks than text-based secret codes.

B. *Guessing*

Unfortunately, it seems that graphical secret codes are often predictable, a serious problem typically associated with text-based secret codes. More research efforts are needed to understand the nature of graphical secret codes created by real world users

C. Shoulder Surfing

Like text based secret codes, most of the graphical secret codes are vulnerable to shoulder surfing. At this point, only a few recognition-based techniques are designed to resist shoulder-surfing.

D. *Spy ware*

Except for a few exceptions, key logging or key listening spy ware cannot be used to break graphical secret codes. It is not clear whether "mouse tracking" spy ware will be an effective tool against graphical secret codes. However, mouse motion alone is not enough to break graphical secret codes. Such information has to be correlated with application information, such as window position and size, as well as timing information.

E. *Social Engineering*

Comparing to text based secret code, it is less convenient for a user to give away graphical secret codes to another person. For example, it is very difficult to give away graphical secret codes over the phone. Setting up a phasing web site to obtain Graphical secret codes would be more time consuming.

V. PROPOSED SYSTEM

Now-a-days, all business, government, and academic organizations are investing a lot of money, time and computer memory for the security of information. Online secret code guessing attacks have been known since the early days of the Internet, there is little academic literature on prevention techniques. This project deals with guessing attacks like brute force attacks and dictionary attacks as shown in Figure.7

A. *Proposed System Architecture*

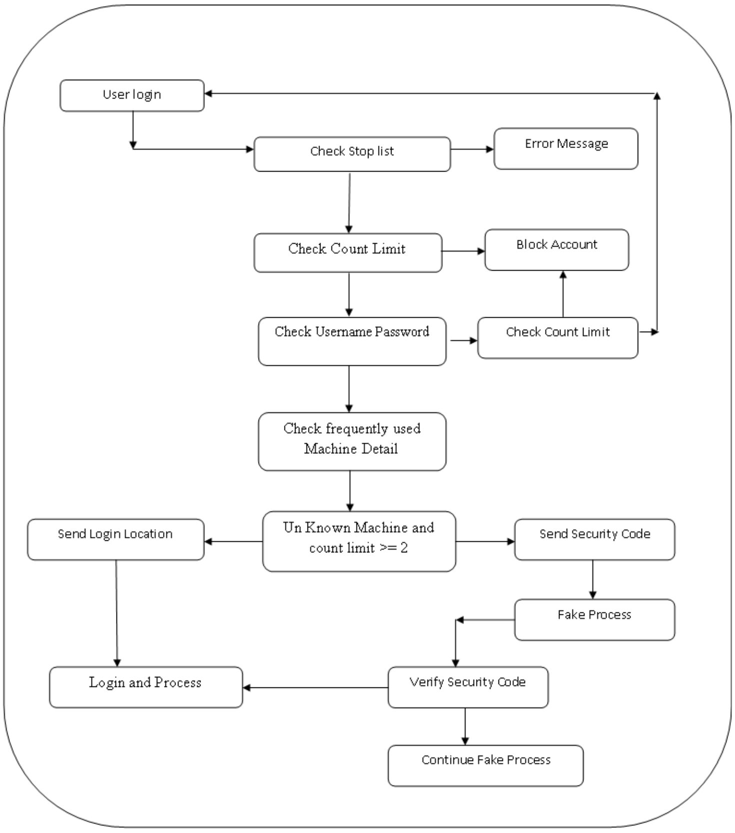


Figure: 7 System Architecture

This project proposes a click-based graphical secret code system. During secret code creation, there is a small view port area that is randomly positioned on the image. Users must select a click-point within the view port. If they are unable or unwilling to select a point in the current view port, they may press the Shuffle button to randomly reposition the view port. The view port guides users to select more random secret codes that are less likely to include hotspots. Therefore this works encouraging users to select more random, and difficult secret codes to guess.

Brute force and dictionary attacks on secret code-only remote login services are now widespread and ever increasing. Enabling convenient login for legitimate users while preventing such attacks is a difficult problem. Automated Turing Tests (ATTs) continue to be an effective, easy-to- deploy approach to identify automated malicious login attempts with reasonable cost of inconvenience to users.

This project proposes a new Secret code Guessing Resistant Protocol (PGRP), derived upon revisiting prior proposals designed to restrict such attacks. While PGRP limits the total number of login attempts from unknown remote hosts, legitimate users in most cases (e.g., when attempts are made from known, frequently-used machines) can make several failed login attempts before being challenged with an ATT.

This proposed system also provides protection against key logger spy ware. Since, computer mouse is used rather than the keyboard to enter our graphical secret code; this protects the secret code from key loggers.

VI. Conclusion and Future Work

A major advantage of Persuasive cued click point scheme is its large secret code space over alphanumeric secret codes. There is a growing interest for Graphical secret codes since they are better than Text based secret codes, although the main argument for graphical secret codes are that people are better at memorizing graphical secret codes than text-based 7 secret codes. Online secret code guessing attacks on secret code-only systems have been observed for decade's .Present-day attackers targeting such systems are empowered by having control of thousand to million node botnets. In previous ATT-based login protocols, there exists a security-usability trade-off with respect to the number of free failed login attempts (i.e., with no ATTs) versus user login convenience (e.g., less ATTs and other requirements). In contrast, PGRP is more restrictive against brute force and dictionary attacks while safely allowing a large number of free failed attempts for legitimate users. PGRP is apparently more effective in preventing secret code guessing attacks (without answering ATT challenges), it also offers more convenient login experience, e.g., fewer ATT challenges for legitimate users. PGRP appears suitable for organizations of both small and large number of user accounts.

References

1. Sonia Chiasson, P.C. van Oorschot, and Robert Biddle,"Graphical Secret code Verification Using Cued Click Points" ESORICS , LNCS 4734, pp.359-374,Springer- Verlag Berlin Heidelberg 2007.
2. A. Adams and M. A. Sasse, "Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures," *Communications of the ACM*, vol. 42, pp. 41-46, 1999.
3. I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A.D. Rubin, "The Design and Analysis of Graphical Secret codes," in *Proceedings of the 8th USENIX Security Symposium*, 1999.
4. Alain Forget, Sonia Chiasson, and Robert Biddle,"Shoulder-Surfing Resistance with Eye-Gaze Entry inCued-Recall Graphical Secret codes", ACM 978-1-60558-929-9/10/04, April 10 – 15, 2010.
5. RealUser, "www.realuser.com," last accessed in June 2005.
6. T. Valentine, "An evaluation of the Passface personal verification system," Technical Report, Goldsmiths College, University of London 1998.
7. Manu Kumar, Tal Garfinkel, Dan Boneh and Terry Winograd, "Reducing Shoulder-surfing by Using Gazebased Secret code Entry", Symposium On Usable Privacy and Security (SOUPS) , July 18-20, 2007, Pittsburgh,PA, USA.
8. Zhi Li, Qibin Sun, Yong Lian, and D. D. Giusto, 'An association-based graphical secret code design resistant to shouldersurfing attack', International Conference on Multimedia and Expo (ICME), IEEE.2005
9. R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Verification," in *Proceedings of 9th USENIX Security Symposium*, 2000.
10. S. Akula and V. Devisetty, "Image Based Registration and Verification System," in *Proceedings of Midwes Instruction and Computing Symposium*, 2004.
11. L. Sobrado and J.-C. Birget, "Graphical secret codes," *The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research*, vol. 4, 2002.
12. Sonia Chiasson ,Alain Forget , Robert Biddle, P. C. van Oorschot, "User interface design affects security: patterns in click-based graphical secret codes", Springer-Verlag 2009.
13. I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A.
14. S. Man, D. Hong, and M. Mathews, "A shouldersurfing resistant graphical secret code scheme," in *Proceedings of International conference on security and management*. Las Vegas, NV, 2003.
15. D. Rubin, "The Design and Analysis of Graphical Secret codes," in *Proceedings of the 8th USENIX Security Symposium*, 1999.

AUTHOR(S) PROFILE

Mr.J.Kanagaraj, received the M.Sc Computer Science in 2013 from Bharathiyar University, Affiliated to Bharathiyar University Coimbatore, Tamilnadu, India.currently pursuing M.Phil in Computer Science in Kovai Kalaimagal College of Arts and Science Affiliated to Bharathiyar university,Coimbatore,Tamilnadu,India.

Mr.K.Noel Binny received M.Phil (Computer science) in 2010 from Coimbatore Institute of Management and Technology, Affiliated to Bharathiyar University, Coimbatore, Tamilnadu, India. He received M.sc (Computer Science) in 2004 from C.M.S College of Science and Commerce, Affiliated to Bharathiyar University, Coimbatore, Tamilnadu, India. He is currently working as a Assistant Professor and Head in Computer Application Department, Kovai Kalaimagal College of Arts and Science, Coimbatore, Tamilnadu, India.