The Design and Implementation of Background Pass-Go Scheme Towards Security Threats

L. Y. Por[1], X. T. Lim[2], M.T. Su[3], F. Kianoush[4]
Faculty of Computer Science and Information Technology,
University of Malaya,
50603, Kuala Lumpur,
MALAYSIA
porlip@um.edu.my[1], emilylim1986@hotmail.com[2], smting@um.edu.my[3], kianoushf@gamil.com[4]

Abstract: - Currently, access to computer systems is often based on the use of alpha-numeric. The textual passwords or alpha-numeric passwords have been the basis of authentication systems for centuries. Similarly, it had also been the major attraction for crackers and attackers. However, users tend to face difficulty in remembering a password that is considered as secured password because this type of secured password usually has long string of characters and they appear randomly [14]. Hence, most users tend to create simple, short and insecure passwords. As a consequence, most of the time, the usability level of passwords has not achieved an optimum for a secured password [14]. In order to solve this problem, a new password scheme had been invented, known as Graphical Password System (GPS). Graphical password is an alternative mean of authentication for login intended to be used in place of conventional password; it utilizes images instead of text. In this paper, we discuss the design and intention of our proposed scheme, called Background Pass-Go (BPG). BPG is an improved version of Pass-Go, as it keeps most of the advantages of Pass-Go and achieves better usability. We had analyzed the BPG scheme in terms of 1) how BPG is able to improve other schemes of GPS especially in Pass-Go, 2) how BPG acts as a solution to different types of threats to networked computer systems. We had verified that BPG manages to overcome the shortage of other GPS schemes. Moreover, the BPG also manages to address most of the security threats for the network security system.

Key-Words: - BPG, Background Pass-Go, Pass-Go, GPS, Graphical Passwords System, Security.

1 Introduction

Passwords are the most commonly used method for identifying users in the networked computer system. Conventional textual passwords use a string of alphanumeric characters (or printable ASCII characters) to identify a user. Hence, conventional textual passwords are also known as alpha-numeric passwords. However, it is well known that textual passwords are vulnerable to small dictionary attack [1]. Small dictionary attack is a method in which an individual uses several tools to crack passwords by automatically testing all the words that occur in dictionaries or public directories. Alpha-numeric passwords were first introduced in the 1960s as a solution to security issues that became evident as the first multi-user operating systems were being developed [2].

The alpha-numeric passwords are only able to offer good security when they are complicated enough to be deduced or guessed. In term of security, a password should consist of a string of 8 or more random characters, including upper and lower case alphabetic characters, digits, and special characters [2]. A random password does not have meaningful content and must be memorized by rote, but rote learning is a weak way of remembering [12]. Hence, many users forget their passwords [10], and with the number of passwords per user increasing, the rate of forgetting increases further [11]. So, due to the limitation of human memory, users often tend to choose passwords that are easy to remember such as a common word. Unfortunately, common word passwords are easily to be guessed and cracked by using several tools in a “small dictionary” attack. This “small dictionary” attack is so successful that in Klein’s case study [3], about 25% of 14,000 passwords were cracked by a dictionary with only 3 million entries (the size of the dictionary is 21.5 bits).

A survey had been conducted on 100 computer literate users from the Faculty of Computer Science and Information Technology, University of Malaya,

Malaysia for the purpose of identifying the vulnerability of the textual passwords which has been used. As shown in Table 1, there are 88% of the users not using the combinations of letters, numbers and symbols as their passwords.

Table 1: The distribution of the passwords constitutions

Constitutions of textual passwords	Computer Users (%)
Letters and symbols	3%
Numbers and symbols	5%
Letters, numbers and symbols	12%
Only letters	25%
Only numbers	15%
Letters and numbers	40%

Based on Fig. 1 and Fig. 2, 55% of the users tend to use the same passwords for accessing all services and 90% of the users have the tendency of changing their textual passwords more than three months (one semester is approximately four and a half months).

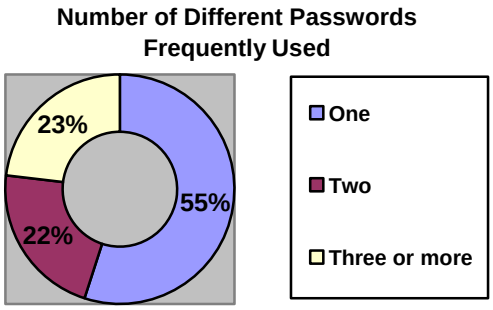

Figure 1: Number of different passwords frequently used for accessing all services

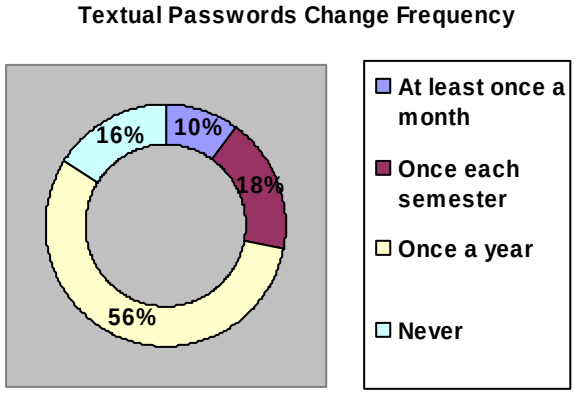

Figure 2: Textual Passwords Change Frequency

The above analyzed results have shown that there are still many users unaware that their textual passwords are vulnerable to security threats. The textual passwords are actually not secured enough for those users who either tend to use the same passwords for accessing all services or rarely change their passwords because it can be easily hacked and retrieved. [22] has mentioned that the choice of the passwords by human users is the core weakness instead of the password authentication itself. Many researches have been carried out and some of the guidelines for selecting and maintaining textual passwords can be obtained from [24, 25].

However, threats from a software security breach could range from the very mild to the disastrous [26]. Due to the increasing number of different types of threats and the general improper practice by most of the users when using textual passwords, the alpha-numeric passwords are no longer sufficient, efficient and secure enough to fully protect the networked-computer systems from being compromised by hackers. Hence, a new method has been invented which is the Graphical Password System (GPS). Graphical password is an alternative mean of authentication for login intended to be used in place of conventional password; it utilizes images instead of text. Psychological studies support the hypothesis that humans have a significant capability to recognize and to recall visual images [21]. If users are able to remember more complex graphical passwords, then an attacker has to spend more time or deploy more computational power to build a bigger dictionary to achieve the same success as for textual passwords. In many implementations, the user is required to pick from a series of images in the correct sequence in order to gain access [4]. The idea of graphical passwords was pioneered by Greg Blonder who also holds the US patent 5559961 (1996). His idea – is to let the user click (with a mouse or stylus) on a few chosen (pre-designed) regions in an (pre-processed) image that appears on the screen [5]. If the correct regions were being clicked, the user would be authenticated.

Throughout the time, a few different methods have been proposed by researchers from different places to improve and enhance GPS. Susan Wiedenbeck et al. [15] conducted the original studies of PassPoints, a system which allows any image to be used and does not need artificial predefined click regions with well-marked boundaries. This scheme has addressed solution to the drawback of Blonder's scheme. Then, multiple-

image schemes have been invented and the studies have been carried out to improve features of the graphical password system. One of these schemes is Passfaces™. Passfaces™, a commercial product by Passfaces Corporation, requires a user to select previously seen human face pictures as a password [13].

Another GPS scheme known as Déjà Vu scheme was designed by Dhamija et al. [19] with non-describable abstract images rather than photographs. The Déjà Vu Scheme in which a matrix of m images is set, where n images are part of the user's portfolio, previously chosen from a set of proposed images. The user must identify those n images to login. Déjà Vu scheme is not a popular choice as a GPS scheme selected by users due to the smaller password space compared to password space of textual passwords.

Proposed by Jermyn et al. [9], Draw a Secret Scheme (DAS) led graphical passwords to a grid background. DAS is a GPS scheme which requires a user to draw a secret design on a grid as a way to input a password. Surprisingly, they found that DAS could offer very large password space for reasonable parameters. By superimposing a background over the blank DAS grid, a group of computer scientists from Newcastle University have created a system called Background Draw a Secret (BDAS). Besides BDAS, there are another two schemes which are also being implemented based on the DAS. These two schemes are Multi-Grid DAS and Pass-Go. Multi-Grid DAS was proposed by Konstantinos Chalkias, Anastasios Alexiadis, and George Stephanides from Macedonia University, Greece. Hai Tao from University of Ottawa, Canada proposed a new grid-based graphical password scheme, Pass-Go, in which users select intersections on a grid to authenticate a system. More issues and threats can be obtained from [23].

In this paper, we propose a new graphical password scheme, called Background Pass-Go (BPG). Background Pass-Go can be considered as an improvement of Pass-Go, as it keeps most of the advantages of Pass-Go and provides higher security level and better usability level compared to the Pass-Go scheme.

In Pass-Go scheme, the sensitive areas are quantified with a radius of 0.4×d (where d is the side length of a grid cell) which was suggested by [17] whereby in BPG, the sensitive areas are set to be 0.30×d radius. Hence, the radius should not be too large in order to reduce the success rate of guess attacks by simply clicking at the points without knowing the real passwords while at the same time if the radius of the sensitive area is too small, that will cause a lot of passwords input problems to the users. Based on heuristic testing, we have tested that the radius of 0.30×d is acceptable from user's perspective and the security outcome is higher than the radius of 0.4×d which was proposed by Pass-Go.

BPG scheme is inspired by Pass-Go, in which users still need to select intersections on a grid for system authentication. However, instead of using the blank background in the Pass-Go scheme, we propose a new scheme by superimposing a background over the blank Pass-Go grid, whereby the background consists of the picture image selected and installed by users themselves. We believe that by having an image background selected by the users, it will be much easier in helping users to remember where they have actually drawn their passwords at and also in which intersection points the passwords existed by referring to the image background instead of having to memorize the coordinate pairs of the grids solely.

This paper is divided into three sections. In the first section, we discuss the design of BPG. The second section analyzes the BPG scheme by identifying the improvements that have been made over other approaches of GPS and how BPG is able to overcome certain security threats. In the last section, we draw some conclusions and discuss the future work.

2 Design of Background Pass-Go

Background Pass-Go (BPG) is a grid-based scheme with an image background. However, it is different from Draw a Secret Scheme (DAS) as BPG requires a user to select (or touch) intersections, instead of cells, as a way to input a password. As a result, the coordinate system refers to a matrix of intersections, rather than cells as in DAS. The main difference between BPG with Pass-Go is that BPG's background is superimposed with an image selected by the users. The purpose is to help users remember

their passwords better in such a way that they are able to remember where they started the password or which parts of the image background that contain their passwords.

Instead of having to remember the coordinate pairs of their passwords, the users can remember their passwords better by recalling back which part of the image background they had clicked before as their passwords and at the same time the grid in this scheme provides a better accuracy for their click points. As an intersection is actually a point that does not has an area, so theoretically it will be almost impossible for a user to select it without an error tolerance mechanism. Thus, a sensitive area needs to be identified to solve this problem.

A sensitive area is an area surrounding each intersection. The reason to implement this sensitive area is to allow users to click on an intersection point within a specific error tolerance area. The sensitive areas are sensitive to the interaction with an input device. Thus, clicking any point inside a sensitive area will be treated the same as clicking the exact corresponding intersection point. The shape and size of the sensitive area can be predefined. There are a few aspects need to be considered before identifying the size of the sensitive area. It is no doubt that the larger the size of the sensitive area the easier it is to select an intersection. However, it will become more difficult to avoid clicking neighboring intersections. Therefore, the optimal size of the sensitive area should be studied carefully before implementing it. In order to reduce the success rate of guess attacks and prevent high ratio of invalid password input problems among valid users, we have implemented round circles sensitive areas with a radius of 0.30×d in BPG. The reason why we proposed a radius of 0.30×d is mainly based on heuristic testing and the survey feedback from 250 end users. Based on the sampling result, we have observed that there is a relative high percentage of declining of accessing occurred after the range 0.30×d radius. In the other hand, more than 80% of the end users are able to access the BGP using the range from 0.30×d, 0.35×d and 0.40×d radius for both with and without the guidance of an indicator case studies (Please refer to Figure 1 and Figure 2). However, from the sampling result, the success rate of accessing with and without the guidance of an indicator at 0.40×d radius and 0.35×d radius is relatively small when comparing with 0.30×d radius. The success rate is approximately 2.38% and 7.14% higher when using 0.40×d radius compared to 0.30×d radius under the guidance of using and without using an indicator respectively. However, there is no significant difference between the range of 0.35×d radius and 0.30×d radius. In order to enforce a higher security by reducing the radius range and with more than 80% acceptance successful rate, a sensitive areas range of 0.30×d radius has been proposed in the dot indicator scheme for BPG.

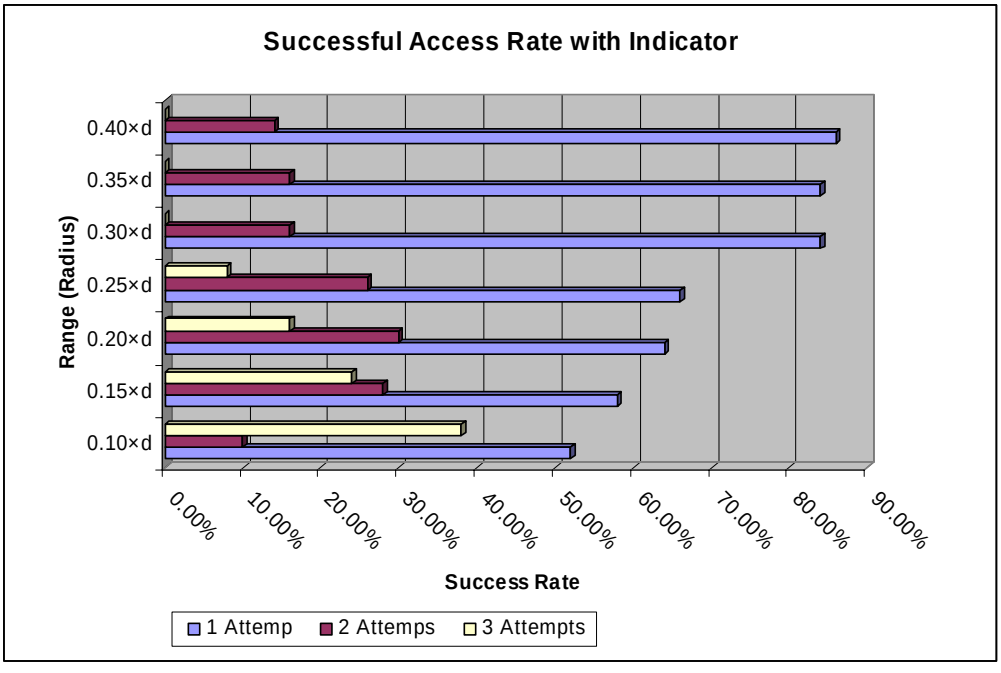

Figure 1: Successful Access Rate with Indicator

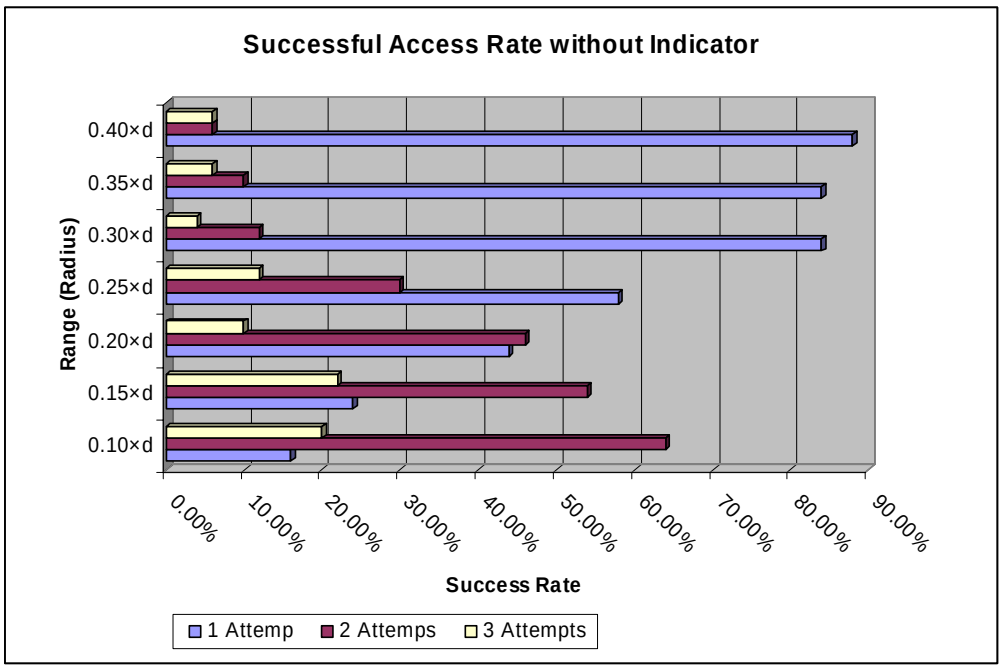

Figure 2: Successful Access Rate without Indicator

BPG also addressed the problem of sensitive area which is invisible in the Pass-Go. To ease the process of inputting a password, the sensitive area in our scheme will be highlighted with a color chosen by users to make it looked more obvious and apparent by the users so that the boundary of sensitive areas are visible to users. Based on that, the user can see exactly where he or she should select. The users have the choice to choose whether they want to show the sensitive areas of BPG for their ease of usage during password inputting process or otherwise, when the surrounding environment around them is not convenient, i.e. at public place to avoid shoulder surfing problem.

BPG uses the same access function as in Pass-Go scheme. The users can draw a shape freely depending on their own preferences. The indicators work the same way as they were in Pass-Go scheme. Dot and line indicators are displayed to show the intersections and grid lines that correspond most closely with the input trace. A dot indicator will only appear when one intersection is selected (or clicked) whereas a line indicator will appear only when two or more intersections are selected continuously. The thickness and pattern of indicators can be optimized accordingly to the preference of users. Besides, BPG uses constant indicators to acknowledge the passwords because we believe that this approach will be able to accelerate the process of memorization by using the invariable indicators. The password is then encoded as a sequence of intersections, represented by the two-dimensional coordinate pairs.

We also implement the feature of disguising indicators in BPG. In response to each user input, one or more disguising dot or line indicators may be displayed at random positions along with the true ones. A disguising dot indicator or disguising line indicator has the exact same style, shape, color and size as the real dot indicator or line indicator in order to prevent the attacker from being able to recognize the users' passwords.

Figure 3 shows the GUI Design of Background Pass-Go

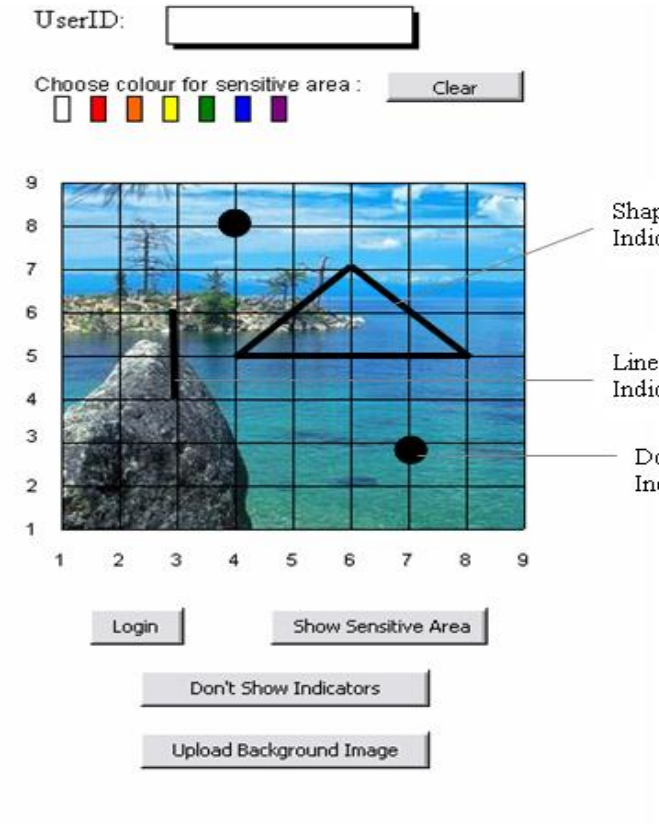

Figure 3: GUI Design of Background Pass-Go

3 Analysis of Other Related Work and the Preliminary Results

In this section, we analyze BPG in term of few aspects.

3.1 Improvement of BPG over Other GPS Schemes

Blonder [6] gave the initial idea of graphical password. In his scheme, a user is presented with one predetermined image on a visual display and is required to select one or more predetermined positions in a particular order to access the restricted resource. The major drawback of this scheme is that users cannot click arbitrarily on the background. The users have to click on their passwords exactly by following the same sequences of order as they were when the passwords were first created. Background Pass-Go has addressed solution to this drawback of Blonder's scheme. In Background Pass-Go scheme, users can click on the intersection points freely without being limited to certain sequences of order. In a single-image scheme like Blonder's scheme, looking for small spots in a rich picture might be tiresome and unpleasant for users with weak vision. Hence, compared with the Blonder's scheme, the grids in BPG scheme help users to click on the points more easily and with more accuracy while the image on the background act as a reference aide to help users remember their passwords better.

Passfaces™, a commercial product by Passfaces Corporation, requires a user to select previously seen human face pictures as a password [13]. Brostoff and Sasse conducted a user study (34 subjects involved) on this scheme and their result suggests that Passfaces™ is easier to remember than textual passwords [18]. However, Davis et al. empirically studied and compared these two schemes by surveying 154 computer engineering and computer science students from two universities. Their result shows that in Passfaces™ the user's choice is highly affected by race, the gender of the user, and the attractiveness of the faces [16]. As an end user, there are two major limitations which we think Passfaces™ need to consider such as 1) some faces displayed might not be welcomed by certain users. In other words, if a

user has to look at some faces he/she dislikes, the login process will become unpleasant. 2) It cannot be used by people who are face-blind (a disease which affects a person's ability to tell faces apart) [16]. BPG is freed from these problems because the background image is selected by the users, hence the unpleasant process which existed in Passfaces™ will not occur in BPG.

By exploiting hash visualization techniques [20], another scheme called Déjà Vu [19] was designed with non-describable abstract images rather than photographs. It uses images that are generated on the fly from stored seed values. Although Déjà Vu has a general advantage which is choosing weak passwords or writing them down becomes difficult, it still has its disadvantage. There are possibilities that a brute force attack can be launched by trying all combinations of images in the challenge set in Déjà Vu scheme. This is due to the password space of Déjà Vu scheme (which is only 53,130) is smaller than the password space of the textual passwords. Compared with Déjà Vu scheme, the memorable password space of BPG is much larger due to its capability of enabling users from select different indicator types. Hence, it is much harder for a "brute force" attack to be launched towards BPG users.

It is undeniably that PassPoints scheme has overcome the limitations of Blonder's initial idea of needing simple, artificial images, predefined regions as well as providing larger password space over alphanumeric passwords, Blonder-style graphical passwords and recognition-based graphical password [15]. However, there is still weakness in this scheme, which is the graphical password input clicking outside the tolerance surrounding the user's click point. Users were often close to, but outside, the tolerance. Most of the users still had difficulty in clicking the points more precisely even after quite some time of practice. Furthermore, users of PassPoints also faced the problem of inputting their passwords slowly due to uncertainties about their clicking points. The researchers of PassPoints believed that this drawback was because of the memory problem. The approach of the sensitive area in our scheme highlighted with a color chosen by users accordingly is able to help users to reduce the possibility of clicking outside the tolerance. This sensitive area feature makes it looked more obvious to the users. User can then see exactly where he or she should select in which the process of inputting a password.

Jeremyn et al. [9] described a graphical password scheme Draw a Secret (DAS), where users draw a shape on a grid. Users need to draw approximately the same shape in order to authenticate themselves One of the drawbacks of the pure grid-based scheme such as Draw a Secret (DAS) is that it introduces additional tasks to memorize and to input a password. In other words, the security improvement of DAS is achieved by sacrificing some degree of usability and ability to memorize. Hence, we add the feature of personalizing an image background which the user is familiar with in BPG so that it can help user to memorize their passwords position better. Besides this, the major drawback of DAS is that diagonal lines are difficult to draw. The users have to draw their input sufficiently away from the grid lines and intersections in order to enter the password correctly. If a user draws a password close to the grid lines or intersections, the scheme may not distinguish which cell the user is choosing. Users might get frustrated if they failed to login consecutively due to the difficulty to input a password. Hence, the most obvious advantage of changing from cell to intersection is that drawing diagonal lines becomes feasible. A user can draw a shape more freely, compared to the DAS scheme. The feature of having image background in BPG also has helped to improve Multi-Grid DAS and Pass-Go the same way as it does with DAS by helping users to remember and memorize their passwords better.

3.2 BPG, a Solution to Threats

Since there are many types of threats and specific attacks towards the networked-computer systems today, it is necessary for us to improve the GPS scheme from time to time in order to provide a better security level to the networked-computer systems. One of the most common threats to most of the graphical passwords system schemes is "shoulder surfing" problem. "Shoulder surfing" is a process of password theft through surreptitious monitoring [2]. "Shoulder surfing" can happen when an attacker directly watches a user during login, or when a security camera films a user, or when an electromagnetic pulse scanner monitors the keyboard or the mouse, or when trojan login screens capture the passwords being entered by the user.

Hence, we believe that by implementing the feature of disguising indicators in BPG is able to provide a solution to "shoulder surfing". In response to each user input, one or more disguising dot or line indicators may be displayed at random positions along with the true ones. A disguising dot indicator or disguising line indicator has the exact same style, shape, color and size as the real dot indicator or line indicator in order to prevent the attacker from being able to recognize the users' passwords.

In the case of "brute force" attack, the software uses all possible combinations that a user could use for a password, until the hacker is able to gain access to the secured system. According to [27], a password authentication protocol can stand guessing attack only if attackers cannot verify their guessing. In BPG, the memorable password space is much larger compared with other schemes due to its capability of enabling users to select different indicator types. Hence, it is much harder for a "brute force" attack to be launched towards BPG users. In addition to this, as compared to DAS scheme, BPG (as an enhanced version of Pass-Go) does offer significant resistance to symmetric graphical dictionary attacks (a threat suggested by Thorpe and Van Oorschot [7, 8]). The above mentioned prove can be obtained from [17].

For the threat of phishing, even though the attackers may be successful in tricking the users to click on the link to access a fake website but by implementing BPG it is not an easy task for the attackers to retrieve the users' actual passwords information due to the line and dot indications mechanisms which has been used. BPG users only input their passwords by clicking on the intersection points with an imaged background instead of typing out the numeric values and alphabet characters, so the usual way which was used by phishing attackers to capture the users' information will not work for BPG.

The same goes for pharming, a process that is able to compromise Domain Name Services (DNS) to automatically redirect users to a fraudulent site when attempt to login to a legitimate website. The method of inputting password by clicking on the intersection points instead of typing out the textual passwords has helped to prevent the pharmers from being able to capture the users' information. Furthermore, the password space of BPG is much larger than the textual passwords, thus it is difficult for a graphical dictionary attack or guess attack to occur as well.

4 Conclusions and Future Work

We have presented a new graphical password scheme and shown that it keeps most of the advantages of the Pass-Go scheme and offers better usability. There is no extra processing power and storage needed for BPG to store and retrieve the background image which had been selected by a user. The reason behind this is because the imaged background which chosen by the user is only used to assist the user in remembering his/her passwords or more precisely the actually location of the selected indicators. Hence, this helped to improve the usability level of graphical passwords and prevent unnecessary pre and post processing and storage utilization of the system.

The size of the memorable password space of BPG is much larger than that of textual passwords. (Evidence can be obtained from [17]). The larger the memorable password space, the harder it is for the attackers to be able to create the graphical dictionary and launch attacks towards the networked computer systems. Thus, the security level of the networked-computer systems is enhanced by the use of BPG.

Usability and security are two main concerns and challenge in developing BPG. While graphical users always took more time to input their passwords than alphanumeric users, even so there was evidence that with continuous use, graphical passwords can be entered quite quickly. The evidence was shown by the research of Susan Wiedenbeck and her team [14]. Hence, the time to enter graphical passwords should not be an obstacle for users to use graphical passwords.

The future work should be focused towards optimizing the Background Pass-Go scheme: designing more helpful referencing aids; looking for better solutions for the shoulder surfing problem, and so on. Besides that, it is important also to put more efforts in studying about memorable passwords space in order to improve the security level. Although now it seems that the possibility for graphical dictionary attacks to occur is not high but

we will continue to further study and enhance the security and usability level of BPG scheme.

References:

[1] Feldmeier, D. and Karn, P., UNIX password security-Ten years later. In *Proceedings of the 19th International Conference on Advances in Cryptology (CRYPTO '89)*, Lecture Notes in Computer Science, vol. 435, Springer Verlag, 1989.

[2] Sobrado, L, and Birget, J. C., Graphical Password, The Rutgers Scholar, *An electronic bulletin of Undergraduate Research*, Vol 4., available at: http://rutgersscholar.rutgers.edu/volume04/sobrbirg/sobrbirg.htm, last access date : 7 Dec 2007.

[3] Klein, D., Foiling the cracker: A survey of and improvements to, password security, In Proceedings of the 2nd USENIX Security Workshop, pp. 5-14, 1990.

[4] Wikipedia, Graphical Passwords, available at: *http://en.wikipedia.org/wiki/Graphical_passwords*, last access date: 7 Dec 2007.

[5] J.C. Birget, The Graphical Passwords Project, Funded by the NSF CyberTrust Project, Co-PIs: J.C. Birget (Rutgers-Camden), D. Hong (Rutgers-Camden), N. Memon (Brooklyn Polytechnic), S.Man (SW Minn. State), S. Wiedenbeck (Drexel), available at: *http://clam.rutgers.edu/~birget/grPssw/*, last access date: 7 Dec 2007.

[6] Blonder, G., *Graphical passwords*. United States Patent 5559961, 1996.

[7] Thorpe, J. and Van Oorschot, P. C., Graphical Dictionaries and the Memorable Space of Graphical Passwords. In *Proceedings of the 13th USENIX Security Symposium*, pp.135-150, 2004.

[8] Thorpe, J. and Van Oorschot, P. C., Towards Secure Design Choices For Implementing Graphical Passwords. In *Proceedings of the 20th Annual Computer Security Applications Conference (ACSAC)*, Tucson, USA, 2004.

[9] I. Jeremyn, A. Mayer, F. Monrose, M.K. Reiter, A.D.Rubin, The design and analysis of graphical passwords, *Proc. 8th Usenix Security Symposium*, 1999.

[10] Adams, A., Sasse, M. A. and Lunt, P., Making Passwords Secure and Usable, in H. Thimbleby, leby, B. O'connailal and P. Thomas (Eds.), *HCI '97- People and Computers XII*, Springer-Verlag, Bristol , pp.1-20, 1997.

[11] Zviran, M. and Haga, W. J., A Comparison of Password Techniques for Multilevel Authentication Mechanisms., *The Computer Journal*, vol 36(3), pp. 227-237, 1993.

[12] Rundus, D. J., Analysis of rehearsal processes in free recall, *Journal of Experimental Psychology*, vol 89, pp. 63-77, 1971.

[13] Passfaces, The science behind PassfacesTM for windows, available at: *http://www.realuser.com/resources/white%20papers.htm*, last access date: 9 Dec 2007.

[14] Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A. and Memon, N, Authentication using graphical passwords: Basic Results, *Proc. Human-Computer Interaction International*, in press, 2005.

[15] Wiedenbeck, S., Waters, J., Birget, J. Brodskiy, A., and Memon, N., PassPoints: Design and longitudinal evaluation of a graphical password system, *International J. of Human-Computer Studies (Special Issue on HCI Research in Privacy and Security)*, vol 63, pp. 102–127, 2005.

[16] Davis, D., Monrose, F., and Reiter, M. K., On User Choice in Graphical Password Schemes., In *Proceedings of the 13th USENIX Security Symposium*, pp. 151-164, 2004.

[17] Tao, H., Pass-Go, *a New Graphical Password Scheme*, Ottawa, Canada, 2006.

[18] Brostoff, S. and Sasse, M. A. 2000. Are Passfaces™ more usable than passwords? A field trial investigation. In *Proceedings of Human Computer Interaction*, pp. 405–424, 2000.

[19] Dhamija, R. and Perrig, A. 2000. Déjà Vu: A User Study Using Images for Authentication. In *Proceedings of the 9th USENIX Security Symposium*.

[20] Perrig, A. and Song, D. 1999. Hash Visualization: a New Technique to Improve Real-World Security. *In International Workshop on Cryptographic Techniques and ECommerce*, pp. 131–138, 1999.

[21] Paivio A., Rogers, T. B., and Smythe, P. C. 1968. Why are pictures easier to recall than words? *Psychonomic Science*, 11:137-138, 1968.

[22] Wanli Ma, John Campbell, Dat Tran, and Dale Kleeman, A Conceptual Framework for Assessing Password Quality, *IJCSNS International Journal of Computer Science and Network Security*, vol.7 No.1, pp. 179-185, 2007.

[23] L. Y. Por, X. T. Lim, Issues, Threats and Future Trend for GSP, *Proceedings of The 7th WSEAS International Conference on Applied Computer & Applied Computational Science*

(ACACOS '08), Hangzhou, China, pp. 627-633, 2008.

[24] Kessler, G.C., Passwords - strengths and weaknesses, *http://www.garykessler.net/library/password.html*, last access date: 30 May 2008.

[25] Klein, D., Foiling the cracker: a survey of, and improvements to, password security, *Proceedings of the 2nd USENIX Security Workshop*, http://citeseer.ist.psu.edu/112514.html, last access date: 30 May 2008.

[26] Ahmad AlAzzazi and Asim El Sheikh, Security Software Engineering: Do it the right way, *Proceedings of the 6th WSEAS Int. Conf. on Software Engineering, Parallel and Distributed Systems*, Corfu Island, Greece, pp. 19-23, 2007.

[27] Y. C. Lee, Y. C. Hsieh and P. S. You, A New Improved Secure Password Authentication Protocol to Resist Guessing Attack in Wireless Networks, *Proceedings of the 7th WSEAS Int. Conf. on Applied Computer & Applied Computational Science (ACACOS '08)*, Hangzhou, China, pp. 160-163, 2008.