Multi-Grid Background Pass-Go

L. Y. POR[1], X. T. LIM[2]
Faculty of Computer Science and Information Technology
University of Malaya
50603, Kuala Lumpur
MALAYSIA
porlip@um.edu.my[1], emilylim1986@hotmail.com[2]

Abstract: - Computer security depends largely on passwords to authenticate the human user for access to secure systems. Remembering the password they have chosen is a frequent problem for all users. As a result, they tend to choose short and insecure passwords as compared to secure passwords which usually consist of a long mixture of random alphanumeric and non-alphanumeric characters. Thus, the tendency of choosing insecure passwords has brought up many security problems. Graphical password is an alternative to replace alpha-numeric password in which users only have to click on the images in order to authenticate themselves rather than typing alphanumeric strings. The main objectives of this paper are to present a classification of graphical passwords system (GPS) and identify its future research area. In this paper, we attempt to identify a number of threats to the networked computer systems, focus on the research of graphical password system (GPS) and analysis on some aspects of GPS; 1) how each GPS algorithm works, 2) the advantages and disadvantages of each GPS algorithm, 3) how each GPS algorithm is able to address solutions to the threats. Besides, the paper also concentrates on the design and the implication of a proposed prototype, namely Multi-Grid Background Pass-Go (MGBPG) which is targeted to be its strength and the winning edge over other graphical password systems. The preliminary result and analysis of the proposed prototype is then presented by comparing it on its role in addressing the drawbacks of current existing GPS and several security attacks. Finally, we highlight a few aspects, which need to be improved in the future to overcome the deficiencies of previous GPS methods that have been invented.

Key-Words: - GPS, Graphical Password System, Background Pass-Go, BPG, Multi-Grid Background Pass-Go, MGBPG, Password, Authentication, Threat.

1 Introduction

Because of the increasing threats to networked computer systems, there is a great need for improving security. Passwords are the most commonly used method to authenticate human users for access to secure systems. Typically, passwords are strings of letters and digits, i.e., alpha-numeric passwords. Alpha-numeric passwords were first introduced in the 1960s as a solution to security issues [8].

However, with the increasing number of threats, alpha-numeric passwords are not efficient and secure enough to fully protect the networked computer system from being compromised by hackers. The traditional alphanumeric passwords have drawbacks from a usability standpoint, and these usability problems tend to translate directly into security problems. That is, users who fail to choose and handle passwords securely open holes that attackers can exploit [6]. The alpha-numeric passwords have some disadvantages such as 1) being hard to remember if they are complicated enough to offer good security, 2) vulnerable to "shoulder surfing", 3) easily exposed to dictionary attack due to the fact that most users tend to choose a common word as their passwords which will be easily guessed.

Due to the weaknesses which exist in alpha-numeric passwords and the fact that most humans process and store graphical information with greater ease, a better password system has been invented, i.e., graphical password system (GPS). Graphical passwords are an alternative means of authentication intended to be used in place of conventional password; they utilize images instead of text. In many implementations, the user is required to pick from a series of images in the correct sequence in order to gain access [1]. 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 (pre-processed) an image that appears on the screen [2]. If the correct regions were clicked in, the user would be authenticated.

GPS is able to overcome the problem of being hard to remember. Thus, graphical passwords provide a way of being more human-friendly passwords while increasing the level of security at the same time.

2 GPS Security Threats

Threats from a software security breach could range from the very mild to the disastrous [18]. As there are many variations of threats and specific attacks towards the networked computer systems today, it is necessary for us to identify the types of threats in order to minimize security threats in GPS.

Spyware is one of the biggest threats to computer security. It gathers information about users and their computer systems without their permissions and sends this lucrative information to the parties who have installed the spyware. Besides spyware, there are some other threats which act as ways to gain access to secure system. These include the use of software that logs keystrokes and the "brute force" method. Key logging software records all the keystrokes input from the keyboard and stores it for the hacker to look through and find out what could be the password. 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 secure system.

Another type of threat is hotspots and dictionary attack. Hotspots are specific areas in the image that have a higher probability of being selected by users as part of their passwords. If the attackers can accurately predict the hotspots in an image, then a dictionary of passwords containing combinations of these hotspots can be built and hence form the dictionary attack.

Phishing and pharming are two types of threats which trick unsuspecting users into clicking on links to fake websites and giving up their usernames, passwords, and other personal information leading to financial fraud and identity theft. Unlike phishing, where users click on links in e-mails and taken to the fake site, pharming compromise Domain Name Services (DNS) to automatically redirect users to a fraudulent site when attempting to login to a legitimate website. What is alarming is that pharming can reroute many thousands of Internet users at a time, causing a potentially huge impact to the computer security. With phishing, the attacker is scamming one person at a time whereas pharming allows attacker to scam a large group of users at once.

Man in the Middle is a form of threat which uses the phishing method to trick users from clicking on a link to login to their bank through a Man-in-the-Middle phishing proxy site. The amazing part is that the users are actually passed through to the real website.

Man in the Browser (MITB) is a variation on the Man in the Middle attack where malware in the web browser interjects itself between the user and the browser to modify the transaction data.

"Shoulder surfing" is a process of password theft through surreptitious monitoring. "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.

All the threats discussed above have caused a potentially large impact to the security of networked computer systems. Hence, different types of graphical password schemes have been studied, enhanced and invented in order to address efficient solutions to those threats.

3 Related Work

Figure 1 shows the evolution of GPS methods. In general, the GPS methods can be categorized into graphic based GPS, spot based GPS and hybrid based GPS.

In year 1996, Greg Blonder [9] presented the initial idea of graphical password. In his scheme, a user is presented with one predetermined image on a visual display and required to select one or more predetermined positions from the displayed image in a particular order to gain access to a secure system.

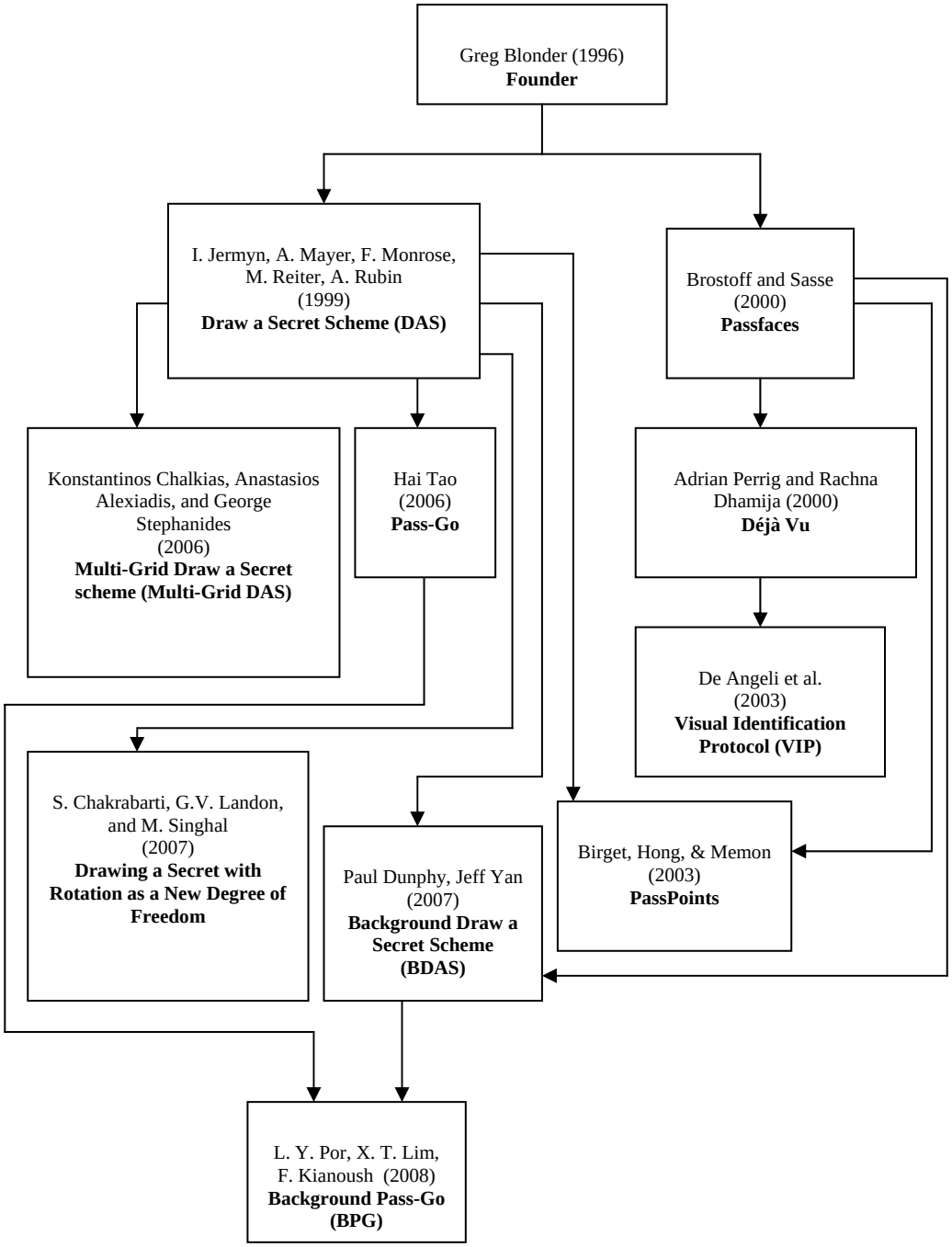

Fig. 1 GPS evolution [17]

However, his scheme has one major drawback which is users cannot click arbitrarily on the background. Thus, several studies and approaches have been made from time to time by different researchers to improve his system. Passfaces Corporation then produced a commercial product named Passfaces™ that uses the idea of multiple-image schemes in the year 2000.

Passfaces Corporation then produced a commercial product named Passfaces™ that uses the idea of multiple-image schemes in the year 2000.

To create a password in Passfaces, a user is required to select previously seen human face pictures as a password [4]. The user needs to choose four images of human faces from a portfolio of faces in the first place. In order to again access into a Passfaces system, the user has to view a grid of nine faces, which includes one face previously chosen by the user and eight decoy faces. The user then has to click anywhere on the known face. This procedure has to be repeated with different target and decoy faces, for a total of four rounds.

The user is only authorized by the system if he or she successfully chose all four correct faces. The order of faces within each grid is randomized so as to help secure a user's Passfaces combination against detection through shoulder-surfing and packet-sniffing.

Brostoff and Sasse have drawn a conclusion that Passfaces™ is easier to remember compared to textual passwords [5] based on users' study survey results which they have obtained.

Due to the fact that for each attempt there are nine faces to be displayed on each screen, an attacker has a 1-in-9 chance of guessing the faces correctly. In order to increase the security level, more attempts such as 15 or 16 rounds would be required. However, the increment of the number of attempts could probably slow down the accessing time and become annoying to users. Moreover, some faces which are predefined by the system might not be welcomed by certain users. If a user has to look at some faces he or she dislikes, the login process will become unpleasant.

In order to prevent the issues which occurred in Passfaces and to alleviate the face-blind (a disease which affects a person's ability to tell faces apart) problem, Adrian Perrig and Rachna Dhamija have proposed another image based GPS named Déjà Vu.

Déjà Vu [22] is a GPS algorithm which uses non-describable abstract images, rather than photographs. It uses images that are generated on the fly from stored seed values. The Déjà Vu system authentication consists of 3 phases. During the first phase (portfolio creation), a user need to select a set of images from the system's portfolio set. Then, during the training phase the user is shown his portfolio to get him accustomed to it. Each time he wishes to login (the login phase), he is shown a randomly generated set of images called the challenge set which contains some images from his portfolio set and some other decoy images. The user then has to select the images that belong to his portfolio in order to login successfully.

However, the seeds storing on the server of Déjà Vu system has created some problems. For instances, if A knows B very well, then there is a possibility of A making an educated guess attack on the system by guessing what images B might have in his portfolio. There are also possibilities that a brute force attack can be launched by trying all combinations of images in the challenge set.

In the year 2003, De Angeli et al [13] have presented a series of Visual Identification Protocol (VIP) models. The similarity of all the VIP series is that they are all using a pictorial concept to replace PIN numbers as in Automatic Teller Machine (ATM) authentication. The VIP images used can be clustered into nine semantic categories such as flowers, animals, rocks, landscapes, humans, vegetables, buildings, skies, boats.

In VIP1, a user had to select a sequence of four pictures out of ten in the same position at each authentication attempt. For every authentication attempt, the user selected categories and a new set of distracters will be extracted from the visual database. In case of authentication failure, three attempts were given as in a normal ATM transaction.

VIP2 differed from VIP1 in that the four pictures forming the authentication code were displayed in random positions around the visual keypad at each authentication attempt [14]. In case of authentication failure, the same visual configuration was displayed in order not to disclose any clue about the authentication code.

According to [14], VIP3 enables a user to identify eight pictures and only four pictures will be randomly displayed for every authentication at each attempt together with 12 distracters so as to avoid duplication of the categories of the code items displayed in the current challenge set. During an authentication failure, the same visual configuration will be displayed.

Although all the VIP models series which have been presented by De Angeli et al managed to increase the ease of users in memorizing their password, however, those VIP models series are still open to shoulder surfing, phishing and pharming attacks which happened in a normal ATM transaction.

Conversely, Draw a Secret Scheme (DAS), the first spot based GPS, has been proposed by Jermyn et al. [11] in year 1999. Users under this scheme can create their secret password by drawing their secret password as a free-form image on a grid. At login time, a user is required to draw the same pattern of image on the grid to gain access to the system. This algorithm involves storing the co-ordinates of grid cells where the user puts his pen down, draws a line and then lifts his pen up. Each pen up has a specific value. The bit string generated from the drawing is hashed using a one way hash function, and stored. This hash is then matched with the stored hash in order to authenticate the user.

DAS is an algorithm which is easier to remember as the users are freed from having to remember any kind of alphanumeric string. By implementing DAS, users are able to obtain authentication that is convincingly stronger than textual passwords but not significantly harder to remember. Besides these, DAS can derive a secret key, e.g., to encrypt and decrypt files, without need to store the password on the device. Hence, both the password and the encrypted content can be protected from the attacker even if the device falls into the attacker's hands. The effect that lack of knowledge of the distribution of user choices has on an attacker is able to improve the security as well.

There are some problems in DAS algorithm. One of this is if the attacker obtains a copy of the stored secret, then there is a possibility that he can launch a brute force attack by trying all possible combinations of co-ordinates of the grid. Another problem is that users accessing the system at public places using PCs will be susceptible to “shoulder-surfing”. In addition to the above, the diagonal lines are difficult to draw. Difficulties might arise when the user chooses a drawing that contains strokes that pass too close to a grid-line, the scheme may not distinguish which cell the user is choosing. DAS requires that the cells must be sufficiently large and must not be too small. Thus, the scalability of DAS is restricted. This has become one of the disadvantages. This limitation further sacrifices the ease of inputting passwords, restricts freedom of choosing passwords, and subsequently reduces the memorable password space and the security level.

Multi-Grid DAS was proposed by Konstantinos Chalkias, Anastasios Alexiadis, and George Stephanides in year 2006. Multi-Grid DAS is a different modified DAS scheme where the cells are not identical in size. This idea can be easily implemented using a multi-grid construction. The final grid could be composed from several internal grids. The aim of this scheme is to decrease the password centering effect. In multi-grid scheme, the user is able to focus in a single internal grid, so there is more than one area where the password can be centered to. Besides that, the user has the opportunity to choose a grid from a list of pre-defined multi-grid templates. In the simple DAS algorithm, every cell has at most four adjacent cells. However, in Multi-Grid DAS, a cell can have more than four neighbors.

Multi-Grid has the advantage of enabling users to center their passwords in different areas on the grid. The use of nested grids provides better security while remaining user-friendly. The selection of custom grid-templates makes this algorithm become even more resistant to dictionary attacks. The researchers suppose that the multi-grid approach will decrease the shift errors as the full

grid consists of small nested grids. The results of their survey suggested that multi-grid approach really eliminates the shift errors. Another important factor of security when using multi-grids is that the user has the opportunity to choose a grid from a list of pre-defined multi-grid templates. In this case, every user will have his custom grid which means that an attacker has to try even harder to find a password using massive brute-force techniques. This is caused by the fact that the number of the neighbor cells is not fixed [12]. Although it reduces the number of shift errors but the results of the ordering errors still stay unchanged.

In year 2006, Hai Tao was inspired by the Japanese chess game and proposed a new GPS scheme named Pass-Go. Pass-Go requires a user to select (or touch) intersections, instead of cells, as a way to input a password. Consequently, the coordinate system refers to a matrix of intersections, rather than cells as in DAS. The users have to select intersections on a grid in order to authenticate a system. The dot and line indicators displayed are to show the intersections and grid lines which correspond most closely with the input trace. A dot indicator appears when one intersection is selected (or clicked), and a line indicator appears when two or more intersections are touched continuously. There is a sensitive area surrounding each intersection which helps users to touch the intersection with an error tolerance.

By implementing Pass-Go algorithm, a user can draw a shape more freely, compared to the DAS scheme. Besides that, Pass-Go achieves stronger security and better usability. An extremely large full password space is offered by this algorithm. Despite all these advantages, there are some problems that arise as well. Firstly, the more digits the encoding of a password contains, the more difficult it is to input it. Secondly, sensitive areas are invisible; therefore a user will not know if he or she has successfully selected an intersection or not until the dot or line indicator appears. Hence, the users have to spend a period of time to practice before they are able to draw lines without making any unintentional errors.

Paul Dunphy and Jeff Yan from Newcastle University then superimposed a background over the blank DAS grid as to create a brand new system called Background Draw a Secret (BDAS) in year 2007. The mechanism of BDAS is exactly the same as DAS except with an aid of background image.

According to [15], one of the advantages of superimposing a background over the blank DAS grid is helping users to remember where they began the drawing that they are using as a password and also leads to graphical passwords that are less predictable, longer and more complex. BDAS software encourages people to draw more complicated password images such as the password images with a larger stroke count or length, that were less symmetrical and did not start in the centre. This makes them much harder for people or automated hacker programs to guess.

For example, if a person chooses a flower background and then draws a butterfly as their secret password image onto it, they have to remember where they began on the grid and the order of their pen strokes. The BDAS passwords are recognized as identical if the encoding is the same, not the drawing itself, which allows for some margin of error. This feature helps to make sure that the drawing does not have to be recreated exactly.

BDAS helps users to remember where they began the drawing [15]. It also leads to graphical passwords that are less predictable and longer. Thus, BDAS is a simple enhancement that improves security and enhances the usability at the same time. However, it may take longer time to create the graphical password initially.

Susan Wiedenbeck et al. [10] have proposed a hybrid scheme named PassPoints in year 2003. PassPoints scheme: (1) allows any image to be used and (2) does not need artificial predefined click regions with well-marked boundaries – a password can be any arbitrarily chosen sequence of points in the image [3]. The complex images can have hundreds of memorable points, for an instance, with 5 or 6 click points one can make more passwords than 8-character Unix-style passwords. In order to log in successfully, the user has to click close to the chosen click points, within some sets of tolerance distance, e.g., within .25 to .50 cm from the user's click point [7].

This tolerance is needed because the user's click point literally is a single pixel, which is too precise

for a user to be able to click on it successfully. The tolerance gives a margin of error around the click point where the user's click is recognized as correct. This feature enables user to log in successfully within the tolerance distance.

One of the advantages of PassPoints is that it is able to overcome Blonder's original idea limitations of needing simple, artificial images, predefined regions [7]. Besides this, PassPoints also provides larger password space over alphanumeric passwords and Blonder-style graphical passwords. It is also a much more secure system.

Despite the advantages stated above, PassPoints has some disadvantages that need to be considered. Firstly, it takes significantly longer total time to input the graphical passwords. Secondly, PassPoints identifies certain important points on an image, rather than areas, and the user has to click relatively close to all those points to gain access to the system [7]. There are possibilities that the graphical password input clicking outside the tolerance around the user's click point. Participants were often close to, but outside, the tolerance. The users had trouble handling multi-PassPoints image. In addition to that, the attackers are often able to guess PassPoints due to image "hotspots".

In year 2007, S. Chakrabarti, G.V. Landon, and M. Singhal have proposed another hybrid method named DAS with Rotation (R-DAS) which allowed the users to rotate the canvas on which he draws the password. R-DAS inherited all DAS features in addition with extra rotation angles. Based on the analyzed result from [16], R-DAS not only increases the full graphical password space, but also increases the predictable graphical password space corresponding to the number of components (strokes). With the visually obvious technique of rotation, R-DAS manages to provide greater security than DAS scheme. However, in terms of memorability, R-DAS faces a bigger challenge compare to DAS.

Background Pass-Go (BPG) [20] is an enhanced version of Pass-Go which was proposed by L. Y. Por, X. T. Lim and F. Kianoush in the year 2008. According to [20], the BPG scheme manages to ease users in remembering and memorizing their passwords by superimposing an image that is selected by the users together with the background of the system. To reduce the success rate of guess attacks and to prevent a high ratio of invalid password input problems among end users, the BPG scheme has managed to reduce the sensitive areas of an indicator from 0.4×d radius (which was proposed by Pass-Go scheme) to 0.3×d radius. However, the fix grid size which was proposed by the BPG scheme and the Pass-Go scheme can still be enhanced. As a consequence, Multi-Grid Background Pass-Go (MGBPG) has been proposed.

4 Multi-Grid Background Pass-Go Design and Implication

MGBPG is an enhanced scheme which has been proposed and designed based on the inspiration of Multi-Grid DAS, Pass-Go and BGP schemes. A prototype which uses Java Applet has been developed for testing the proposed MGBPG scheme. Figure 2 shows the graphical user interface (GUI) for the MGBPG.

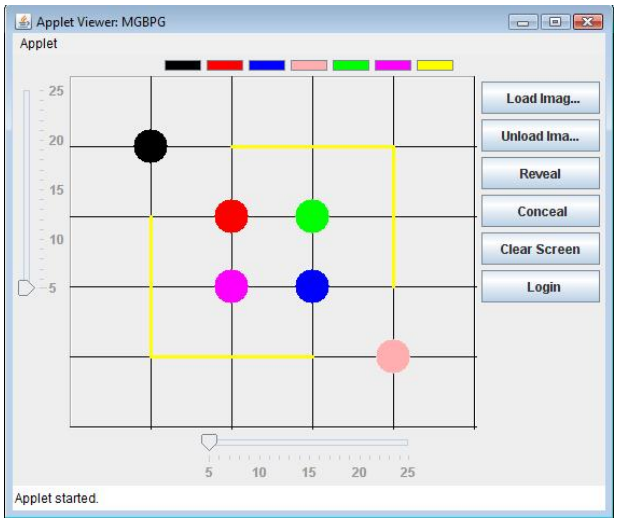

Fig. 2 MGBPG GUI

MGBPG uses the same access function as in Pass-Go and BPG schemes. The dot and line indicators work the same way as they were in both of the above mentioned schemes. As in general, a dot indicator will only appear when one intersection is selected (or clicked) whereas a line indicator only will appear when two or more intersections are touched continuously [20]. As in the BPG scheme, the MGBPG scheme does use invariable indicators to acknowledge the passwords and the passwords are then encoded as a sequence of intersections which is represented by the two-

dimensional coordinate pairs. Besides, the MGBPG scheme also provides an option to load and unload a user preference background image together with the reveal and conceal indicators functions as in BPG scheme.

The main difference between the MGBPG scheme with the BPG scheme is that the MGBPG's background can be superimposed with an image which can be selected by the users. At the same time, an extra grid line scaling function has been added to ease users in remembering their passwords better in such a way that they are able to locate and remember the starting point and the shape of their password at a specific part of the background image more precisely by using the grid line scaling (please refer to Figure 3, 4 and 5).

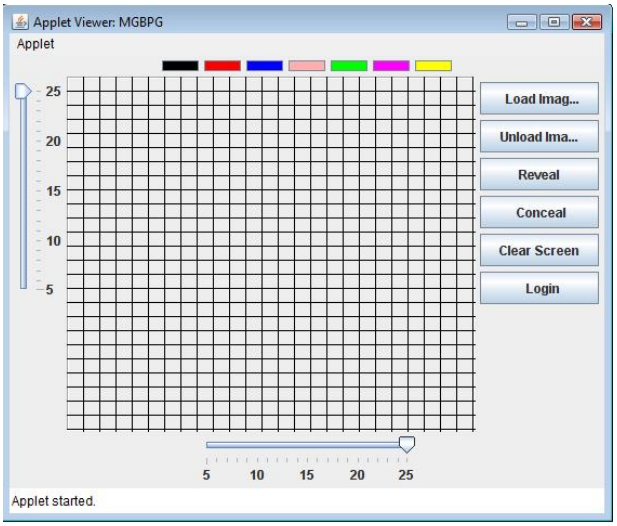

Fig. 3 MGBPG Grid Line Scaling Without Background Image

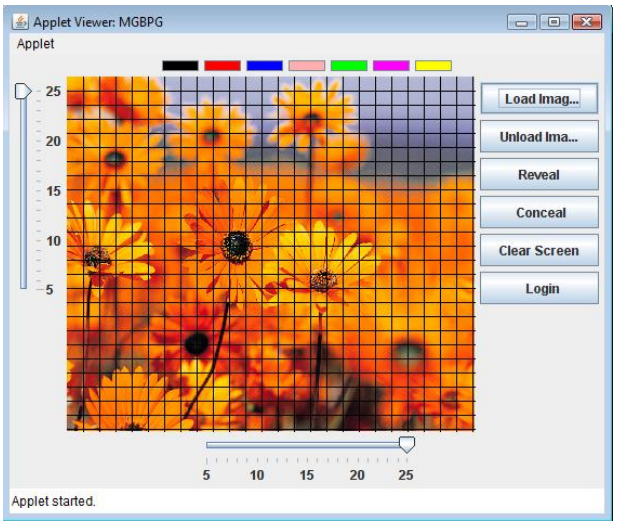

Fig. 4 MGBPG Grid Line Scaling With Background Image

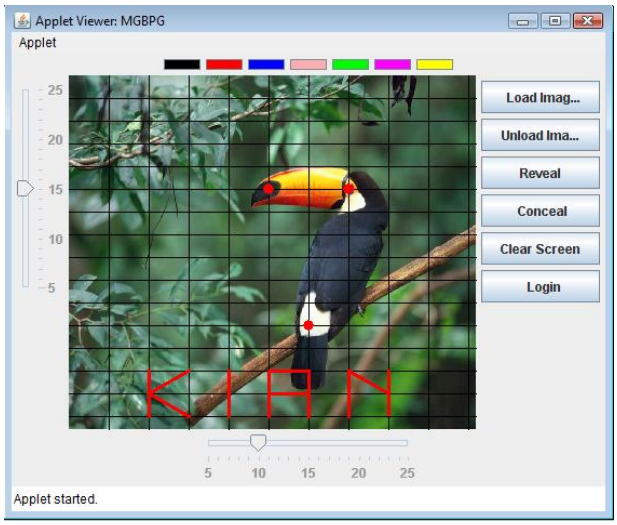

Fig. 5 An Instance Password Used By A User In the MGBPG Scheme

There are two scroll bars which used to control the grid line scaling of the MGBPG scheme. Due to the significant indicator size of 0.3×d radius (the significant indicator size can be obtained from [20]), an end user can only manipulate the grid lines up to the scale of 25 lines each (please refer to Figure 6). When the grid line has been scaled more than 25 lines (either vertically or horizontally), the indicators which are selected by the user will potentially overlapped. When an overlapping of the indicators has arisen, the user might have difficulty in identifying the correct password due to the poor vision and the messy GUI display of the system.

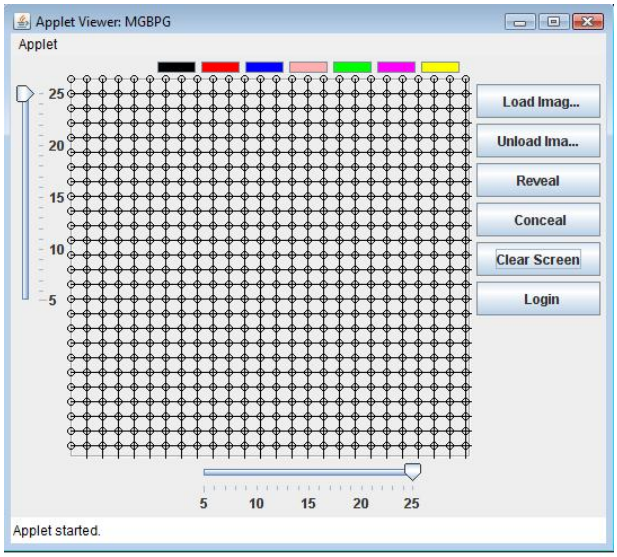

Fig. 6 Dot Indicator in Maximum Scaling

Instead of having to remember the coordinate pairs of their passwords, the users can now

remembering their passwords better by recalling back which part of the background image and the specific grid coordinate scale that they had clicked or drawn.

In term of authentication, a user is still required to identify the correct color code together with the correct sequence order of the indicators which have been set by the user before he or she can gain access into the system. Figure 7 and 8 show the MGBPG scheme password authentication processes.

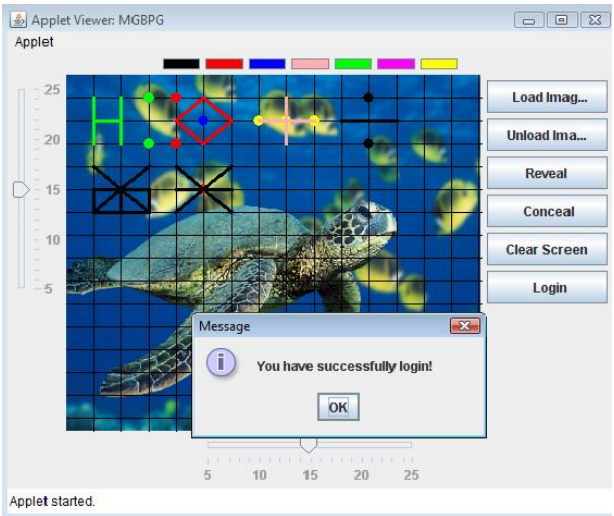

Fig. 7 MGBPG: Password Authentication

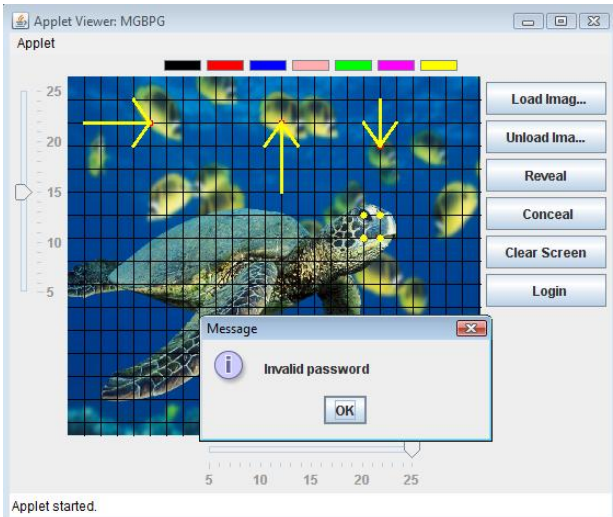

Fig. 8 MGBPG: Invalid Password Authentication

5 Analysis and Preliminary Result

An in depth review have been carried out by [20] in comparing the BPG scheme over the other GPS schemes. Due to the fact that the MGBPG scheme is modeled mostly based on the BPG scheme, the MGBPG scheme should be able to address the drawbacks and the security threats of other GPS schemes which have been mentioned in [20].

As an illustration, the major drawback of Blonder scheme is users cannot click arbitrarily on the background. To address the issue, the MGBPG scheme enable users to click on the intersection points more easily and more accurately with the help of the background image together with the grid line scaling functions.

As compared to Passfaces™, the unpleasant process due to the dislike of faces and face-blind (a disease which affects a person's ability to tell faces apart) [21] issues which existed in Passfaces™ scheme will not occur in MGBPG scheme because the MGBPG scheme enable the users to select and personalize their background image as well as their convenience grid line scale.

According to [20], Déjà Vu [22] scheme which is designed using non-describable abstract images is vulnerable to brute force attack due to the password space of Déjà Vu scheme (which is only 53,130) that is smaller than the password space of the textual passwords. Compared with Déjà Vu scheme, the memorable password space of MGBPG scheme is much larger due to its capability of enabling users to select different indicator types and grid line scaling. Hence, it is much harder for a brute force attack to be launched towards MGBPG users due to the above mentioned functions.

Fault tolerance has become the major issue In PassPoints scheme. As said by [20], most of the users still had difficulty in identifying their password more precisely even after quite some time of practicing using the PassPoints scheme. Besides, users of the PassPoints scheme also faced problem in remembering and identifying their passwords slowly due to uncertainties about their clicking points. In order to alleviate the user from clicking outside the tolerance points, the MGBPG scheme has enabled users to select their preference background image and the grid line scaling. Moreover, the MGBPG scheme has the enable visible sensitive area feature that makes it possible for a user to see exactly the process of his or her password selection. However, the user has to bear

the consequences for a shoulder surfing attack if the enable visible sensitive area feature is activated.

Draw a Secret (DAS) scheme has introduced additional tasks for users to memorize and to input their password due to the security issue [20]. Moreover, is it very challenging for a user to draw a diagonal line as a password in the DAS scheme due to its GUI design. If a user has input or drawn a password which is close to the grid lines or intersections, the DAS scheme may not be able to distinguish which cell the user is choosing. As a result, the user might get frustrated if he or she failed to login consecutively. Hence, we have included the feature of personalizing a background image which the user is familiar with as well as the grid line scaling functions that help the user to memorize their passwords position easier and better in the MGBPG scheme. Moreover, a user can draw a shape more freely in the MGBPG scheme when the cell approach has been replaced with an intersection approach in drawing diagonal lines.

As stated earlier, the development of the MGBPG scheme was inspired by Multi-Grid DAS, Pass-Go, and BPG schemes. As compared to Multi-Grid DAS and Pass-Go schemes, the feature of having background image in MGBPG scheme manages to help users to remember and memorize their passwords better. Evidence can be obtained at [20] since MGBPG scheme is mainly modeled from BPG scheme. Moreover, the MGBPG scheme is endowed with the grid line scaling function which will manage to help users locate and remember the starting point and the shape of their password at a specific part of the background image. The grid line scaling feature in MGBPG scheme also help in advancing the BPG scheme the same way as in Multi-Grid DAS and Pass-Go schemes by improving the memorability issue in such a way that users are able to remember and memorize their passwords better.

In term of security threats, the feature of invisible disguising indicators which has been implemented in MGBPG is able to prevent shoulder surfing attack. Users are able to input one or more disguising dot or line indicators at random positions without having them being shown. With this feature, an attacker is unable to recognize the users' passwords although shoulder surfing attack.

According to [19], a password authentication protocol can stand a guessing attack only if attackers cannot verify their guessing. In the case of brute force attack, the MGBPG scheme has memorable password space which is much larger compared with other schemes except compared to the BPG scheme 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 and MGBPG users. In addition to this, as compared to DAS and Pass-Go schemes, the MGBPG scheme (an enhanced version of BPG scheme) does offer significant resistance to symmetric graphical dictionary attacks (a threat suggested by Thorpe and Van Oorschot [23, 24]) [20]. The above mentioned proof can be obtained from [25].

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 with MGBPG scheme, 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. The above statement can be proven when the MGBPG users only required verifying their passwords by clicking on the intersection points with the guidance of their preference image background and the grid line scaling instead of typing out the numeric values and alphabet characters. As a result, the usual way which was used by phishing attackers to capture the users' information will not work for MGBPG users. Moreover, to identify the correct color code and the sequence of the indicators which is used by a user in this scheme will be a challenge for the phishing attackers.

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 [20]. The password authentication method by identifying the correct color code to be used and clicking on the correct sequence of the intersection points instead of typing out the textual passwords in the MGPBG scheme has helped to prevent the pharmers from being able to capture the users' information. Furthermore, the password space of the MGBPG scheme is much larger than the textual passwords, thus it is difficult for a graphical dictionary attack or guess attack to occur as well.

6 Summary and Research Perspective

We have presented a new graphical password scheme and shown that it keeps most of the advantages of the BPG scheme and offers better usability and memorability to the other GPS schemes after reviewing, analyzing and comparing several graphical password system algorithms according to its strengths and weaknesses in cooperate with its security threats.

As similar to the BPG scheme, the performance of the MGBGP scheme is not affected by the enhanced features of the background image and the grid line scaling functions due to the fact that there is no extra processing power and storage needed for the scheme to store and retrieve the background image which was selected by a user. Moreover, the MGBGP scheme manages to perform real time pre-processing by using Java Applet platform as in generating the grid line scaling and the indicators identification before the actual authentication process was taken place.

Compared to the other GPS schemes, the MGBPG scheme manages to minimize the memorability issue by enabling each user to personalize their background image and the grid line scaling. However, the issue of finding a balance in between a memorable password and a higher security level of password usage is still the biggest challenge for the MGBPG scheme. In future, we still believe in improvising alternative schemes especially in modeling the memorability of passwords to a higher level structure as compared to the current models or GPS schemes.

7 Acknowledgment

We would like to thank Dr. Goh Chong Tien for proof reading and giving us feedback on the paper and Kianoush Farhat for enhancing the GUI of the MGBPG scheme.

References:

[1] Wikipedia, Graphical Passwords, available at: *http://en.wikipedia.org/wiki/Graphical_passwords*, last access date: 2 Dec 2007.

[2] The Graphical Passwords Project Funded by the NSF CyberTrust Program, available at: *http://clam.rutgers.edu/~birget/grPssw/index.html*, last access date: 2 Dec 2007.

[3] Birget, J.C., Hong, D., and Memon, N, Robust discretization, with an application to graphical passwords, *IEEE Transactions on Information Forensics and Security*, 1(3), pp.395-399, 2006.

[4] Passfaces White Paper, The science behind passfaces, available at: *http://www.realuser.com/published/The%20Science%20Behind%20Passfaces.pdf*, last access date: 30 Nov 2007.

[5] Brostoff, S. and Sasse, M.A., Are Passfaces more usable than passwords: A field trial investigation. In McDonald S., et al. (Eds.), People and Computers XIV - Usability or Else, *Proceedings of HCI 2000*, Springer, pp. 405-424, 2000.

[6] Brown, A. S., Bracken, E., Zoccoli, S. and Douglas, K., Generating and remembering passwords, *Applied Cognitive Psychology*, 18, pp. 641-651, 2004.

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

[8] The Rutgers Scholar, An Electronic Bulletin of Undergraduate Research, available at: *http://rutgersscholar.rutgers.edu/volume04/sobrbirg/sobrbirg.htm*, last access date: 2 Dec 2007.

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

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

[11] Jermyn, I., Mayer, A., Monrose, F., Reiter, M. K., and Rubin, A. D., The Design and Analysis of Graphical Passwords, In *Proceedings of the 8th USENIX Security Symposium*, 1999.

[12] Chalkias, K., Alexiadis, A., Stephanides, G., A Multi-Grid Graphical Password Scheme, In *Proceedings of the 6th International Conference on Artificial Intelligence and Digital Communications (AIDC)*, Thessaloniki, Greece, 2006.

[13] A. De Angelia, L. Coventry, G.I. Johnson and M. Coutts, Usability and user authentication: Pictorial passwords vs. pin. In: P.T. McCabe,

Editor, *Contemporary Ergonomics 2003*, Taylor & Francis, London, pp. 253–258, 2003.

[14] A. De Angelia, L. Coventry, G.I. Johnson and K. Renaud, Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems, *International Journal of Human-Computer Studies*, Vol 63, Issues 1-2, pp. 128-152, 2005.

[15] P. Dunphy and J. Yan, Do Background Images Improve "Draw a Secret", *Proceedings of the 14th ACM conference on Computer and communications security*, Session: Authentication and passwords, Alexandria, Virginia, USA, pp. 36-47, 2007.

[16] S. Chakrabarti, G.V. Landon, and M. Singhal, Graphical Passwords: Drawing a Secret with Rotation as a New Degree of Freedom, *The Fourth IASTED Asian Conference on Communication Systems and Networks (AsiaCSN 2007)*, pp. 561-173, 2007.

[17] 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.

[18] 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.

[19] 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.

[20] L. Y. Por, X. T. Lim, F. Kianoush, 2008, Background Pass-Go (BPG), a New Approach for GPS, *The 12th WSEAS International Conference on COMPUTERS (part of the 12th WSEAS CSCC Multiconference)*, Heraklion, Crete Island, Greece.

[21] 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.

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

[23] 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.

[24] 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.

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