Issues, Threats and Future Trend for GSP

L. Y. POR\textsuperscript{1}, X. T. LIM\textsuperscript{2}

Faculty of Computer Science and Information Technology,
University of Malaya,
50603, Kuala Lumpur,
MALAYSIA

Abstract: Computer security depends largely on passwords to authenticate human users during the process of gaining access to secure systems. However, users have difficulty remembering passwords most of the time if they choose a secure password. This is because secure passwords usually consist of passwords that are long and random. Therefore, they tend to choose short and insecure passwords. The tendency of choosing insecure passwords has led to many security problems. Graphical passwords are an alternative to alpha-numeric passwords in which users only have to click on images in order to authenticate themselves rather than type alpha-numeric strings. The purposes of this paper are to do classification of graphical passwords system (GPS) and identification of future research area for researchers. In this paper, we attempt to identify a number of threats to the networked computer systems, do research on 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. We highlight a few aspects which needs to be improved for the future new approach of GPS in order to overcome the shortages of the previous GPS methods which have been studied.

Key-Words: GPS, Graphical Password System, Password, Authentication, Verification, Threat.

1 Introduction

Because of the increasing threats to networked computer systems, there is a great need for improving the security level. Passwords are the most commonly used method to authenticate human users to gain 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 different types of threats, the alpha-numeric passwords are not efficient and secured enough to fully protect the networked computer systems 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” problem, 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 for login 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
2 GPS Security Threats

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 attempt 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 intercepts 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 GPS Evolution and Issues

Figure 1 shows the evolution of GPS methods. In general, the GPS methods can be categorized into
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. 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 produces a commercial product named Passfaces™ that uses the idea of multiple-image schemes in year 2000.

To create a password in Passfaces, a user is requires 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 included 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 only authorized by the system if he or she successfully chosen 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.

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 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 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 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 Jermy 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 advantages 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 becomes 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 has been 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 an 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.

4 Summary and Research Perspective
After analyzing and comparing each graphical password system algorithm, the strengths and weaknesses in cooperate with its threats of each algorithm has been identified and presented.

Usability and security are two main concerns in developing a better GPS algorithm. From the viewpoint of usability, we should put more efforts in determining the effect of the particular image used on success with graphical passwords, studying users’ speed in skilled performance, and discovering what kind of insecure password practices users invent for graphical passwords. There is also potential for future research in increasing the security level of GPS because research on representing or storing images in a secure manner is important.

For future work we should try to explore more alternative schemes for modeling the memorability of passwords that we hope will capture their high-level structure more intuitively than our current models. Finding a balance in between a memorable password and a higher security level of password usage will become a challenge.

5 Acknowledgement
We would like to thank Dr. Omar Zakaria from Faculty of Computer Science & Information Technology, University of Malaya, Malaysia, for giving us feedback about this paper.

References:


