Journal of Theoretical and Applied Information Technology
20th August 2014. Vol. 66 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

MEMORABILITY RATES OF GRAPHICAL PASSWORD SCHEMES

[1]OBASAN ADEBOLA OLUKAYODE, [2]NORAFIDA ITHNIN, [3]OLUMIDE SIMEON OGUNNUSI
Information Assurance and Security Research Group,
Dept. of Computer System & Communication
Faculty of Computing, Universiti Teknologi Malaysia, Malaysia
Skudai, 81310 Johor, Malaysia
E-mail: [1]aolukay@yahoo.com, [2]afida@utm.my, [3]soolumide2@live.utm.my

ABSTRACT

Passwords authentication has become a widely recognized element of computer security for confirming users' identity before access can be granted or repudiated to an intended information contents or applications of the system. Graphical password schemes are a login option that use images instead of alphanumeric strings for the purpose of user authentication. This alternative means of authentication is mainly designed to achieve good memorability and secutity of any choosen passwords based on widely known superiority effect of images over random strings. This paper provides a comprehensive survey of graphical password schemes and reports a memorability comparison between them. It also highlights how different memory tasks affect the graphical passwords and the relationship between them.

Keywords: *Graphical Password, Authentication, Memorability, Memory Tasks*

1. INTRODUCTION

Information systems and other mobile devices are taking over all our day-to-day activities being banking, accounting and others, as such they require some measures of control and protection to ensure reliability, integrity and other security goals. In order to achieve reasonable level of protection, username-password methods have been widely used as method of choice for identifying, authenticating and authorizing users by many banks, government and corporate bodies and even all websites on the internet [1] . The user identification is employed to identify a user to the system while the authentication proves user's claimed identity as being right or wrong depending on username and corresponding password. In order to complete used authentication process, authorization deals with the users' right to access resources ones they are authenticated. Text-based password method has been widely used as a means to restrict access of useful information to the authorized users alone both within a computer system setup or worldwide networked computers.

However, it is popularly known that the conventional passwords authentication has some limitations which are bone out of human memory capabilities[2] . There has been tremendous interest in recent years in the effort to improve password memorability. This is a worthwhile endeavor because memorability problem is the root cause of security flaws from time immemorial. This is because users circumvent security rules in order for them to have a memorable passwords not minding the security implications. Even, when they try to balance the two standards on their own, they are still limited by the natural memory capabilities or loads which make many people to either forget their very secure passwords or use very predictable passwords that are vulnerable to attacks [3, 4]. For these reasons, service providers adopt all manners of features to ease and complement memory requirements for secure passwords without sacrificing security with the help of pictures on the premise that human . Studies focusing on password memorability are large in number but each of them gives cause for improvement. Our study will be mostly directed to graphical passwords This section is focused on the study of variety of memorability tests conducted by different authors. The self-study conducted by Ebbinghaus [5], cited in [6] : Brostoff was made to describe a forgetting curve for nonsense syllables measured by savings method. The curve shows rapid drop at the beginning and becomes progressively slower with respect to time. Results show that after 5 days, approximately only 25% savings are made and the overall memorability rate of the study is about 41%. In the pilot study conducted by Werner and his colleague to

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

investigate memorability of verbal materials [7] ,385 university students were gathered for the study. The results yield better long-term performance when compared with conventional alphanumeric passwords and the memorability rate is about 64.5% memorability rate. The memorability evaluation of a stroke-based authentication system called PassShapes [4] developed by Roman and Alexander showed an improvement. They conducted three user studies where 52 participants were involved to prove that the PassShapes method can be used as a means for enhancing password memorability. The participants were randomly assigned to 3 groups for the experiment. The participants' average age was 34.5 years, ranging between 22 and 63 years of age. The gender ratio of the subjects was 46% female to 54% male. Each of the three groups had almost the same demographic data which includes age, sex, and education. Three retention tests were conducted for each study condition. Immediately after the learning phase, the first test was taken, both PIN and PassShapes with repeated drawing study groups had 100% memorability rate each, while the remaining one group had about 79%. The second retention test was taken 5 days later and results showed about 94% memorability rate for PIN group , still followed by PassShapes with repeated drawing group which had 76% , while PassShapes group which is the least had 68% memorability rates. The last retention test was taken exactly 15 days after the first test. The results indicated that PassShapes with the repeated drawing group had the best result where over 94% was obtained as the memorability rate for the group. The PIN group had over 81% while PassShapes group had over 63% memorability rate. Therefore, the overall memorability rate for PassShapes with repeated drawing group is computed as 90.19% and PassShapes group is 70.18% while that of PIN is 91.7%. The results revealed that the PassShapes system if combined with the repeated drawing strategy showed a good memorability rate.

Furthermore, another comparative study conducted by Dimitropoulos [8] primarily designed to ascertain the effects of background images on GrIDsure authentication system, in terms of memorability and security of chosen passwords. The study was conducted with 81 university students that were divided into 3 different groups: 1 group without and 2 with different background images for a period of 15 days for 3 retention intervals. The average age of the volunteers was 32 years , ranging between 18 and 54 years. 59% of the participants were male while the remaining 41% of the participants were female. The memorability evaluation showed that London map and room image had 92% and 97% each respectively which made the average password memorability rate of the system to be 94% . This means that the two background images showed significant improvement in password memorability.

The rest contents of this paper is organized as follows. Section 2 is focued on authentication techniques. In section 3, discussion is focused on graphical password security challenges. Section 4 discusses grid-based graphical passwords. In section 5, Image-Based Graphical Password Systems were discussed. Section 6 discusses Memorability and memory tasks reqired for passwords and section 7 concludes the work.

2. AUTHENTICATION TECHNIQUES

The process of proving a level of assurance in the correctness of a claim is called authentication. Authentication is usually of two main types, namely; data origin authentication and user or identity authentication. Data origin authentication provides confidence that the source of a message is correct as claimed. While user authentication is process of identifying an individual, usually based on a alphanumeric username and password. User authentication is a very important part of security, in addition to confidentiality and integrity, for information systems that allow remote access over unreliable public networks like the Internet. The goal of an authentication protocol is to provide the communicating parties with some assurance that they know each other's true identities [9].Consequently, a remote password authentication scheme authenticates the legitimacy of users over an insecure channel, where the password is often regarded as a secret shared between the remote system and the user. Using the on knowledge of the secret (password), a user can use it to create and send a valid login message to a remote system to gain the right to access. Meanwhile, the remote system also uses the shared password to check the validity of the login message and authenticate the user.

There are four different techniques to establish correctness of a user's identity claim by the authentication system. These include:

- Something you are (static biometrics): This involves use of some unique physical characteristic such as fingerprints, facial

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

scans, iris and behavioral trend posed by the user to distinguish him or she

- Something an entity has (tokens based) Authentication with this factor is done based on device owned or possessed by the user that can help to gain access to a specific resource of a remote site for a time period. Examples of token include a National or School ID card, Smart Cards, a driver's license, credit card to mention a few
- Where an entity is at the time of authentication (location-based authentication) Location information can be used to determine if a user is attempting to authenticate from an approved location.
- Something an entity can recall correctly (such as PIN, Passwords) at the time authentication

3. GRAPHICAL PASSWORD SECURITY CHALLENGES

The primary goal of every reliable authentication system is ability to provide adequate security for access into intended applications without hitches. Graphical password authentication has been used to provide purpose. However, despite being a widely known alternative to conventional surname/alphanumeric password, the scheme is still vulnerable to some treats. This is a course for concern because the effects could be serious and alarming if they are not identified and combated against with necessary measures to manage the treats. For this reason, it is expected that a proposed system should be evaluated against common attacks like spyware, keyboard logging, phishing and Pharming, Man-In-The-Middle (MITM), Man-In-The-Browse (MITB), shoulder surfing, brute force in order to determine if it provide adequate security requirement. The following subsections offer discussions on these attacks.

In computer security spyware is one of serious threats. It includes a malware installed on computer systems to collect information about users without their awareness in order to compromise their privacy [10]. Personal information may include user logins and bank or credit account information. Besides, they can change computer settings to course system malfunctions like slow Internet connection speeds, un-authorized changes in browser settings, or changes to software settings and other undesirable actions.

Keyboard logging software is a form of spyware which may be installed by an attacker to record all the keystrokes character input as they are being typed by the users and latter used for malicious purpose to harm the user [11]. Key logging is done in such a manner that the user of the keyboard is unaware that their actions are being monitored.

Phishing is attempting to acquire information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication . Communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public. Phishing emails may contain links to websites that are infected with malware. Phishing is typically carried out by e-mail spoofing or instance messaging and it often directs users to enter details at a fake website that appears almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users and exploits the poor usability of current web security technologies [11].

The man-in-the-middle is a form of active eavesdropping in which the attacker makes independent connections with two communicating parties (the victims) and exchanges messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker [12]. The attacker must be able to intercept all messages going between the two victims and inject new ones. A man-in-the-middle attack can succeed only when the attacker can impersonate each endpoint to the satisfaction of the other.

Man-In-The-Browser (MITB) is a form of Internet threat related to Man-In-The-Middle (MITM) [13], is a proxy Trojan horse that infects a web browser by taking the advantage of vulnerabilities in browser security to modify web pages, modify transaction content or insert additional transactions, all in a completely covert fashion invisible to both the user and host wed application. A MITB attack will be successful irrespective of whether security mechanisms such as SSL/PKI and/or two or three-factor Authentication solutions are in place. A MITB attack may be countered by utilizing out-of-band transaction verification, although SMS verification can be defeated by Man-In-The-Mobile (MITMo) malware infection on the mobile phone.

Shoulder surfing refers to using direct observation techniques [14] , such as looking over someone's shoulder, to get information or at a distance with binoculars or other vision enhancing devices to observe data entry. It is commonly used to obtain passwords, PINs, security codes and similar data. Shoulder surfing is particularly effective in crowded places because it is relatively

Journal of Theoretical and Applied Information Technology
20th August 2014. Vol. 66 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

easy to observe someone as they enter their PIN at an automated teller machine or a POS terminal and at other public places like university libraries, or airport kiosks.

4. GRID-BASED GRAPHICAL PASSWORD SYSTEMS

In a grid-based graphical system, user typically draws and reproduces their password on a grid to verify its identity [15] . This approach is alphabet independent and as such making it equally accessible for users of any language .These systems exist in different forms as detailed in the following subdivisions.

4.1. Drawing-A-Secret

Draw-A-Secret (DAS), is a the first of its kinds. It was developed by Jermyn in the year ,1999 as a graphical passwords on grid backgound. This form of graphical password was motivated primarily by PDAs that offer graphical input capabilities [15]. DAS is a purely graphical password selection and input scheme. The scheme replaces in part password strings, with a picture drawn on a 2D, that is (5×5) grid using a stylus mouse as in the following figure 1. Instead of typing a password, this authentication method allows users to use a set of gestures in the selected picture to login [16]. These gestures, which takes into account the shape, the start and end points and the directionality, are limited to tapping and tracing a line or a circle for improving the slow speed of sign-ins by using this method. Suppose that the user is given a stylus with which she can draw a design on this grid. The drawing is then mapped to a sequence of coordinate pairs by listing the cells through which the drawing passes in the order in which it passes through them, with a distinguished coordinate pair inserted in the sequence for each "pen up" event, i.e., whenever the user lifts the stylus from the drawing surface as illustrated in Fig. 1.

Fig. 1. Draw-A-Secret (DAS) (Jermyn et al.,

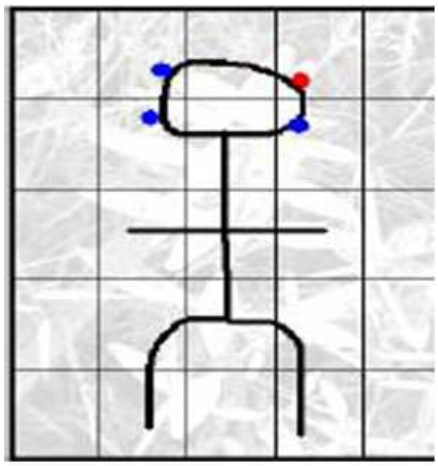

Fig. 2. BDAS Graphical scheme

For authentication, users are asked to recall the picture in the coordinate sequence. Correct coordinate sequence authenticates the user while wrong coordinate sequence (gestures) will always deny a login and it will lock out the system after five unsuccessful attempts, until a text password is provided [17]. Jermyn *et al*. (1999) proved that doodles are harder to crack due to a theoretically much larger number of possible doodle passwords than text passwords.

Up-to-date studies reveal that, there is little or no definite information on either the usability or security of the original DAS recall-based system because it has only been user tested through paper prototypes. This makes it difficult to get very accurate and reliable usability or security analysis of DAS system.

Several studies were conducted on DAS to analyze the memorable password space. In 2002, a user study using "paper prototype" of the system was conducted by Goldberg et al to explore the use of a hand-drawn doodle password ("passdoodle"). The findings of their study show that users could recall all visual elements of the doodle as well as they could recall alphanumeric passwords, but most could not perfectly redraw their selected doodles. Users perceive passdoodles as easier to remember than alphanumeric passwords; however, they prefer whichever authentication method they perceive to be more secure. Also, the results of the study could be used to serve as guidelines for future prototype development.

In 2004, another user study was conducted by Nali and Thorpe on DAS-like scheme where 16 participants were used to draw "doodles " and "logos" 6 each on 6×6 grids . The objective of this study is to focus on usability challenge with the DAS

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

scheme and to establish whether or not user drawings contain the predictable characteristics relating:

- to symmetry, number of composite strokes and
- centering within the grid

It was found in their result that users drawings contain the predictable characteristics relating to symmetry with few pen strokes and users tend to draw within the center of the grid. In other words, this means that DAS users tend to choose weak passwords and their choices would alternately render the scheme less secure in real life.

4.2. Background Draw a Secret Graphical Passwords (BDAS)

In 2007, Dunphy and Yan developed BDAS as an improvement on DAS. This scheme is purely graphical password selection and input scheme where an effort to improve DAS scheme in terms of large password space and memorability an image background was made by Paul Dunphy and Jeff Yan to come up with BDAS. BDAS scheme is exactly the same as DAS except that image background was superimposed over the blank canvas DAS grid to help users remember where they began the drawing that is being used as a password as illustrated in [15] **Fig. 2**. In this way it was showed that people aided with background images tend:

- To set significantly more complicated passwords than their counterparts using the DAS scheme
- To reduce predictable characteristics in DAS passwords such as symmetric and centering within the drawing grid
- To improve the strength of the passwords
- DAS scheme with a background image enhances memorability of the more complex and secure passwords

Therefore, BDAS with a simple enhancement turns out to be a more effective system than DAS for user authentication in terms of enhanced usability and security of graphical passwords.

4.3. Grid Selection

In 2004, a remarkable research was proposed by Thorpe and Van Oorschot to improve the DAS security. The method called Grid Selection with zoom feature which enable the user to select a drawing grid. In this technique, a large scale grid (e.g., 35×35) is offered and a user is required to choose a small drawing grid and then draw the password as illustrated in **Fig. 3**. They had aim of strengthening security and increasing the size of password space of DAS technique . The grid selection technique enables the users to select a drawing grid in which to draw their passwords. The result of their study showed that the item which has the greatest effect on the DAS password space is the number of coordinate pairs otherwise known as strokes. By implication, this means that for a fixed password length, if a few strokes are chosen then the password space will appreciably reduce [18] . The two main limitations are as follows:

- input a password can be a challenge if a user has problem in identifying the correct grid cell used
- it so predictable that most of users will still choose symmetric passwords when using this method

4.4. Qualitative Draw-A-Secret (QDAS)

QDAS scheme is an extention and improvement of DAS. It was developed by Lin et al. in 2007 [19] with the primary aim of solving one possible limitation of graphical passwords which is shoulder surfing [15].

QDAS is resistant to shoulder surfing through the use of a qualitative mapping between user strokes and the password and the use of dynamic grids to both obfuscate attributes of the user secret and encourage them to use different surface realizations of the secret. The use of qualitative spatial relations relaxes the tight constraints on the reconstruction of a secret; allowing a range of deviations from the original .

Moreover, The QDAS drawing-grid is initially similar to a typical DAS grid however each cell in QDAS is explicitly annotated using an integer index. As for DAS, QDAS assumes stylus-based input and the user must create a sequence of strokes that they feel they can remember. Also different techniques of drawing selection must be developed as the proportions of any meaningful drawing are removed by grid transformations. Similar to DAS, there is a one-to-many relationship between an encoding and the corresponding free-form images. QDAS introduces two components that distinguish it from its DAS counterpart:

- qualitative spatial descriptions of strokes; meaning that encoding starts at 6, followed by “down”, “right” and “up”
- the use of dynamic grid transformations as illustrated in **Fig. 4**

The main aims of QDAS are as follows:

Journal of Theoretical and Applied Information Technology
20th August 2014. Vol. 66 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

- to allow users to set strong secrets that do not impose load on long-term memory and
- to be resistant to shoulder surfing.

4.5. Multi-Grid Graphical Password Scheme

Multi-grid scheme was designed by Chalkais et al. in 2006 as a knowledge-based graphical password technique and a good extension or alternative to the Draw-A-Secret scheme (DAS). In this scheme, grid-squares not identical in size and shape as illustrated in Fig 6 where user draws a design on a display grid whose coordinates are used as the password. Multi-grid scheme of the DAS technique is inspired by the fact that users tend to draw lines and shapes on specific areas in the grid .Therefore, the aim of this scheme is to decrease the password centering effect so that user could focus in a single internal grid, so there is more than one area where the password can be centered to. It was also claimed that the approach increases the password strength in user-friendly environment of the scheme.

4.6. Passdoodle Algorithm

Passdoodle is a graphical password scheme which was proposed in the year 2004 by Chistopher [20]. The scheme was based on the idea of hand written designs or words, drawn with a pen onto a sensitive touchable screen as illustrated in figure 7 below. Doodle-based graphical passwords have been proposed as an alternative to traditional passwords in touch screen-enabled devices.

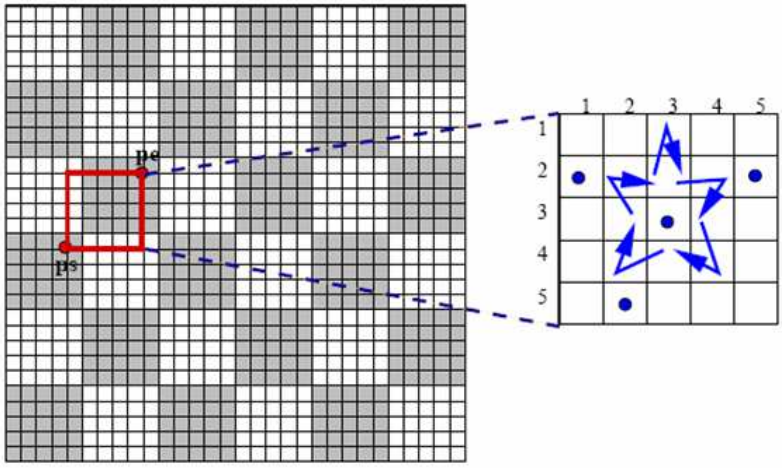

Fig. 3. Grid Selection: Where User Selects A Drawing Grid For The Password .

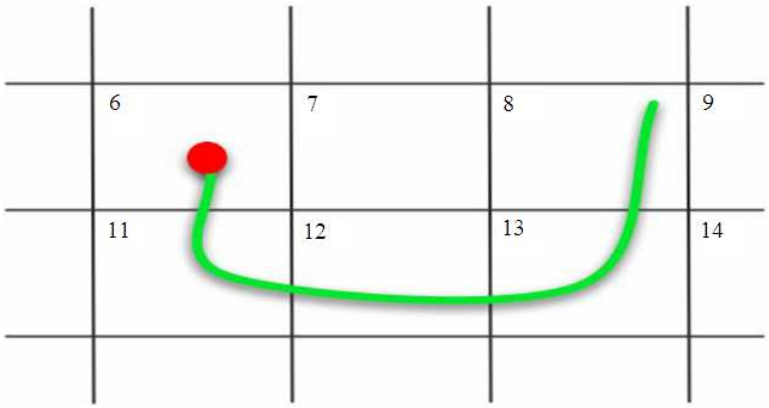

Fig. 4. Qualitative Spatial Descriptions Of Strokes

Journal of Theoretical and Applied Information Technology
20th August 2014. Vol. 66 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

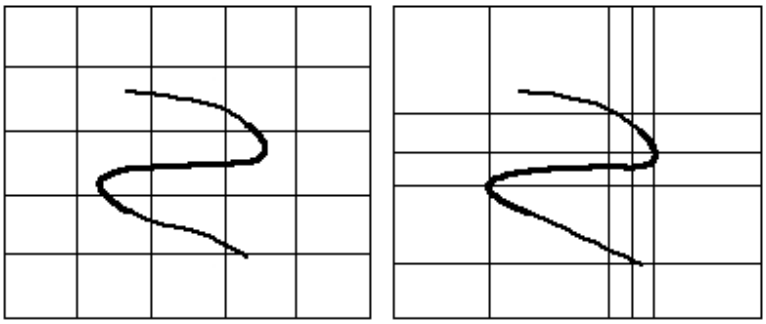

Fig. 5. An Example Of The Dynamic Grids After A Stroke

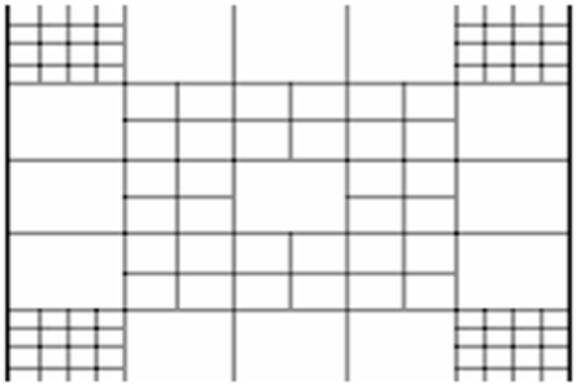

Fig. 6. A Multi-Grid Template

Fig. 7. An Example Of A Passdoodle

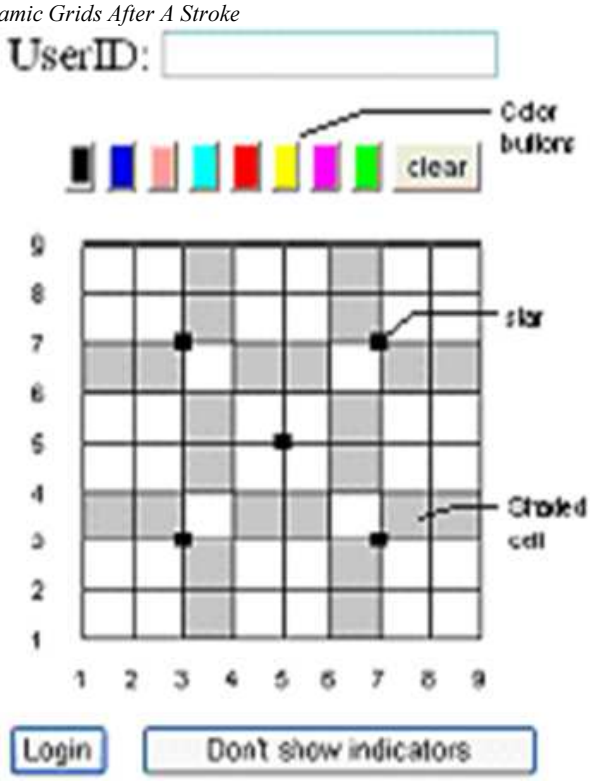

Fig. 8. Pass-Go Scheme

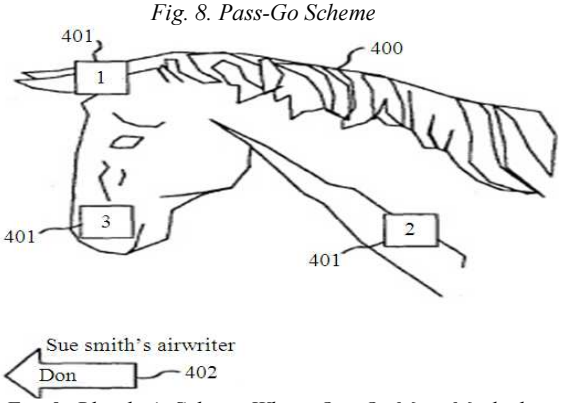

Fig. 9. Blonder's Scheme Where One Or More Marked Areas In An Image Can Be Used For The Password

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Users are validated by tracing a doodle over a touch screen, which is then accepted or rejected by the system. Due to their graphical nature, they are in general easier to remember than strings composed of characters and numbers. It only requires a touch screen, which is now popular in handheld devices, opposed to specific acquisition hardware needed to capture biometric traits such as fingerprints. Within biometrics, signature verification is the most similar trait with respect to doodles. Users are validated by tracing a doodle over a touch screen, which is then accepted or rejected by the system. Due to their graphical nature, they are in general easier to remember than strings composed of characters and numbers.

4.7. Pass-Go

Pass-Go is a graphical password scheme, motivated by an old Chinese game, Go. The scheme was proposed by Tao in 2006 as an improvement of the DAS which is the first grid based graphical algorithm [21]. For user to enter password in this scheme, he selects intersections instead of cells on a grid as in the case of DAS . The dots shows the intersections as illustrated in Fig. 8.

By this difference of usage, the algorithm is referred to as a matrix of intersections, which is different from cell as in the case of DAS's scheme. The use of intersections as against cells allows the user to use password from greater password space (256 bits for the most basic scheme) and provides better usability than DAS counterpart. Also, the size of the grid in the Pass-Go changes to 9 * 9. Pass-Go scheme supports most application environments and input devices, rather than being limited to small mobile devices (PDAs).

However, the limitations of the original scheme are as follows:

- Users suffer error tolerance mechanism because of the interceptions which are invisible areas usable by the user for password are difficult to know. In order, to solve this problem, the sensitive areas must be defined
- The scheme is vulnerable to shoulder surfing attack

Two versions of this scheme inspired by the above stated limitations are designed and implemented by Por n and his colleagues in order to enhance it. It was claimed to be better than the original scheme in terms of usability and security.

5. IMAGE-BASED GRAPHICAL PASSWORD SYSTEMS

5.1 Greg Blonder

In 1996, Blonder pioneered and developed the idea of graphical passwords scheme. In this scheme, the user clicks with a mouse or other device like stylus on a few chosen regions in a single image-based background that appears on the screen as illustrated in **Fig. 9** and a password is a number of clicks on these locations in a particular order. The password space is restricted to the number of predefined locations and no other valid one in the image. Before the user can log in, the user has to click in the same areas again to gain access to a secure system. The image background chosen for this scheme assists the user to remember the likely areas of the password. Ultimately, image background in this scheme makes it more convenient than the unaided conventional alphanumeric text-based passwords. However, the author did not provide any information on user study of the scheme. The following are the major drawback of Blonder's scheme: (a) The scheme has a limited password space because the number of available click regions is small. (b) users can only click pre-processed images as their chosen passwords. (c) In this scheme It is difficult for user to search small spots in a rich image.

By these limitations, it means that the passwords generated from the scheme may not guarantee security because it could be easy for attacker to crack the system with the knowledge on the predetermined locations /areas of the given image.

5.2. Passpoints

This flexible graphical password scheme called Passpoint that can use any kind of image provided by the system or chosen by user was developed in order to overcome some of drawbacks found in Blonder's scheme that was limited to one pre-proccessed image.This authentication scheme was developed by [22]. The scheme is illustrated in figure 10, where a PassPoints password is a number of points, selected by a user in an image that is displayed on the screen [23]. In Passpoints, the image gives a cue but the sequence can be hard to remember because pixels have to be memorized. This scheme is similar to Blonder's scheme for involving click of one image, except that:

- it does not use any pre-processed images or well marked or restricted areas
- Also, it allows arbitrary images to be selected by the user as he or she likes

Journal of Theoretical and Applied Information Technology
20th August 2014. Vol. 66 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

- User has the freedom to click anywhere in an image instead of choosing from some pre-defined locations for a password creation
- It has large password space defined by Y^X where Y represents number of pixels while X is number of pixels selected for password .

A user study was conducted with the help of a prototype of passpoints to evaluate or determine the effectiveness and efficiency of the scheme compared with the conventional text-based password scheme. The results of the evaluation confirmed the memorability of the graphical password.

Moreover, another investigation was conducted in 2005 by Wiedenbeck on the passpoint system to determine the effect of tolerance and image choice on the overall system. With focus on effect of tolerance by using (10×10) and (14 by 14) pixels for this study , the results reveal that the password accurate memory was strongly reduced by almost all the participants when small tolerance (10×10 pixels) was used around the user's password points. Also, with focus on the image choice study where four different but familiar types of images were used. It was reported that no significant differences in performance of the images was obtained.

5.3. Passlogix V-GO

It was reported in the literature that several graphical password schemes based on the Blonder's technique have been developed by Passlogix and Microsoft in large scale. In their schemes, authenticating user has to click on several pre-selected locations of various items in the image in the expected sequence for successful authentication [24]. If the sequence of the images selected for password is not followed, then the authentication would be unsuccessful. In this scheme, the image gives a cue but the sequence could be hard to remember. Invisible boundaries are defined for every item in order to detect whether an item is clicked by mouse. Example of commercial graphical password schemes produced by Pass-logix Inc. includes V-GO.

Fig. 10. Every pixel on an image used in the PassPoints system can be used for the password

Journal of Theoretical and Applied Information Technology
20th August 2014. Vol. 66 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

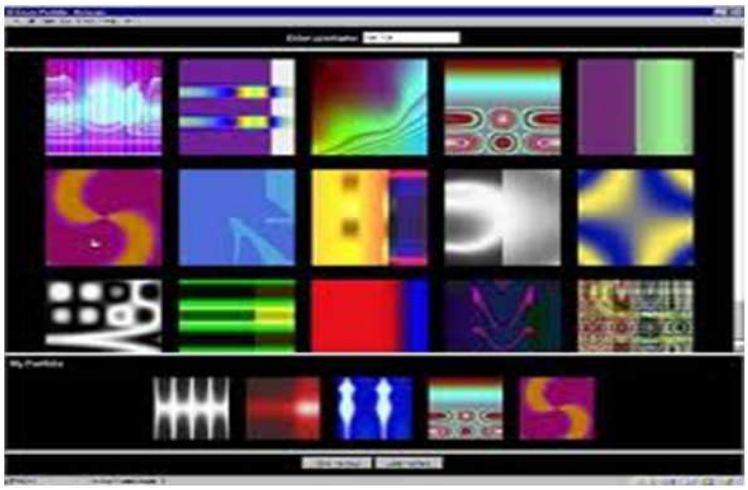

Fig. 11. Deja Vu system, where users select some images out of a greater set of images for authentication

To create a password with V-GO, a user can click on a number of items in a single image in a particular sequence. V-Go system can be used to create a password in various ways. For example, a user can take different food items from the cardboard and place them on a dining table or clean a table, transferring one plate from one table to another, even setting date and time. The major limitations of V-GO system include:

- It has small password space defined by Y^X where Y represents number of marked locations while X is number of locations selected for password. Passlogix password space is less than that of Passpoints
- It could not resist brute force, shoulder surfing and guessing attack
- Also, users with bad vision might find it difficult searching for small spots in any given image
- The sequence of the pre-registered locations selected for passwords can be difficult to remember

5.4. Random Image Selection Deja Vu

In 1999, Dhamiji and Perring proposed Déjà Vu system for the purpose of user authentication based on Hash Visualization technique. Its design involved the use of random or non-describable abstract images, rather than photographs as illustrated in figure 11 (Perrig, 2000). Deja Vu scheme is based on the widely belief that human beings have an excellent memory for images. During registration phase of Déjà Vu scheme, the user selects a specific number of images from a larger set of images presented by a server. The user has to identify the pre-selected images for him or her to be authenticated. The multiple art images of this scheme make it difficult for the users to write down passwords or describe the passwords for others.

In the portfolio creation phase of Deja Vu, the user selects Random Art images from a larger set of the images stored in the server .This scheme has a number of limitations as follows:

- Firstly, the server needs to store a large number of pictures which may have to be transferred over the network, delaying the authentication process
- Secondly, another limitation of this scheme is that the server needs to store the seeds of portfolio images of each user in plaintext
- Thirdly, the process of selecting a set of pictures from picture database can be tedious and time consuming for the user

Also, it has small password space defined by:

- $\binom{K}{N} = \frac{K!}{N!(K-N)!}$ Where K is the total number of images and N represents the number of pre-registered images
- Deja Vu is vulnerable to brute force, guessing and shoulder surfing attacks because the passwords are stored in database in plaintext that is easy to see

For these many limitations, the graphical image-based system is not a good replacement for text-based passwords.

5.5. Passfaces

"Passfaces" is a graphical password authentication technique developed by Real User Corporation. During the registration stage, the users are expected to choose just any four images of human beings faces from a face database as their future password. In the authentication stage,

Journal of Theoretical and Applied Information Technology
20th August 2014. Vol. 66 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

in order to gain access into a Passfaces system, the user sees a grid of nine faces, consisting of one face previously chosen by the user and eight decoy faces as in **Fig. 12**. The user recognizes and clicks anywhere on the known face. This procedure is repeated for several rounds. The user is authenticated if he/she correctly identifies the four faces. The technique is based on the popular assumption that people can recall human faces easier than other pictures. User studies conducted revealed that Passfaces are very memorable over long intervals and equally the comparative studies conducted pointed that Passfaces is easier to remember compared to textual password [25]. It had only a third of the login failure rate of text-based passwords, despite having about a third the frequency of use.

However, I was established that the scheme has some drawbacks as follows:

- The scheme has a small password space defined by: Y^X, where Y denotes total number of faces. While X denotes number of rounds to complete the authentication process. In this case Y = 9 and X = 4, both Y and X are small
- Some faces may not be pleasant for the user
- Some people who are face-blind cannot use it reliably without mistakes
- Another limitation is that the Passfaces based log-in process takes longer time than the text based passwords

5.6. Story Scheme

In the light of the limitations of Passfaces system, a similar scheme was proposed by Davis *et al*. In Davis *et al*.'s scheme otherwise called the story scheme, a user's password is a sequence of k images selected by the user to make a story. A sample collection of images for the story scheme is shown in **Fig**. **13**.

An empirical study was conducted in 2004 by Davis et al compared Passfaces system and story scheme, their result shows that in Passfaces the user's choice was highly influenced by their gender, race and attractiveness of the faces [25]. This implies that attackers might guess passwords based on his knowledge about user's gender, race and interest. This scheme claimed to offer better security because user select random images that not related to them.

Fig. 12. Passfaces™ Login Window Screenshot. During Authentication, The Users Are Presented With Nine Faces In 3×3 Grid, Each Containing One Of The Passfaces And Eight Decoy Faces

6. MEMORABILITY OF GRAPHICAL PASSWORDS

Memory is the ability of the brain to store, retain, and subsequently recall information. Human ability to recall useful information like password varies from one individual to another [26-28] . The ability to recall password correctly and accurately can be partly determined by human memory effectiveness and partly by the design of password authentication system in use. Forgetting is conceived as the distortion of memory or a loss of useful information resource like password between the memory report and the actual event. Password authentication systems involve memory accuracy of the users because of the fact that every user of the secure system needs to memorize one or more passwords and recall them correctly [26] at the time of login in order to gain access to secure network. To address the memory deficiencies of text-based passwords, graphical passwords have been developed on the premise that recognition of pictures was better than

Journal of Theoretical and Applied Information Technology
20th August 2014. Vol. 66 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Fig. 13. Story Graphical Scheme

that of English text for the purpose of authentication. The concept is referred to as the *picture superiority effect* [29] where study was conducted to examine memory capacity and retrieval speed for pictures and for words . Many studies have been made in this regard and the results of different memorability rates of graphical passwords are illustrated in the following table. The table shows three main congnitive activities of memory as they affect the graphical passwords. Different graphical passwords require different memory tasks during their applications . They are used in authentication mechanisms such as graphical passwords illustrated in table 1. The memorability of graphical passwords may be affected by different kinds of memory tasks used by the users. There are three different types of memory tasks. Firstly, pure recall is a process of retrieving information from the memory by

Table 1: Memorability And Memory Tasks Of Graphical Passwords

*Table 1: Memorability and Memory tasks of graphical passwords***schemes**	**Memory Task**			**Recall Rate**	**Type of User Studies**
	Recall	**Cued Recall**	**Recognition**		
DAS	Y	N	N	57-80%	Paper-based
BDAS	N	Y	N	50-80%	Paper prototypes
Passdoodle	Y	N	N	38-46%	Paper and Lab
Qualitative DAS				100%	Paper-based
Pass-Go	Y	N	N	78%	Field study
Grid Selection	Y	N	N	-	None
Multi-Grid	Y	N	N	-	None
Haptic	Y	N	N	86.29-93.89 %	lab
GrIDsure	Y	N		87%	lab
YAGP				87-96%	lab
Passfaces	N	N	Y	83-100%	Field
Déjà vu	N	N	Y	90-100%	Field
Faces	N	N	Y	96%	Field
Story	N	N	Y	85%	Field
Blonder's	N	Y	N	-	None
Passlogix	N	Y	N	-	None
Passpoints	N	Y	N	55-90%	Multi-session

generating correct answer without retrieval cues. Secondly, cued recall is kind of recall in which the retrieval of memory is facilitated by the provision of cues, which are not provided in pure recall. Thirdly, another task of memory is recognition, where the user views stimuli such collection of words or pictures. After a retention interval, the user is shown a grid of words or pictures and indicate whether each item in targets (from the earlier list) from the distracters (items not shown earlier). Figure 14 below, illustrates the ratio of number of items correctly remembered using different memory tasks. The pure recall returns the least correct responses , while recognition recalls the highest[6] [30]

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

.

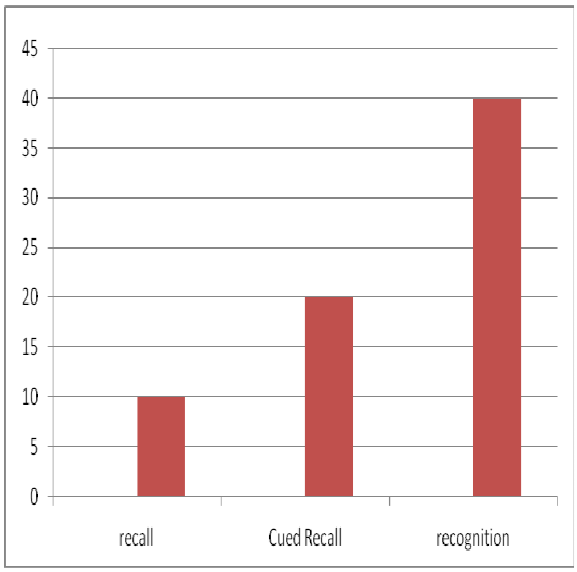

Figure 14:Memory Tasks:Recall, Cued Recall And Recognition Relationship

7. CONCLUSION

Graphical password schemes as alternative means of user authentication is now a popular claim. This is because of the fact that people are good at memorizing graphics
than that of text. Today, we have good number of graphical password schemes available for implementation. In this study, we have conducted a comprehensive survey of existing password techniques in different classifications. Up-to-date study reveals that graphical passwords could be classified into three (3) main categories bases on different backgrounds: Image-based, Grid-based and Hybrid systems. A comparison of some graphical passwords in Table 1 highlighting the memorabity test of each scheme. The study reveals that more researches need to be conducted to have better enhanced schemes in terms of memorability

ACKNOWLEDGEMENT

The authors would like to express their appreciation to Universiti Teknologi Malaysia , (UTM) for providing conducive environment for research. Also, enormous support provided by the members of staff of Faculty of Computing is highly appreciated.

REFERENCES

[1] ADEBOLA, O., et al., *GRAPHICAL PASSWORD SCHEMES DESIGN: ENHANCING MEMORABILITY FEATURES USING AUTOBIOGRAPHICAL MEMORIES.* Journal of Theoretical & Applied Information Technology, 2013. 53(1).

[2] ITHNIN, N. and C.S. WENG, *MEMORABILITY FEATURES OF DRAW-BASED GRAPHICAL PASSWORDS.* Journal of Theoretical & Applied Information Technology, 2013. 53(1).

[3] Polyviou, A., *The impact of interference and frequency of use on the performance of three authentication mechanisms*, 2010, MSc Thesis, University College London, UCL Interaction Centre-UCLIC, London, UK.

[4] Weiss, R. and A. De Luca. *PassShapes: utilizing stroke based authentication to increase password memorability*. in *Proceedings of the 5th Nordic conference on Human-computer interaction: building bridges*. 2008. ACM.

[5] Ebbinghaus, H., *Memory: A contribution to experimental psychology*. 1913: Teachers college, Columbia university.

[6] Brostoff, A., *Im proving passw ord system effectiveness*, 2004, University College London.

[7] Werner, S. and C. Hoover. *Cognitive approaches to password memorability–the possible role of story-based passwords*. in *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*. 2012. SAGE Publications.

[8] Dimitropoulos, L.K., *GrIDsure: Effects of background images on pattern choice, usability and memorability.*

[9] Orhanou, G., et al., *EPS Confidentiality and Integrity mechanisms Algorithmic Approach.* International Journal of Computer Science Issues (IJCSI), 2010. 7(4).

[10] Lehtinen, R., *Computer security basics*. 2011: O'Reilly Media.

[11] Sreenivas, R.S. and R. Anitha, *Detecting keyloggers based on traffic analysis with periodic behaviour.* Network Security, 2011. 2011(7): p. 14-19.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[12] Ding, W., et al., *Research of man-in-the-middle attack in robust security network.* Journal of Computer Applications, 2012. 1: p. 010.

[13] Dougan, T. and K. Curran, *Man in the Browser Attacks.* International Journal of Ambient Computing and Intelligence (IJACI), 2012. 4(1): p. 29-39.

[14] Zakaria, N.H., et al. *Shoulder surfing defence for recall-based graphical passwords*. in *Proceedings of the Seventh Symposium on Usable Privacy and Security*. 2011. ACM.

[15] Tyagi, V.K., S.K. Chowdhary, and N. Garg. *Notice of Violation of IEEE Publication Principles Authentication using graphical password to upgrade security & memorability*. in *Recent Advances in Intelligent Computational Systems (RAICS), 2011 IEEE*. 2011. IEEE.

[16] Zangooei, T., M. Mansoori, and I. Welch. *A hybrid recognition and recall based approach in graphical passwords*. in *Proceedings of the 24th Australian Computer-Human Interaction Conference*. 2012. ACM.

[17] Broenink, R. and S. Drenthen, *Viability and Usability of Drawing-Based Password Systems.* 2012.

[18] FULKAR, A., et al., *A STUDY OF GRAPHICAL PASSWORDS AND VARIOUS GRAPHICAL PASSWORD AUTHENTICATION SCHEMES.* World, 2012. 1(1): p. 04-08.

[19] Vu, K.-P.L., et al., *Improving password security and memorability to protect personal and organizational information.* International Journal of Human-Computer Studies, 2007. 65(8): p. 744-757.

[20] Varenhorst, C., M. Kleek, and L. Rudolph, *Passdoodles: A lightweight authentication method.* Research Science Institute, 2004.

[21] Biddle, R., S. Chiasson, and P.C. Van Oorschot, *Graphical passwords: Learning from the first twelve years.* ACM Computing Surveys (CSUR), 2012. 44(4): p. 19.

[22] Wiedenbeck, S., et al., *PassPoints: Design and longitudinal evaluation of a graphical password system.* International Journal of Human-Computer Studies, 2005. 63(1): p. 102-127.

[23] Chiasson, S., et al., *Persuasive cued click-points: Design, implementation, and evaluation of a knowledge-based authentication mechanism.* Dependable and Secure Computing, IEEE Transactions on, 2012. 9(2): p. 222-235.

[24] Umar, M.S., M.Q. Rafiq, and J.A. Ansari. *Graphical user authentication: A time interval based approach*. in *Signal Processing, Computing and Control (ISPCC), 2012 IEEE International Conference on*. 2012. IEEE.

[25] Towhidi, F., M. Masrom, and A.A. Manaf, *An Enhancement on Passface Graphical Password Authentication.* 2013.

[26] Denning, T., et al. *Exploring implicit memory for painless password recovery*. in *Proceedings of the 2011 annual conference on Human factors in computing systems*. 2011. ACM.

[27] OBASAN ADEBOLA O. , N.I., CHUA SIEW WENG, *MEMORABILITY FEATURES OF DRAW BASED GRAPHICAL PASSWORDS.* Journal of Theoretical and Applied Information Technology, 2013. 54(1): p. 187-197.

[28] OBASAN ADEBOLA O. , N.I., MOHD ZALISHAM JALI ,NICHOLAS AKOSU, *GRAPHICAL PASSWORD SCHEMES DESIGN: ENHANCING MEMORABILITY FEATURES USING AUTOBIOGRAPHICAL MEMORIES*

[29] Journal of Theoretical and Applied Information Technology, 2013. 53(1): p. 124-130.

[30] Standing, L., *Learning 10000 pictures.* The Quarterly Journal of Experimental Psychology, 1973. 25(2): p. 207-222.

[31] Parkin, A.J., *Memory: Phenomena, experiment and theory*. 1993: Psychology Press.