Scientific Research and Essays Vol. 5 (24), pp. 3865-3875, 18 December, 2010
Available online at http://www.academicjournals.org/SRE
ISSN 1992-2248 ©2010 Academic Journals

Full Length Research Paper

A new algorithm on Graphical User Authentication (GUA) based on multi-line grids

Arash Habibi Lashkari[1]*, Abdullah Gani[1], Leila Ghasemi Sabet[2] and Samaneh Farmand[1]

[1]Faculty of Computer Science and Information Technology, University Malaysia (UM), Kuala Lumpur, Malaysia.
[2]Information Technology and Quantitative Science, University Technology MARA (UITM), Shah Alam, Malaysia.

Accepted 25 October, 2010

Today user authentication stands out as one of the most essential areas in information security which has several ways of being implemented. From time in memorial authentication schemes that apply strong text-based passwords have been typically expected to offer some assurance of security. But committing to memory such strong passwords can prove to be quite a daunting task thus forcing users to resort to writing them down on pieces of papers or even storing them onto a computer file. As a means of thwarting such habits, graphical authentication has been proposed as a replacement for text-based authentication. This has been spurred by the fact the humans have a natural inclination to remember images more easily than text. Most Information Communication and Telecommunication (ICT) environments in the last 20 years have tried to implement graphical user authentication schemes. The effectiveness of a graphical password is measured by its level of usability and security. Despite there being many existing algorithms most have failed to achieve both aspects simultaneously. To start with this paper reviews the pure and cued recall-based algorithms graphical password authentication schemes together with their shortcomings and probable attacks. Thereafter a comparative analysis of all Recall-Based algorithms based on attack patterns of graphical user authentication is tabulated. This is then followed by a discussion on the newly proposed algorithm that is based on a multi size grid and its evaluation by an attacker team. Finally, a comparison of the newly proposed algorithm and previous algorithms will be evaluated in a table.

Key words: Recall-based GUA, pure recall-based algorithm, cued recall-based algorithm, graphical password, usability, security, attack patterns.

INTRODUCTION

Only in the last few years has computer and network security been recognized as a technical problem, especially when dealing with user authentication. User authentication typically in form of a password, is a key security process that either allows or denies access to a system or resource depending on the credentials presented. A password comprises of authentication data which is used to control access to resources. The security of a password lies in it being kept secret from unauthorized users while those wishing to gain access use passwords for the system to be able to determine whether to grant or deny them access accordingly.

The use of passwords can be traced back to ancient times when soldiers guarding a location would only exchange shifts only with a person who knew the password. In modern times passwords have been proliferated to a wide range of applications such as controlling access to protect computer operating systems, mobile phones, automated teller machines (ATM), and others. This has necessitated a typical computer user to use several passwords for computer related tasks like logging in to computer accounts, retrieving e-mail from servers, accessing files, databases, networks, web sites, and including reading the morning newspaper online.

Conventional passwords have been used for authentication for a long time due to their many advantages

*Corresponding author. E-mail: a_habibi_l@hotmail.com.

however over time drawbacks such as stolen passwords, forgetting passwords, and weak passwords have frequently compromised security. This has lead to an urgent need for a stronger authentication method that can manage to secure all our applications. Apart from security issues conventional passwords have been known to have usability problems. Thus today, alternative solutions such as graphical authentication have been proposed to resolve security and usability issues.

The motivation behind proposing graphical passwords as alternative solutions to text-based passwords is based on the fact that humans can recall pictures better than text. This has been proven through Psychological studies which have shown that pictures are generally easier to be remembered or recognized than text, especially portrait photos, which are even easier to be remembered than random pictures (Xiaoyuan et al., 2005).

The main drawbacks associated with graphical passwords, come about due to two fundamentals requirements that must be attained:

i. A password should be easy to remember.
ii. A password should be secured.

The original description of Graphical passwords by Blonder (Greg, 1996) states that it is an image that would appear on the screen, and the user would click on a few chosen regions within the image. Given that the correct regions were clicked on, the user would be authenticated. There are two key human factor criteria which make it possible for a person to have the ability to memorize and efficiently input this type of password. The two memorizing ability aspects are:

i. How the user chooses and encodes the password?
ii. What task the user does when retrieving the password?

In a scheme which uses graphical passwords, a user is required to select memorable images. The process of selecting memorable images is dependent on the nature of the process of image and the specific sequence of click locations. In order to support the ability for memorization, images should have meaningful content because meaning for arbitrary things is lacking in most humans.

Literature review

Graphical-based password methods such as recognition and recall-based have been proposed as an alternative to conventional password techniques. The main reason behind this is because graphic pictures are more easily recalled than text. This ease with which graphics are easily recalled has been widely referred to as "Picture superiority effect" by most of researchers (Christopher, 2004). To clearly distinguish these graphical password techniques, most literature regarding graphical password techniques from 1994 till 2009 show that the techniques can be classified into three groups:

1. Recognition-Based Technique: For this technique a user is presented with a collection of images from which they are able to select pictures, icons or symbols. During the authentication process, the user is required to recognize their registration choice from among a set of candidates. Research shows that it is possible for the majority (90%) of users to remember their password after one or two months (Saranga and Dugald, 2008).
2. Pure Recall-Based Technique: For this technique, a user is required to reproduce their password without being given any reminder, hints or gestures. With the ease and convenience of this method one would expect that users would remember their password but just like the drawing of a secret (DAS) (1999) and Qualitative DAS (2007), most users could barely remember their passwords.
3. Cued Recall-Based Technique: This technique is based on a framework of reminders, hints and gestures that are meant to assist the user to reproduce their password or to make a reproduction more accurate. This technique is comparable to the Blonder Algorithm and the Passpoint algorithm.

Pure recall-based algorithms

Several Pure Recall-Based algorithms have been created with varying levels of usability and security features.

Passdoodle

This is a graphical password which is made up of handwritten designs or text that is normally drawn with a stylus onto a touch sensitive screen. According Jermyn et al. (1999) cracking the doodles is harder because they have a theoretically much larger number of possible doodle passwords than text passwords. A sample of a Passdoodle password is shown in Figure1.

Usability wise the Passdoodle is not widely used because it has problems with recognition. What's more the limits of the system are predefined by the length and identifiable features of the doodle. In addition to this only a predetermined amount of computer differentiable doodles can be created and the doodle is the only means of identification. In terms of security maintenance, the system cannot merely authenticate a user who records a very similar doodle, a minimum threshold of likeliness and similarity must be attained. This enhances security by preventing authentication of users who use random

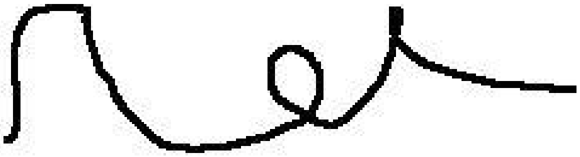

Figure 1. An example of a Passdoodle.

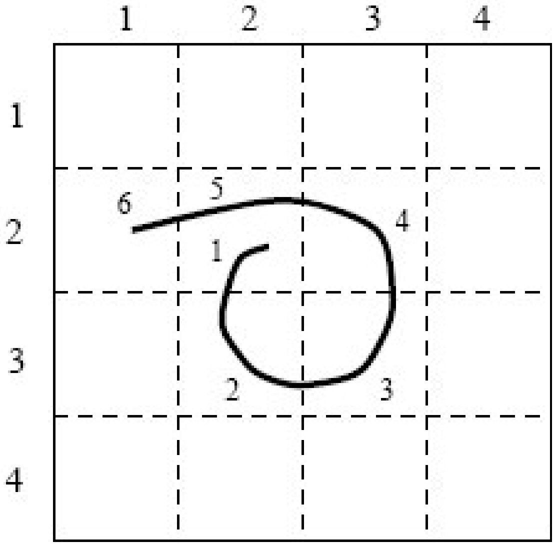

Figure 2. Draw a Secret (DAS) method on a 4*4 Grid.

and obvious guessing.

On the other hand speed and accuracy are still top priorities for the system. Thus a complex recognition design that needs hundreds of training samples and approximately one minute of computation to authenticate does not justify the purpose of the original pervasive design. After careful consideration the proposed system applies a combination of doodle velocity and distribution mapping to recognize and authenticate a doodle (Christopher, 2004).

Goldberg el al (Christopher, 2004) created a Passdoodle algorithm, using a graphical password made up of handwritten designs or text drawn with a stylus onto a touch sensitive screen. The results of their research show that users were able to recall entire doodle images just as accurately as alphanumeric passwords.

Lack(s): Unfortunately as much as the resulting image could be completely and accurately remembered the same users were highly unlikely to recall the order in which they drew a doodle.

In another related research (Karen, 2008) users were more fascinated by doodles drawn by other users, and repeatedly attempted accessing the system using other users' login details simply to see a different set of doodles from theirs.

Draw A Secret (DAS)

This technique, presented in 1999, allowed the user to draw a simple picture onto a 2D grid as shown in Figure 2. The interface consisted of a rectangular grid of size G * G. Each cell in this grid was denoted by discrete rectangular coordinates (x,y). Figure 2 shows the coordinate sequence generated by drawing which is:

(2,2), (3,2), (3,3), (2,3), (2,2), (2,1), (5, 5)

In this method the stroke is considered to be a sequence of cells on the grid which does not contain a pen up event. Thus the password is defined as a sequence of strokes, separated by pen up events. In order to be authenticated, the user is supposed to re-draw the picture by creating the stroke in the exact sequence that was used in the registration phase. In the event that the drawing touches the same grids as well as in the same sequence, then the user is successfully authenticated (Jermyn et al., 1999).

Lack(s): When this method was used in 2002 for the Goldberg survey, it showed that most of the users were unable to remember their stroke order. It also showed that the users deemed text based passwords to be much easier to recall than DAS passwords. Further users are inclined to opt for weak graphical passwords that are inherently vulnerable to the graphical dictionary attack (Paul et al., 2007).

Qualitative DAS (QDAS)

To improve the DAS method, in 2007, the QDAS method in which each stroke is encoded was designed. The raw encoding consists of its starting cell and the sequence of qualitative direction change in the stroke relative to the grid. A direction change is considered when the pen crosses a cell boundary in a direction different from the direction of the cross of the previous cell boundary. The research results indicate that, the image which has a larger area of interest (Hot Spot) could be more useful as a background image (Di et al., 2007). An example of the QDAS is presented in Figure 3.

Lack(s): This model is implemented using dynamic grid transformation so as to conceal the process of creating the password. Although this method could be safer than the original DAS because it prevents shoulder surfing attacks, it has a lot more entropy than the previous DAS. Thus making it even less memorable than the original

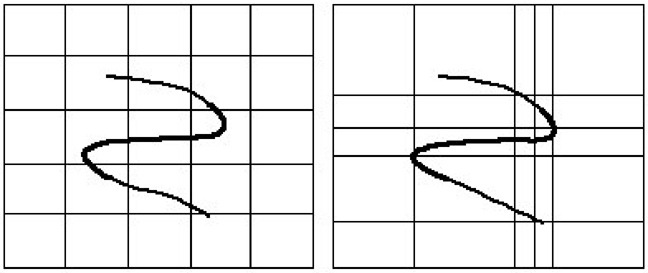

Figure 3. A sample of qualitative DAS algorithm.

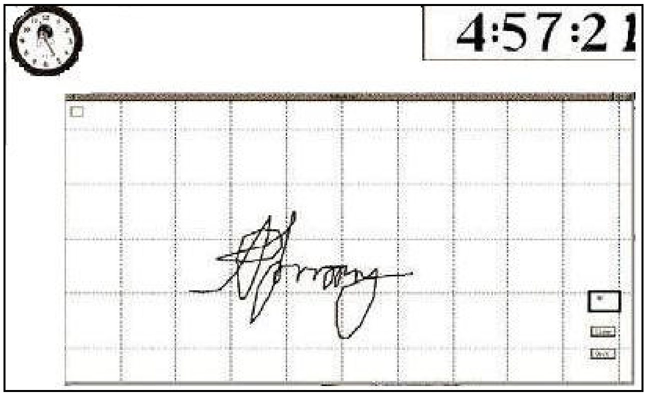

Figure 4. A sample of Syukri algorithm.

one (Di et al., 2007).

Syukri

1. The Syukri algorithm proposes a system where authentication is achieved by the user using a mouse to draw their signature as can be seen in Figure 4 (Di et al., 2007).
2. This technique is made up of two stages, namely, registration and verification. To start with, during theregistration stage the user is requested to draw their signature with a mouse, this is then followed by the system extracting the signature area and either enlarging or scaling-down signatures, and rotating if required, (also known as normalizing). Subsequent to this, the information is stored into the database. The verification stage begins by obtaining the user input, on which it repeats the normalization; thereafter it extracts the parameters of the signature. Basically the system uses geometric average means and a dynamic update of the database for verification purposes. Based on the study (Ali, 2008) undertaken, the rate of successful verification was satisfying. The major benefit to this approach is that not only is there no requirement for memorization of one's signature but counterfeit signatures is difficult to come up with.

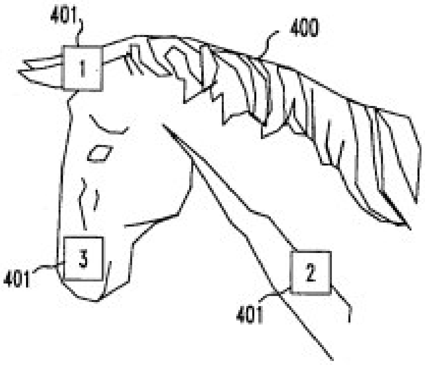

Figure 5. A sample of Blonder method.

Lack(s): However, since a good number of people are unfamiliar with using the mouse as a writing device; the signature can therefore prove to be difficult to draw. To resolve this drawback a pen-like input device could be employed. Since such devices are not extensively used, adding them as new hardware to the current system could turn out to be expensive (Ali, 2008). Although researchers from this study, believe that such a technique can still be more useful on small devices.

Cued recall-based techniques

Also, there are several Pure Recall-Based algorithms created in varying levels of usability and security features.

Blonder

Greg E. Blonder created this method in 1996. To begin with a pre-determined image is presented to the user on a visual display and then the user is supposed tap regions by pointing to one or more predefined locations on the image (in a predetermined order as a way of pointing out his or her authorization to access the resource. According to Blonder this method is secure since it has a million of different regions to pick from. Figure 5 shows a sample of the Blonder password.

Lack(s): The drawback to this scheme was that the amount of predefined click regions was relatively small so the password had to be quite long in order for it to be secure. Apart from this, the use of pre-defined click objects or regions meant that simple, artificial images, for example cartoon-like images, were supposed to be used

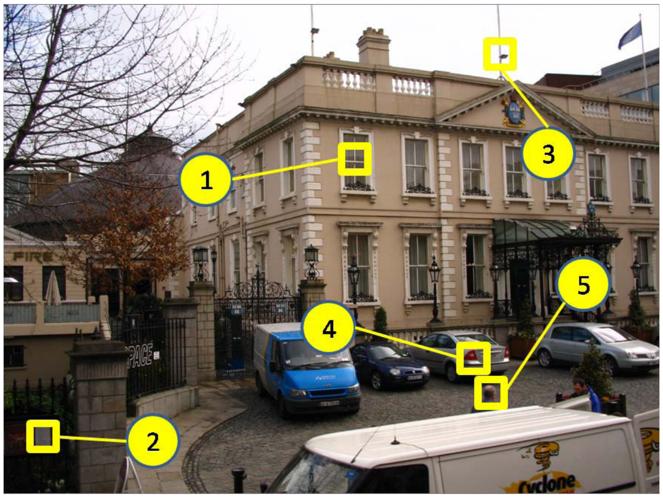

Figure 6. A sample of PassPoint method.

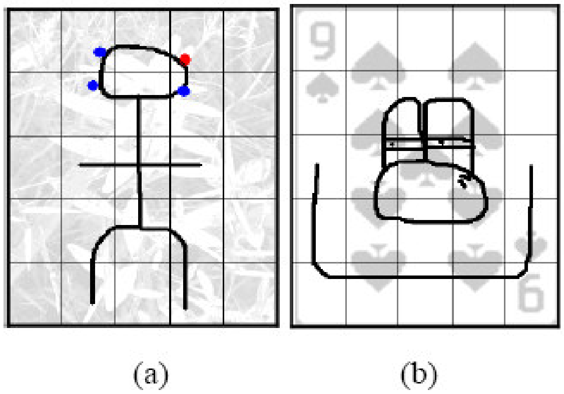

Figure 7. A sample of BDAS algorithm.

in place of complex, real-world scenes (Susan et al., 2005a).

PassPoint

To improve upon the shortcomings of the Blonder Algorithm, in 2005, PassPoint was created Passpoint was able to fill in the gaps left by blonder. In this case the image could be any natural picture or painting as well as rich enough so as to have several possible click points. Apart from this the image is not secret and has no other role other than that of assisting the user to remember the click point. Furthermore it is not as rigid as the blonder algorithm which requires the setting of artificial predefined click regions with well-marked boundaries.

The authentication process involves the user selecting several points on picture in a particular order. When logging in, the user is supposed to click close to the selected click points, within some (adjustable) tolerance distance, for instance within 0.25 cm from the actual click point (Susan et al., 2005b). Figure 6 shows a sample of the PassPoint password.

Lack(s): Studies indicate that when using the PassPoint system users were easily able to quickly create a valid password. They found it much harder to know their passwords compared to alphanumeric users, hence they had to take a lot more trials and more time to complete the process. Comparatively the login time, in this method is longer than that of the alphanumeric method (Susan et al., 2005b).

Background DAS (BDAS)

In order to enhance the original DAS, by adding a background image this method was proposed in 2007. In this method both the background image and the drawing grid can be used to provide a cued recall (Paul et al., 2007). The user begins by following through these three different steps:

1. At the onset the user must have a secret in mind, and then draw it using the point from a given background image.
2. The user’s choice of secret is affected by various characteristic of the image.
3. A mix of the two aforementioned methods.

Figure 7 shows a sample of BDAS algorithm. Lack(s): Research on the BDAS algorithm, regrettably shows that one of the main problems is memory decay after a week or more. As much as users did not have any difficulties in recreating it, within the five-minute test, a week later they could hardly reproduce their previous secret password. In addition to this shoulder-surfing and interference between multiple passwords are issues that need to be taken into consideration for BDAS (Paul et al., 2007).

PassMap

A major drawback to using passwords is that very good passwords are difficult to commit to memory and the ones that are easy to remember are too short and simpleto be secure. All in all studies on human memory indicate that it is quite straightforward to remember landmarks on a well-known journey. As such one can opt to use a map as an alternative. For instance using the map of Europe a user who has never been to Europe before should have no difficulty in remembering that he would like to one day see the Eiffel Tour in Paris, the Big Ben in London and the Kremlin in Moscow and his

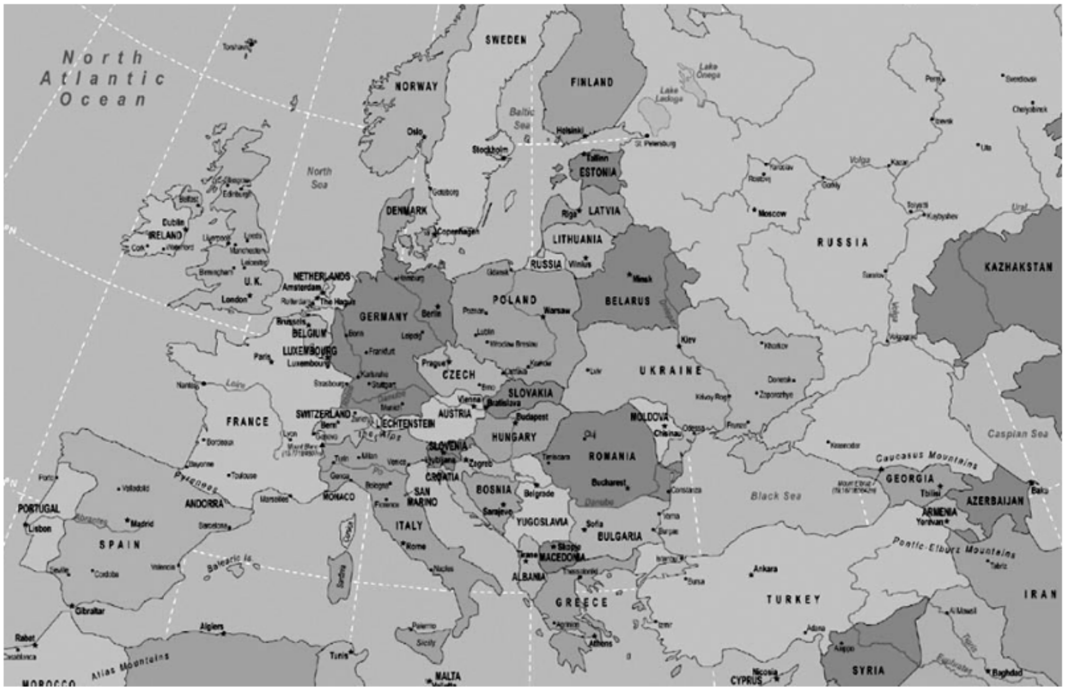

Figure 8. A sample of PassMap method.

PassMap might be to visit all of them one at a time flying in from his hometown (Roman, 2007). Figure 8 shows a sample of the PassMap password.

Lack(s): From Figure 8 it is obvious that the PassMap technology is not very susceptible to "shoulder surfing" attacks. This is due to the fact that the ability to notice a single new edge or the absence of some edge in a large graph requires a high level of concentration. However Brute Force attacks are very likely and one has to consider how good those mechanisms are in terms of how easy to remember the PassMap password is (Roman, 2007).

Passlogix v-Go

Passlogix Inc. is a New York City USA based commercial security company which created a scheme called Passlogix v-Go. It applies a technique which is referred to as “Repeating a sequence of actions” which basically implies that a password is created by following a predefined chronological order. In this scheme, a user has the option of choosing their preferred background images based on the environment, such as the kitchen, bathroom, or bedroom (Figure 9). By clicking and/or dragging on a series of items within that image, a user is able to input their password. In the event that the environment opted for by the user is the kitchen environment, the user can choose to prepare a meal by selecting cooking ingredients, for instance take fast food from fridge and microwave it, select some fruits and wash them in a washbasin and then place them into a clean bowl (Muhammad et al., 2008).

Lack(s): Some of the drawbacks to this scheme are the size of password space which tends to be small and it has limited places for one to take vegetables, fruits or food from and put into, as a result causing the passwords to be somewhat guessable or predictable (Muhammad et al., 2008).

VisKey SFR

A company called SFR from Germany recently commercialized the VisKey scheme which is a recall-based authentication scheme. The creation of a password in this scheme requires the user to tap their spots in sequence (Figure 10) (Muhammad et al., 2008). The VisKey scheme was original purposed for mobile devices such as PDAs.

Lack(s): This scheme’s main drawback is the input tolerance. Pointing to the exact spots on the picture has proven to be quite hard thus Viskey accepts all input within a certain tolerance area around it. It also allows users to set the size of this area in advance. However, some caution related to the input precision needs to be

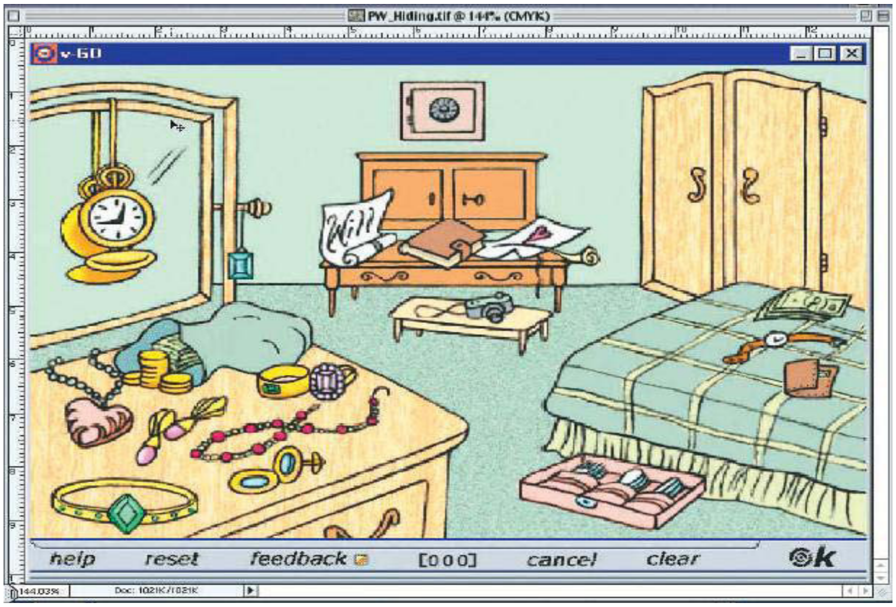

Figure 9. A sample of PassMap method.

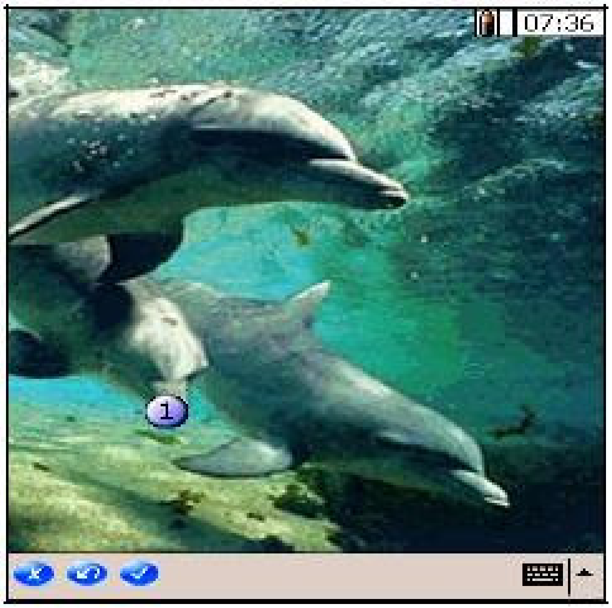

Figure 10. A sample of VisKey SFR method.

taken, since it will directly influence the security and the usability of the password. In order to practically set parameters, a four spot VisKey theoretically provides approximately 1 billion possibilities for defining a password. Unfortunately this is not large enough to prevent off-line attacks from a high-speed computer.

Therefore no less than seven defined spots are required to overcome the likelihood of brute force attacks (Muhammad et al., 2008).

Pass-Go scheme

In 2006, this scheme was created as an enhancement on the DAS algorithm by adding on some extra security features to the advantages of the DAS. This scheme is based on a grid from which users select intersections, instead of cells so the new system refers to a matrix of intersections, rather than cells as in DAS. Since an intersection is actually a point with no area, it would be impossible for a user to touch it without any error tolerance mechanism. To resolve this sensitive areas are defined as seen in Figure 11.

By typing on intersections and not cells the user is given more choices to choose from. In addition to this with the enhanced algorithms grid the size of grid increases and thus changes to 9*9.

Common attacks on graphical passwords

All the articles on graphical schemes that cover common attacks are thus explained further (Arash et al., 2009).

Password brute forcing attack

In this attack, which has the attack pattern ID 112, the

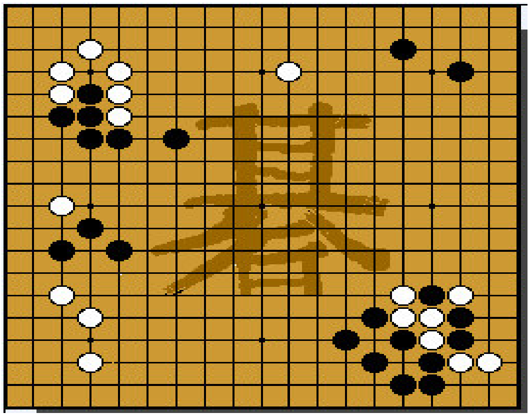

Figure 11. Pass-Go scheme, 2006.

attacker tries every possible value for a password until they succeed (Common Attack, 2009). A brute force attack, if feasible computationally, will always be successful because it will essentially go through all possible passwords given the alphabet used and the maximum length of the password. A system will be vulnerable to this type of an attack if it does not have a proper mechanism to ensure that passwords are strong and comply with an adequate password policy. In practice, a pure brute force attack on passwords is rarely used, unless the password is suspected to be weak. The speed with which an attacker discovers a secret is directly related to the resources that the attacker has. This attack method is resource expensive as the attackers' chance for finding user's password is high only if the resources be as complete as possible.

Dictionary based password attack

In this attack which has the attack pattern ID 16, an attacker tries each of the words in a dictionary as passwords to gain access to the system via some user's account. If the password chosen by the user was a word within the dictionary, this attack will be successful. This is a specific instance of the password brute forcing attack pattern.

Guessing attack

Since many users try to select their password based on their personal information like the name of their pets, passport number, family name and so on, the attacker also tries to guess passwords by trying these possible passwords. Password guessing attacks can be broadly categorized into online password guessing attacks and offline dictionary attacks. In an online password guessing attack, an attacker tries a guessed password by manipulating the inputs of one or more oracles. In an offline dictionary attack, an attacker exhaustively searches for the password by manipulating the inputs of one or more oracles (Roman, 2007).

Spyware attacks

Spyware is a type of malware which is installed on computers with the aim of collecting sensitive information about users, using a key logger or key listener. This information is gathered without the user's knowledge and reported back to an outside source. During graphical password authentication the attacker attempts to gain sensitive information like user names or selected password images by intercepting information exchanged.

Shoulder surfing attack (Observer attack)

Shoulder surfing refers to using direct observation techniques, such as looking over someone's shoulder, to get information. Shoulder surfing is effective in crowded places because it's really easy to stand near someone and watch them entering a PIN number for instance at an ATM machine. This attack is also possible at a distance using vision-enhancing devices like miniature closed circuit cameras which can be concealed in ceilings, walls or fixtures to observe data entry. To prevent shoulder surfing, it is advised to shield paperwork or the keypad from view by using one's body or cupping one's hand. Nearly most graphical password schemes are quite vulnerable to shoulder surfing.

Social engineering attack

In this kind of attack an attacker uses human interaction to obtain or compromise information about an organization or computer systems, while claiming to be one of employees in order to gain identity. On the other hand, the attacker tries to ask many questions in order to infiltrate an organization's security. If an attacker is not able to gather enough information from one source, he or she may contact another source within the same organization and rely on the information from the first source to add to his or her credibility.

Our new proposed algorithm

In order to overcome all the prior methods shortcomings, the objective of this paper is to propose a new algorithm

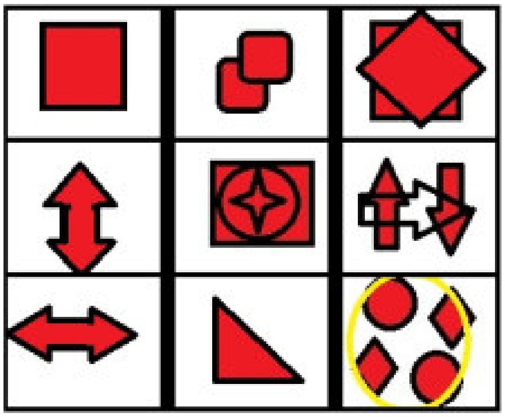

Figure 12. The registration phase grid.

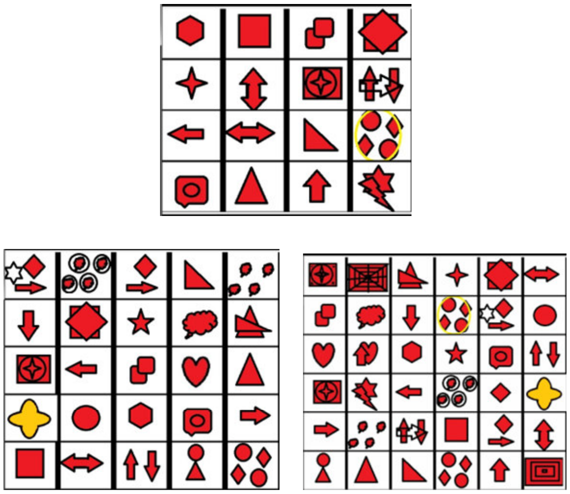

Figure 13. The possible log-in phase grids.

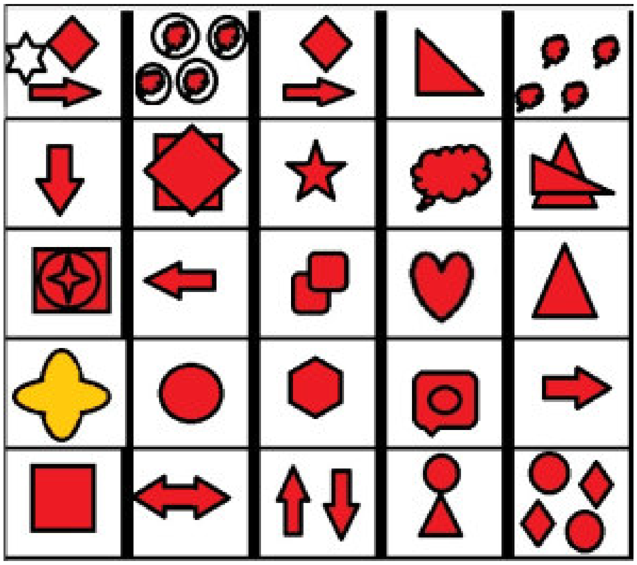

Figure 14. The grid selected for the registration phase.

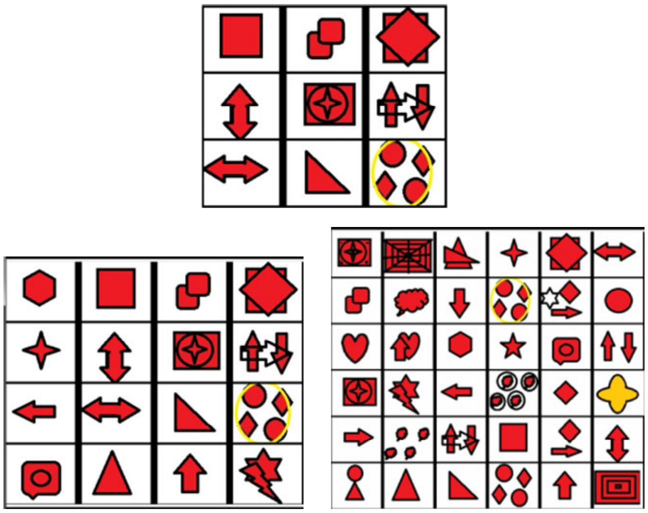

Figure 15. The possible grids for the log-in phase.

based on the Cued Recall scheme. the proposed algorithm focus on the size of grids in the log-in phase by ensuring that they are different from what the user had chosen during the registration phase. Even though our proposed algorithm is based on the Qualitative DAS, instead of changing the size of grid lines distance at login we shall change the number of cells in the log-in phase during the registration phase. For instance if a chooses a password in a 3*3 grid then in the log-in phase the user has to obtain the password from a 4*4 or 5*5 or 6*6 grid.

The system can save The size of the grid used during the registration phase is stored on the system so as to allow it to randomly find a different grid for every user during the log in phase and later create a different grid password using the user's password and some fake images. The registration phase of a user on a 3*3 grid is shown in Figure 12.

In the event that this user wishes to log-in, the system, will refer to the saved grid size used during the registration phase and use it to choose a random number from among the available grids for example 4*4 or 5*5 or 6*6. The available grids that can be used by this user during the log-in phase are shown in Figure 13.

A further example depicted in Figures 14 and 15 show the registration and log-in phases where the user selects a 5*5 size grid during registration. In this case the 3*3 or 4*4 or 6*6 grids will be displayed for the user to choose from in the log-in phase.

Table 1. Comparative table based on attack patterns.

Row	Algorithm	Cued recall- based	Pure Recall-Based	Attacks					
				Brute force	Dictionary	Guessing	Spyware	Shoulder surfing	Social engineering
1	Passdoodle	√		N					
2	Draw A Secret (DAS)	√		N	Y	Y	N	Y	N
3	Grid Selection	√		N					
4	Qualitative DAS	√		N					
5	Syukri Algorithm	√		N	Y	Y	N	Y	N
6	Proposed algorithm	√		Y		Y	Y	Y	Y
7	Blonder		√	Y	N	Y	N	Y	N
8	Passpoint		√	Y	N	Y	N	Y	N
9	Background DAS		√	N					
10	PASSMAP		√	Y	N		N	Y	N
11	Passlogix V-Go		√	Y	N	Y	N	Y	N
12	Viskey SFR		√	Y	N	Y	N	Y	N
13	Pass-Go		√	Y					

DATA COLLECTION

A web based system was developed and accessible online using the URL www.graphicalpassword.net to allow us to gather users' feedback and execute the attack plan.

Data analysis

In order to evaluate users' feedback on the proposed algorithm, we considered two plans. To start with, a questionnaire was distributed to get user perceptions on satisfaction and usability attributes based on 15 questions. This was then followed by a policy designed in such a way that 5 attackers positioned on the left, right and behind a user in a public place (our faculty hall) could be attempt a shoulder surfing attack. To augment this one camera was also used for monitoring.

RESULTS

The initial evaluation phase based of results from 50 questionnaire respondents show that 95% of users were satisfied with the registration and login phase that focused on four attributes:

i. Easy to use
ii. Easy to memorize
iii. Easy to understand
iv. Easy to execute

Results from the second phase which was used to evaluate attack resistance to guessing and shoulder surfing attacks, indicated a system resistance of approximately 92%. In addition to this, unnatural images were used to create grids thus making it even more difficult for an attacker to deduce any information about a user's behavior and using the social engineering attack. Since the proposed system is not dependant on any sensitive information about users, it renders attacks using key loggers or key listeners useless. On the other hand an attacker cannot even use spyware techniques making our proposed algorithm and developed system resistant to the majority of professional attacks on graphical password authentication.

DISCUSSION

Based on the literature review, we studied twelve algorithms on cued and pure Recall-based schemes. As part of our discussion on our proposed algorithm and previous works, we use a comparative table which includes attacks for all thirteen algorithms (Table 1).

As shown in Table 1, the brute force attack is the main weakness of all cued-recall based algorithms analyzed. In addition spyware and social engineering attacks are also weaknesses of some of these algorithms.

Conclusions

Seven Pure Recall-Based and five Cued Recall-Based graphical password authentication algorithms were reviewed in this study. From all these algorithms we were able to come up with a number of shortcomings that can allow attacks to be perpetuated. Therefore, it can be concluded that the most common Lacks on the nine algorithms were:

i. Due to users frequently being fascinated by pictures drawn by other users the common picture for passwords became obvious.
ii. After some time has elapsed users tend to forget
iii. The drawing sequence that they had used
iv. Typically users have a tendency to choose weak passwords which are vulnerable to the graphical dictionary attack.
v. The use of a mouse as a drawing input device for graphical password is not common.
vi. It is not easy to commit to memory and use some of the algorithms.
vii. The choice of weak passwords leads to passwords that are easily guessable or predictable.

After this a GUA attack patterns survey was done in an attempt to make a comparison table for recall-based algorithms based on attack patterns. As part of future works, an algorithm that is resistant to most of the shortcomings mentioned in this paper will be proposed and developed.

In conclusion, our newly proposed algorithm for a graphical password is based on multi size grids used during the login phase and was uploaded on a website (www.graphicalpassword.net) for a 3 month evaluation period. The evaluation included an attacking scenario and an on-line questionnaire on the same website.

ACKNOWLEDGMENTS

We would like to express our appreciation to our parents and all the teachers and lecturers who helped us to understand the importance of knowledge and show us the best way to gain it.

REFERENCES

Ahmet ED, Nasir M, Jean-Camille B (2007). Modeling user choice in the PassPoints graphical password scheme, Symposium on Usable Privacy and Security. Pittsburgh, Pennsylvania, USA. ACM, 20-28; July.

Ali Mohamed E (2008). Study and Develop a New Graphical Password System", University Technology Malaysia, Master Dissertation.

Arash HL, Rosli S, Samaneh F, Omar BZ (2009). A wide-range survey on Recall-Based Graphical User Authentications algorithms based on ISO and Attack Patterns, IJCSIS, 6: 3.

Christopher VP (2004). a Lightweight Authentication Method, Massachusetts Institute of Technology, Research Science Institute, July 27.

Di L, Paul D, Patrick O, Jeff Y (2007). Graphical Passwords and Qualitative Spatial Relations, Proceedings of the 3rd symposium on Usable privacy and security. Pittsburgh, Pennsylvania. ACM, 161-162; July.

Greg EB (1996). Graphical Password", U.S. Patent No. 5559961.

Jermyn I, Mayer A, Monrose XA, Reiter MK, Rubin AD (1999). The design and analysis of graphical passwords, Proceedings of the Eighth USENIX Security Symposium. August 23-26. USENIX Assoc., pp. 1-14.

Karen R (2008). On user involvement in production of images used in visual authentication"; Elsevier, J. Visual Languages and Computing.

Muhammad DH, Abdul HA, Norafida IT, Hazinah KM (2008). Towards Identifying Usability and Security Features of Graphical Password in Knowledge Based Authentication Technique; IEEE Explore, 2008

Roman VY (2007). User Authentication via Behavior Based Passwords; IEEE Explore, 2007.

Saranga K, Dugald RH (2008). Order and Entropy in Picture Passwords, Proceedings of graphics interface 2008. Windsor, Ontario, Canada. Canadian Information Processing Society, pp. 115-122.

Susan W, Jean-Camille B, Alex B (2005a).'Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice, Symposium On Usable Privacy and Security (SOUPS), Pittsburgh, PA, USA.

Susan W, Jim W, Jean-Camille B, Alex B, Nasir M (2005b). PassPoints, "Design and longitudinal evaluation of a graphical password system", Academic Press, Inc. 102-127, July.

Xiaoyuan S, Ying ZG, Scott O (2005). Graphical Passwords: A Survey, Proceedings of the 21st Annual Computer Security Applications. IEEE, pp. 463-472.