Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 9, September 2014, pg.361 – 375

RESEARCH ARTICLE

COMPARATIVE STUDY OF GRAPHICAL USER AUTHENTICATION APPROACHES

Radhika
Department of Computer
Science & Engineering
Gurgaon Institute of
Technology & Management,
Gurgaon
radhika11malik@gmail.com

Siddhartha Sankar Biswas
Department of Computer
Science & Engineering
Gurgaon Institute of
Technology & Management,
Gurgaon
mailtossbiswas@gmail.com

ABSTRACT

Today, authentication technology is the main measure to guarantee information security, and the most common and convenient authentication method in use is the alphanumeric password. However, their inherent defects led to the development of graphical password as an alternative. Graphical password which uses images as passwords, rather than alphanumeric characters is motivated particularly by the fact that it is generally easier for users to remember and recall images than words, and it is conceivable that graphical password would be able to provide better security than alphanumeric password. Authentication, authorization and auditing are the most important issues of security on data communication. In particular, authentication is the life of every individual essential closest friend. The user authentication security is dependent on the strength of user password. A secure password is usually random, strange, very long and difficult to remember. For most users, remember these irregular passwords are very difficult. To easily remember and security are two sides of one coin. Graphical password authentication technology is the use of click on the image to replace input some characters. The graphical user interface can help user easy to create and remember their secure passwords. However, in the graphical password system based on images can provide an alternative password, but too many images will be a large database to store issue.

In this thesis, a study of various schemes of graphical user authentication is made and also several challenges in graphical authentication are discussed.

Keywords: Graphical password, Authentication, Security, Usability, Password space

1. INTRODUCTION

Graphical authentication schemes have been proposed as a possible alternative to replace the traditional username/password authentication schemes. In graphical user authentication we use images as the password. Graphical password can be defined as that; Graphical password is an authentication system that works by having the user select from images, in a specific order, presented in a graphical user interface (GUI)". For this reason, the authentication method in which graphical images or pictures are used as a password is sometimes called graphical user authentication (GUA). User authentication involves issues of both usability and security. Too often, one or the other is ignored even though both are important and necessary. This problem is evident in knowledge-based authentication systems. For example, passwords are often either memorable-but-insecure or secure-

But difficult to remember when they should be memorable and secure. Graphical passwords are potentially more memorable and secure than traditional text passwords because they harness the human ability to easily recognize and recall images. In this thesis, we advance research in the area of knowledge-based authentication through usability and security evaluations of graphical password schemes, the creation of novel schemes that offer improved memorability and security, and the identification of some underlying design strategies to inform the design of other knowledge-based authentication schemes. Computer applications today uses user authentication as its fundamental security component. It provides the basis for access control and user accountability. While there are various types of user authentication systems, alphanumerical username/passwords are the most common type of user authentication. They are versatile and easy to implement and use. Alphanumerical passwords are required to satisfy two contradictory requirements.

- They have to be easily remembered by a user.
- They have to be hard to guess by impostor.

Users are known to choose easily guessable and/or short text passwords, which are an easy target of dictionary and brute-forced attack. Enforcing a strong password policy sometimes leads to an opposite effect, as a user may resort to write his or her difficult-to-remember passwords on sticky notes exposing them to direct theft.

One innovation is graphical passwords, i.e., passwords that are based on images rather than alphanumeric strings. The basic idea is that using images will lead to greater memorability and decrease the tendency to choose insecure passwords. This, in turn, should increase overall password security.

2. GRAPHICAL PASSWORDS

Graphical password can be defined as that; Graphical password is an authentication system that works by having the user select from images, in a specific order, presented in a graphical user interface (GUI)". For this reason, the authentication method in which graphical images or pictures are used as a password is sometimes called graphical user authentication (GUA). Many techniques have been designed in the field of graphical password since 1996. Existing graphical password schemes can be categorized into following categories:

- Recall-based
- Recognition-based
- Cued-recall

In the recall-based scheme, a user is asked to reproduce a pre-drawn outline drawing with the mouse or stylus on a grid.

Recognition-based scheme requires the user to memorize a portfolio of images during password creation, and then recognize their images from among decoys during authentication.

Cued-recall scheme, intends to the memory load on users, generally provides a background image and the user must remember and target specific locations on the image.

2.1 Recognition Based Techniques

Dhamija and Perrig [1] proposed a graphical authentication scheme based on the hash Visualization technique. In their authentication system, user selects a certain number of images from a set of program generated random pictures (Figure 2.1). For a user to be authenticated, he or she would have to identify the pre-selected images. One weakness of their system is that the server needs to store the seeds of the selected images of each user in plain text. Also, it is a bit time consuming and tedious for the users to select images from the database. Akula and Devisettys algorithm is similar to the technique proposed by Dhamija and Perrig. The main difference is that they make the authentication more secure and require less memory. They did this by using hash function SHA-1, which produces a 20 byte output. The authors also suggested that this could be deployed on the Internet, cell phones and PDA's. Weinshall and Kirkpatrick[2] proposed and study several authentication schemes. They conducted a number of user studies. The various studies includes picture recognition, object recognition, and pseudo word recognition. In the picture recognition study, out of a database of 20,000 images, a large set of images are selected (100-200 images). Then the user is trained to recognize those set of images.

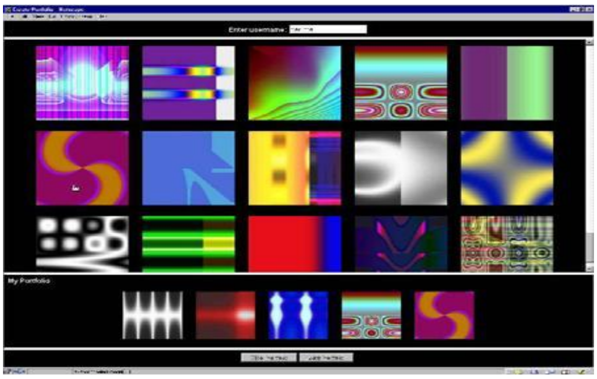


Figure 2.1: Graphical Authentication Scheme By Dhamija And Perrigreduce

After one to three months, users in their study were able to recognize over 90% of the images in the training set. This study showed that pictures are the most effective among the three schemes tested. Pseudo codes can also be used, but require proper setting and training.

Sobrado and Birget [3] developed a graphical authentication technique that is considered to be shoulder surfing resistant. In the first scheme, the system will display a number of pass-objects (pre-selected by user) among many other objects. To be authenticated, a user needs to recognize pass-objects and click inside the convex hull formed by all the pass-objects (Figure 2.2). In order to make the password hard to guess, Sobrado and Birget suggested using 1000 objects, which makes the display very crowded and the objects almost indistinguishable, but using fewer objects may lead to a smaller password space, since the resulting convex hull can be large. In their second algorithm, a user moves a frame (and the objects within it) until the pass object on the frame lines up with the other two pass objects.

Man, et al.[4] proposed another shoulder-surfing resistant algorithm. In their method, a user selects a number of pass-objects which are nothing but thumbnails of images. Each pass-object has several variants and each variant is assigned a unique code. During authentication, the user is challenged with several scenes. Each scene contains several pass-objects (each in the form of a randomly chosen variant) and many decoy-objects. The user has to type in a string with the unique codes corresponding to the pass-object variants present in the scene as well as a code indicating the relative location of the pass objects in reference to a pair of eyes. The argument is that it is very hard to crack this kind of password even if the whole authentication process is recorded on video because where is no mouse click to give away the pass-object information. However, this method still requires users to memorize the alphanumeric code for each pass-object variant. Hong, et al. later extended this approach to allow the user to assign their own codes to pass-object variants. Figure 2.3 shows the log-in screen of this graphical password scheme. However, this method still forces the user to memorize many text strings and therefore suffer from the many drawbacks of text-based passwords.

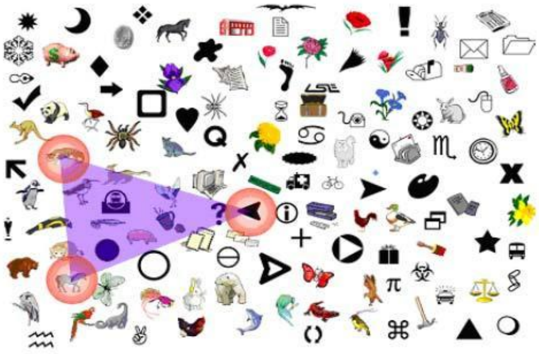


Figure 2.2: Graphical Authentication Scheme By Sobrado And Birget

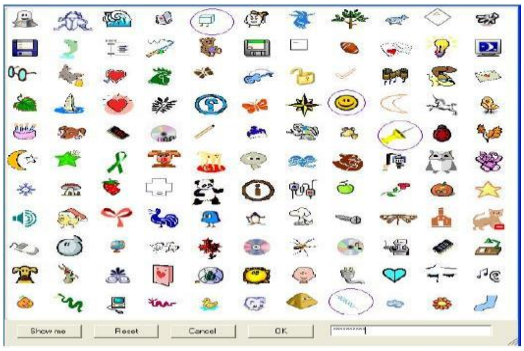


Figure 2.3: Graphical Authentication scheme by Hong, et

A technique called **Passface** is developed by Real User Corporation. The basic idea is as follows. The user have to choose four images of human faces from a face database. These selected faces are stored as their password. In the authentication stage, the user is presented with a grid consisting of nine faces, consisting of one face previously chosen by the user and eight decoy faces (Figure 2.4). 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 assumption that people can recall human faces easier than other pictures. User studies by Valentine[5] have shown that Passfaces are very memorable over long intervals. Comparative studies conducted by Brosto and Sasse showed that Passfaces had only a third of the login failure rate of text-based passwords, despite having about a third the frequency of use. Their study also showed that the Passface-based login process took longer than text passwords and therefore was used less frequently by users. However the effectiveness of this method is still uncertain.

Davis, et al.[6] studied the graphical passwords created using the Passface technique and found obvious patterns among these passwords. For example, most users tend to choose faces of people from the same race. This makes the Passface password somewhat predictable. This problem may be alleviated by arbitrarily assigning faces to users, but doing so would make it hard for people to remember the password.

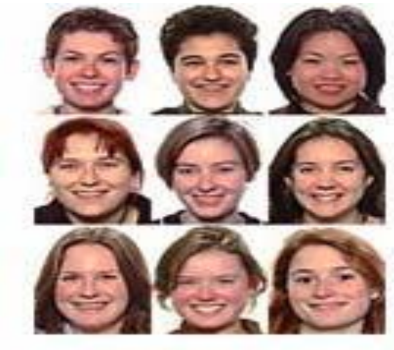


Figure 2.4: Passface Graphical Authentication Scheme

Jansen[7] proposed a graphical password mechanism for mobile devices. During the enrollment stage, a user selects a theme (e.g. sea, cat, etc.) which consists of thumbnail photos and then registers a sequence of images as a password (Figure 2.5).During the authentication, the user must enter the registered images in the correct sequence. One drawback of this technique is that since the number of thumbnail images is limited to 30, the password space is small. Each thumbnail image is assigned a numerical value, and the sequence of selection will generate a numerical password. The result showed that the image sequence length was generally shorter than the textural password length. To address this problem, two pictures can be combined to compose a new alphabet element, thus expanding the image alphabet size.

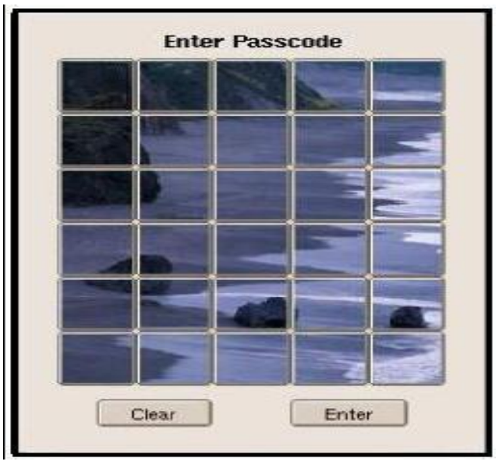


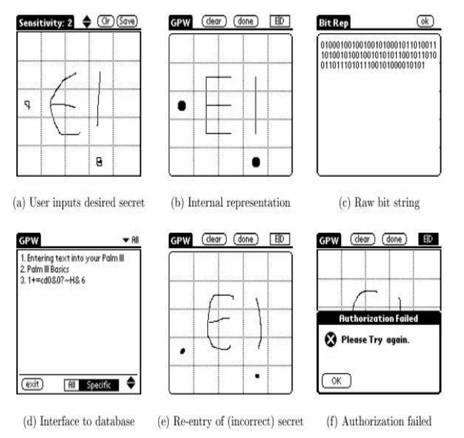
Figure 2.5: Graphical Authentication Scheme By Jansen Et Al.

2.2 Recall Based Techniques

In this section we discuss two types of picture password techniques: reproducing a drawing and repeating a selection.

2.2.1 REPRODUCE A DRAWING

Jermyn, et al.[8] proposed a technique, called Draw-a-secret (DAS)", which allows the user to draw their unique password (Figure 2.6). A user is asked to draw a simple picture on a 2D grid. The coordinates of the grids occupied by the picture are stored in the order of the drawing. During authentication, the user is asked to re-draw the picture. If the drawing touches the same grids in the same sequence, then the user is authenticated. Jermyn, et al. suggested that given reasonable-length passwords in a 5 X 5 grid, the full password space of DAS is larger than that of the full text password space.



01000100100100101000101101001110100101001001010101100101101001101110101110010100001010 1

1. Entering text into your Palm III
2. Palm III Basics
3. 1+=cd0&0?~H& 6

Authorization Failed

Please Try again.

(a) User inputs desired secret (b) Internal representation (c) Raw bit string

(d) Interface to database (e) Re-entry of (incorrect) secret (f) Authorization failed

Figure 2.6: Das Authentication Technique

Syukri, et al.[9] proposes a system where authentication is conducted by having the user drawing their signature using a mouse (Figure 2.7). Their technique included two stages, registration and verification. During the registration stage: the user will first be asked to draw their signature with a mouse, and then the system will extract the signature area and either enlarge or scale-down the signature, and rotates if needed, (also known as normalizing). The information will later be saved into the database.

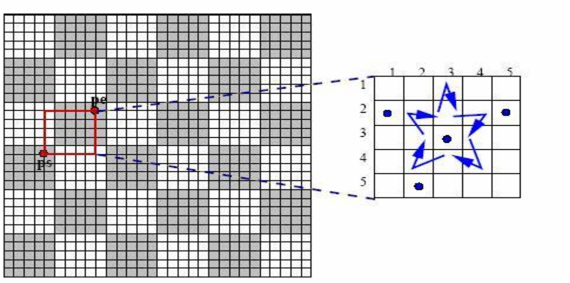


Figure 2.7: Signature Drawn By Mouse

The verification stage first takes the user input, and does the normalization again, and then extracts the parameters of the signature. After that, the system conducts verification using geometric average means and a dynamic update of the database. According to the paper the rate of successful verification was satisfying.

Recently, **Dunphy and Yan[10]** added background images to DAS to encourage users to create more complex passwords. Their study compared the new BDAS with DAS using paper prototypes. It shows that the background image reduced the amount of symmetry and led to longer passwords that were similarly memorable to the weaker DAS passwords. They did not investigate whether the background images introduced other types of predictable behaviour such as targeting similar areas of the images or image specific patterns.

2.2.2 REPEAT A SEQUENCE OF ACTIONS

Blonder designed a graphical password scheme in which a password is created by having the user click on several locations on an image. During authentication, the user must click on the approximate areas of those locations. The image can assist users to recall their passwords and therefore this method is considered more convenient than unassisted recall (as with a text-based password). Passlogix has developed a graphical password system based on this idea. In their implementation (Figure 2.8), users must click on various items in the image in the correct sequence in order to be authenticated. Invisible boundaries are defined for each item in order to detect whether an item is clicked by mouse. It was reported that Microsoft had also developed a similar graphical password technique where users are required to click on pre-selected areas of an image in a designated sequence. As a result, a user can click on any place on an image (as opposed to some pre-defined areas) to create a password. A tolerance around each chosen pixel is calculated. In order to be authenticated, the user must click within the tolerance of their chosen pixels and also in the correct sequence. Because any picture can be used and because a picture may contain hundreds to thousands of memorable points, the possible password space is quite large. However, their studies showed that graphical password users had more difficulties learning the password, and took more time to input their passwords than the alphanumerical users.

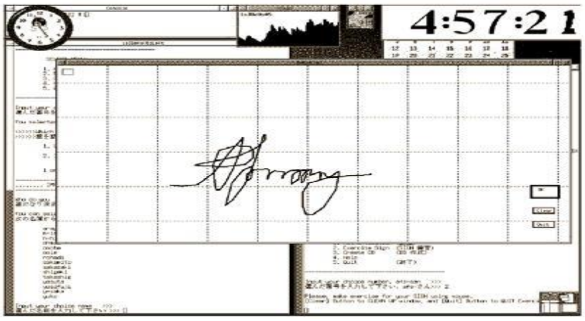


Figure: 2.8: A Recall-Based Technique Developed By Passlogix

Passlogix[11] has also developed several graphical password techniques based on repeating a sequence of actions. For example, its v-Go includes a graphical password scheme where users can mix up a virtual cocktail and use the combination of ingredients as a password. Other password options include picking a hand at cards or putting together a \meal" in the virtual kitchen. However, this technique only provides a limited password space and there is no easy way to prevent people from picking poor passwords.

Passpoint[12] PassPoints , is based on Blonder's idea of representing the password by multiple clicks on a single image. However, it overcomes some of the limitations of his scheme: There are no artificial predefined boundaries around areas of the image within which the user can click. This means that in the PassPoints scheme, users may choose any place in the image as a click point. After a sequence of click points (i.e., pixels) is chosen (a "password"), the system cryptographically hashes ("encrypts") the password and calculates a tolerance region around the chosen pixels. When logging in, to make a valid click the user will have to click within this tolerance. The size of this tolerance can be varied, but for the password space to be large the tolerance should not be too large, e.g., 2 to 5 mm around each chosen pixel. To log in the users must click within the tolerance of their chosen click points. Their memory is cued by the image as they enter their password. The system or the user could provide the image.

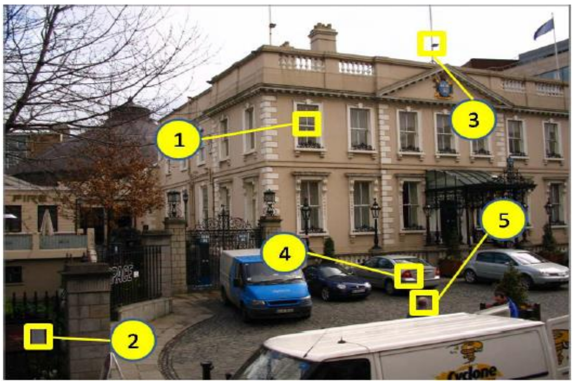


Figure 2.9: An Image Used In The Passpoint Sytem

The main requirement is that it be a complex image that is visually rich enough to have many potentially memorable click places. Without artificial predefined boundaries, more intricate images, such as natural scenes, can be used.

Passdoodle[13]: Passdoodle is similar to DAS, allowing users to create a freehand drawing as a password, but without a visible grid. The use of additional characteristics such as pen color, number of pen strokes, and drawing speed are suggested by the authors to add variability to the doodles. Goldberg et al. report on a small paper-based prototype study of Passdoodle and found that users often remembered their final drawing, but they made mistakes in recalling the number, order, or direction of the pen strokes. In a lab study , 10 users created their doodle by tracing it with their finger on a touch screen. Users repeated the trace several times. This data was used as training for the recognition algorithm and it was found that similar input could be accurately interpreted as similar. No further usability or security analysis has been reported.

Later**, Govindarajulu and Madhvanath[14]** separately proposed a web-based pass- word manager where a master doodle" was used instead of a master password. In their 10-participant user study, they collected Tamil language character samples using Tablet PCs and PDAs. Using only one initial doodle as the master doodle, they used handwriting recognition techniques to evaluate whether the subsequent doodles were correct and reported 90% accuracy with one of the handwriting recognition techniques.

All three Passdoodle studies focus on the users' ability to recall and reproduce their doodles and on the matching algorithms used to accurately identify similar entries. None of the studies look at usability metrics such as login times or success rates. During password creation, however, Passdoodles would likely require training of the recognition algorithm to build an accurate model of the password. Although no security analysis has been reported, we provide here a preliminary evaluation comments based on our understanding of the scheme. Shoulder-surfing would be possible with Passdoodle and accurately observing one login would be sufficient to learn the password. However, reproducing the drawing may be difficult and would depend on which measures (such as drawing speed) are used by the recognition algorithm. We expect that Passdoodle would be susceptible to the same types of predictability seen with DAS (symmetry and short passwords) and as such successful dictionary attacks may be possible. As with DAS, some users are likely to choose personally identifiable passwords that can be guessed by someone who knows the user. It would likely be difficult to accurately describe a Passdoodle password since there is no visible grid to act as a guide, although it may be possible to sketch and share such passwords. Passdoodle passwords (the drawings themselves) would likely need to be stored in a manner accessible to the system, as opposed to hashed, since the recognition algorithm must allow for various approximations of the original password.

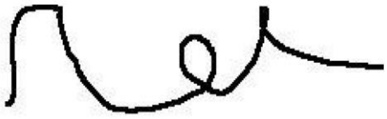


Figure 2.10: An Image Used In The Passdoodle System

Pass-Go :

Pen colour was used as an additional parameter and the authors suggest using a finer grid to further increase the theoretical password space. Dictionary attacks may be less effective than DAS since it is reported that users selected longer passwords and used colour; both add variability to passwords. Interpreting other aspects of security, Pass-Go is similar to DAS in terms of shoulder-surfing, phishing, social engineering, and personalization.

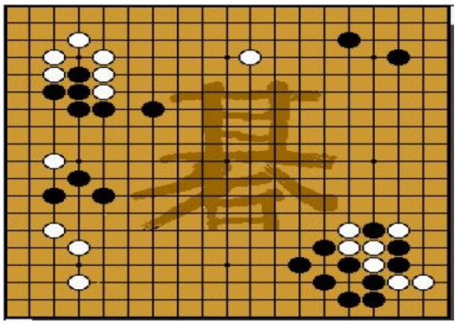


Figure 2.11: An Image Used In The PassGo System

A similar scheme was proposed by Orozco et al. It uses a haptic input device that measures pen pressure while users draw their password. They suggest that this may help protect against shoulder-surfing since an observer would have difficulty distinguishing variances in pen pressure. Results of their user study, however, show that users applied very little pen pressure and hardly lifted the pen while drawing, so the use of haptics did not increase the difficulty of guessing passwords.

2.3 Cued-recall Techniques

Graphical passwords based on cued recall were first discussed by Blonder. In such a scheme the user chooses several locations in an image to create a password. To log in the user must click on or close to those locations. There are no multiple rounds of images, just a single image. In an implementation of this scheme the image had predefined click objects or regions that were outlined by thick boundaries. The users chose the password from these objects and logged in using them (although thick boundaries were not visible when logging in). A click anywhere within the boundary was considered correct. A problem with this scheme was that the number of predefined click regions was relatively small so the password had to be quite long to be secure (e.g., 12 clicks). Also, the use of pre-defined click objects or regions required simple, artificial images, for example cartoon-like images, instead of complex, real-world scenes.

2.3.1 CUED CLICK-POINTS

Cued Click-Points (CCP)[15] is our first proposed alternative to PassPoints. In CCP, users click one point on each of c = 5 images rather than on five points on one image. It offers one-to-one cueing, where each image acts as a cue for the one corresponding Click point, and introduces implicit feedback, where visual cues instantly alert legitimate users if they have made a mistake when entering their latest click-point (at which point they can cancel their attempt and retry from the beginning). It also makes attacks based on hotspot analysis more challenging, as we discuss later. As shown in Figure 2.12. Each click results in showing a next-image, in effect leading users down a \path" as they click on their sequence of points. A wrong click leads down an incorrect path, with an explicit indication of authentication failure only after the final click. Users can choose their images only to the extent that their click-point dictates the next image. If users dislike the resulting images, they may create a new password involving different click-points to get different images.

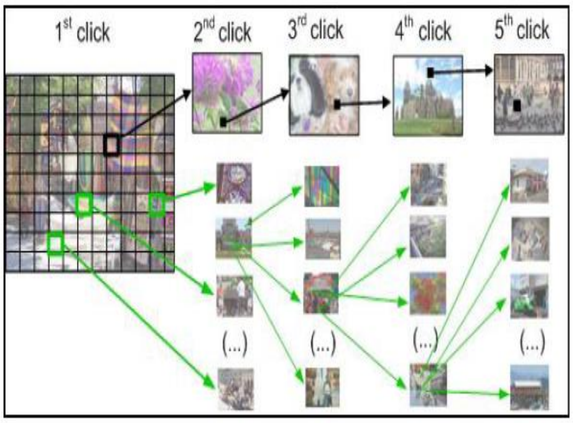


Figure 2.12: An Image Used In CCP

2.3.2 PERSUASIVE CUED CLICK-POINTS:

Using CCP as a base system, we added a persuasive feature to encourage users to select more secure passwords, and to make it more difficult to select passwords where all five click-points are hotspots.

Specifically, when users created a password, the images were slightly shaded except for a randomly positioned viewport. The viewport's size was intended to offer a variety of distinct points but still cover only an acceptably small fraction of all possible points. Users were required to select a click-point in this region, they could press the "shuffle" button to randomly reposition the viewport. While users were allowed to shuffle as often as they wanted, this significantly slowed the password creation process. During password confirmation and login, the images were displayed normally, without shading or the viewport and users were allowed to click anywhere.

Our hypotheses were:

1. Users will be less likely to select click-points that fall into known hotspots.

2. The click-point distribution across users will be more randomly dispersed and will not form new hotspots.

3. The login success rates will be similar to those of the original CCP system.

4. Participants will feel that their passwords are more secure with PCCP than participants of the original CCP system.

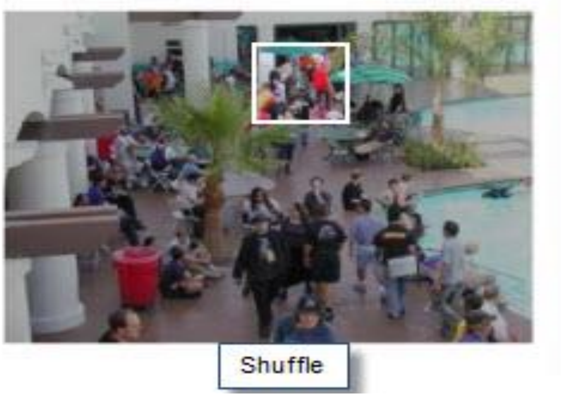


Figure 2.13: An Image Used In PCCP

3. DESIGN AND IMPLEMENTATION ISSUES OF GRAPHICAL PASSWORDS

3.1 Security

An important security goal of authentication mechanisms is to maximize the effective password space; we would like the effective password space to include as much of the theoretical password space as possible (ideally, all of it). Since the effective password space is determined by user behaviour, the design of a system involves us- ability as well. Ideally, passwords should be secure without sacrificing the usability of the system. In practice, increasing one often reduces the other, so typically a middle-ground must be found where both the security and usability of the system are acceptable. Measures of the effective password space are imprecise approximations. One approach that may help is to identify classes of passwords that have higher probability of being chosen by users. In this case, a proximity function (a measure of similarity between items) may be useful.

3.2 Usability

One of the major arguments for graphical authentication is that images are much more easier to remember than text strings. Some research papers presented preliminary user studies to support this. However, current user studies involves only a small number of users and are still very limited. But it is still difficult to be convinced that graphical passwords are easier to remember than text based passwords as we do not have enough evidence. A major complaint among the users of graphical authentication procedure is that the registration process and log-in process take too much time, especially in recognition-based approaches. For instance, in the registration phase, a user has to pick few images from a larger number of image sets. Then in the authentication phase, a user has to identify a few pass-images by scanning through all the images displayed. Users may find this process long and tedious. Due to this users often find graphical passwords less convenient than text based passwords. And also most users are not familiar with the graphical passwords.

3.3 Reliability

The major design issue for recall-based methods is the reliability and accuracy of user input recognition. The error tolerances in graphical authentication schemes have to be set carefully if the tolerances are overly high then it may lead to many false positives. And if the tolerances are overly low, then again it may lead to many false negatives. In addition, if the program is more error tolerant, then it will be more vulnerable to attacks.

3.4 Communication and storage

Graphical authentication schemes require much more space for storage than text based passwords. Huge numbers of images may have to be maintained in a centralized storage database. The delay in loading or transfer of images is also a concern for graphical authentication schemes. Especially for recognition based techniques in which a large number of images may need to be displayed for each round of verification in the authentication process.

4. SECURITY ANALYSIS OF GRAPHICAL AUTHENTICATION

4.1 Brute force search

The main defense against brute force search is to have a sufficiently large password space. Text-based passwords have a password space of 94^N, where N is the length of the password, 94 is the number of printable characters excluding SPACE. Some graphical password techniques have been shown to provide a password space similar to or larger than that of text-based passwords. Recognition based graphical passwords tend to have smaller password spaces than the recall based methods.

It is more difficult to carry out a brute force attack against graphical passwords than text-based passwords. The attack programs need to automatically generate accurate mouse motion to imitate human input, which is particularly difficult for recall based graphical passwords. Overall, we believe a graphical password is less vulnerable to brute force attacks than a text-based password.

4.2 Dictionary attacks

Since recognition based graphical passwords involve mouse input instead of keyboard input, it will be impractical to carry out dictionary attacks against this type of graphical passwords. For some recall based graphical passwords [24][30], it is possible to use a dictionary attack but an automated dictionary attack will be much more complex than a text based dictionary attack. More research is needed in this area. Overall, we believe graphical passwords are less vulnerable to dictionary attacks than text-based passwords.

4.3 Guessing

Unfortunately, it seems that graphical passwords are often predictable, a serious problem typically associated with text-based passwords. For example, studies on the Passface technique have shown that people often choose weak and predictable graphical passwords. Nali and Thorpe’s study revealed similar predictability among the graphical passwords created with the DAS technique . More research efforts are needed to understand the nature of graphical passwords created by real world users.

4.4 Spyware

Except for a few exceptions, key logging or key listening spyware cannot be used to break graphical passwords. It is not clear whether “mouse tracking” spyware will be an effective tool against graphical passwords. However, mouse motion alone is not enough to break graphical passwords. Such information has to be correlated with application information, such as window position and size, as well as timing information.

Table 4.1: 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.	Blonder		•	Y	N	Y	N	Y	N
7.	Pass Point		•	Y	N	Y	N	Y	N
8.	Background DAS		•	N					
9.	PASSMAP		•	Y	N		N	Y	N
10.	Passlogix v-Go		•	Y	N	Y	N	Y	N

5. RESULT AND DISCUSSION

5.1 Analysis of Graphical Password

Table 5.1 A Taxonomy For Graphical Password

Techniques	**Usability**		**Security issues**	
	Authentication process	Memorability	*Password space*	*Possible attack methods*
Text-based password	Type in password, can be very Fast	Depends on the password. Long and random passwords are hard to remember	94^K (there are 94 printable characters excluding SPACE, N is the length of the password).The actual password space is usually much smaller.	Dictionary attack, brute force search, guess, spyware, shoulder surfing, etc.
Perrig and Song	Pick several pictures out of many choices. Takes longer to create than text password	Limited user study showed that more people remembered pictures than text-based passwords	N!/K!(N-K)! (N is the total number of pictures; K is the number of pictures in the graphical password)	Brute force search, guess, shoulder-surfing

Sobrado and Birget	Click within an area bounded by pre-registered picture objects, can be very Fast	Can be hard to remember when large numbers of objects are involved.	N!/K!(N-K)! (N is the total number of picture objects; K is the number of pre-registered objects)	Brute force search, guess
Man, et al. Hong, et al.	Type in the code of pre-registered picture objects; can be very Fast	Users have to memorize both picture objects and their codes. More difficult than text-based Password	Same as the text based password	Brute force search, spyware
Passface	Recognize and pick the pre-registered pictures; takes longer than text-based password	Faces are easier to remember, but the choices are still Predictable	N^K (K is the number of rounds of authentication, N is the total number of pictures At each round)	Dictionary attack, brute force search, guess, shoulder surfing
Jansen et al.	User register a sequence of images; slower than text-based password	Pictures are organized according to different themes to help users remember	N^K (N is the total number of pictures, K is the number of pictures in the graphical password. N is small due the size limit of mobile devices)	Brute force search, guess, shoulder surfing
Takada and Koike	Recognize and click on the pre-registered images; slower than text-based password. Slower than text-based password	Users can use their favorite images; easy to remember than system assigned pictures	(N+1)^K (K is the number of rounds of authentication, N is the total number of pictures at each round)	Brute force search, guess, shoulder surfing
Jermyn, et al. , Thorpe and van Oorschot	Users draw something on a 2D grid	Depends on what users draw. User studies showed the drawing sequence is hard to remember	Password space is larger than text based password. But the size of DAS password space Decreases significantly with fewer strokes for a fixed password length	Dictionary attack, shoulder Surfing
Syukri, et al.	Draw signatures using mouse. Need a reliable signature recognition program.	Very easy to remember, but hard to recognize	Infinite password space	Guess, dictionary attack, shoulder surfing

Goldberg et al.	Draw something with a stylus onto a touch sensitive screen	Depends on what users Draw	Infinite password space	Guess, dictionary attack, shoulder surfing
Blonder , Passlogix , Wiedenbeck, et al.	Click on several pre-registered locations of a picture in the right sequence.	Can be hard to remember	N^K (N is the number of pixels or smallest units of a picture, K is the number of locations to be clicked on)	Guess, brute force search, shoulder surfing

6. CONCLUSION

Our preliminary analysis suggests that it is more difficult to break graphical passwords using the traditional attack methods such as brute force search, dictionary attack, or spyware. However, since there is not yet wide deployment of graphical password systems, the vulnerabilities of graphical passwords are still not fully understood. The relationship between usability and security is a complex one; too often, improvements in one lead to a reduction in the other.

The Cued Click-Point method is very usable and provides great security using hotspot technique. By taking advantage of user’s ability to recognize images and the memory trigger associated with seeing a new image. Cued Click Point is more secure than the previous graphical authentication methods. CCP increases the workload for attackers by forcing them to first acquire image sets for each user, and then analyze for hotspot on each of these images. Cued Click-Points method has advantages over other password schemes in terms of usability, security and memorable authentication mechanism.

REFERENCES

[1] R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in *Proceedings of 9th USENIX Security Symposium*, 2000.

[2] L. Sobrado and J.-C. Birget, "Graphical passwords," The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4, 2002.

[3] J. Birget,D. Hong, and N.Memon. Graphical passwords based on robust discretization. IEEE Transactions on Information Forensics and Security,1(3):395–399, 2006.

[4] D. Hong, S. Man, B. Hawes, and M. Mathews, "A password scheme strongly resistant to spyware," in Proceedings of International conference on security and management. Las Vergas, NV, 2004.

[5] T. Valentine, "An evaluation of the Passface personal authentication system," Technical Report, Goldsmiths College, University of London 1998.

[6]D. Davis, F. Monrose, and M. Reiter. On user choice in graphical password schemes. In 13th USENIX Security Symposium, August 2004.

[7] W. A. Jansen, "Authenticating Users on Handheld Devices," in Proceedings of Canadian Information Technology Security Symposium, 2003.

[8] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin,“The design and analysis of graphical passwords” In 8th USENIX Security Symposium, August 1999.

[9] A. F. Syukri, E. Okamoto, and M. Mambo, "A User Identification System Using Signature Written with Mouse," in Third Australasian Conference on Information Security and Privacy (ACISP): Springer Verlag Lecture Notes in Computer Science (1438), 1998, pp. 403-441.

[10] P. Dunphy and J. Yan. Do background images improve “Draw a Secret” graphical passwords. In 14th ACM Conference on Computer and Communications Security (CCS), October 2007.

[11] Passlogix: Passlogix website. http://www.passlogix.com.

[12] A. Dirik, N. Menon, and J. Birget: Modeling user choice in the Passpoints graphical password scheme. In 3rd ACM Conference on Symposium on Usable Privacy and Security (SOUPS), July 2007.

[13] C. Varenhorst. Passdoodles: A lightweight authentication method. Massachusetts Institute of Technology Resarch Science Institute, July 2004.
[14] N. Govindarajulu and S. Madhvanath: Password management using doodles. In 9th International Conference on Multimodal Interfaces (ICMI), November 2007.
[15] S. Chiasson, P. van Oorschot, and R. Biddle: Graphical password authentication using Cued Click Points. In European Symposium On Research In Computer Security (ESORICS), LNCS 4734, pages 359–374, September 2007.