Towards Identifying Usability and Security Features of Graphical Password in Knowledge Based Authentication Technique

Muhammad Daniel Hafiz[1], Abdul Hanan Abdullah[2], Norafida Ithnin[3], Hazinah K. Mammi[4]
Faculty of Computer Science and Information Systems,
Universiti Teknologi Malaysia, 81300 Skudai, Johor.
Email: mdhafiz@fsktm.upm.edu.my[1], hanan@utm.my[2], afida@utm.my[3], hazinah@utm.my[4]

Abstract

Text-based passwords are ubiquitous authentication system. This traditional authentication system is well-known for it flaws in the aspects of usability and security issues that bring problems to users. Hence, there is a need for alternative mechanism to overcome these problems. Graphical passwords, which consist of clicking or dragging activities on the pictures rather than typing textual characters, might be the option to overcome the problems that arise from the text-based passwords system. In this paper, a comprehensive study of the existing graphical password schemes is performed. We compared and categorized these schemes into two groups; recognition-based scheme and recall-based scheme. We also list out several usability and security features for research continuity in this area.

1. Introduction

Nowadays username and text–based password are the most common and widely used technique in knowledge-based authentication methods. However, the vulnerabilities of this traditional technique are well known. One of the main problems is the difficulty of remembering passwords. Studies have shown that users tend to pick short passwords or passwords that are easily remembered for example pet's name, first name and street address [1]. Unfortunately, these passwords can be easily guessed or broken. According to an article in Computerworld, the security team at a large company tested and ran a network password cracker and surprisingly within 30 seconds, they manage to crack approximately 80% of the passwords [2]. On the other hand, passwords that are hard to guess or break are often hard to remember. Thus a large portion of customer service calls are related to one's forgetting his or her password. Previous studies have showed that human's memory can only remember limited number of text-based passwords, because of that limitation they are likely to write down their password in form of plaintext. In addition, they also tend to use a single password for different kinds of applications [3, 4].

The main objective of improving the existing user authentication technology is to make the method usable and secure for the user. Graphical authentication schemes have been proposed as a possible alternative to traditional text-based password techniques, motivated particularly by the fact that humans can remember pictures better than text [5]. Pictures are generally easier to be remembered or recognized than text, especially photos, which are even easier to be remembered than random pictures. It has also been suggested that graphical passwords is harder to guess or broken by brute force. If the number of possible pictures is sufficiently large, the possible password space of a graphical password scheme may exceed that of text-based schemes and thus presumably offer better resistance to dictionary attacks. Because of these advantages, there is a growing interest in graphical password. In addition, graphical passwords have also been implemented and applied to workstations, websites, login applications, ATM machines and mobile devices such as personal digital assistants (PDAs).

2. Background and Motivation

The existing studies have acknowledged that secure systems in general and authentication solutions in particular, can benefit from improvements in usability. However, many researchers believe that there is a trade-off between the deployment of usability and security [6]. For example, a computer without passwords is considered usable but at the same time it is not secure. In contrast, a computer that requires user to authenticate and change passwords every 15 minutes

978-0-7695-3136-6/08 $25.00 © 2008 IEEE
DOI 10.1109/AMS.2008.136

can be considered as very secure but not usable and nobody will want to use it.

The introduction of graphical authentication by G. Blonder [7] has emerged as an alternative of knowledge based authentication system apart from text-based password approach. Currently there exist a multitude of graphical password schemes. Unfortunately, none of the schemes are considered as both secure and usable [8]. According to Cranor and Garfinkel [6], there are usability and security researchers working together with the aim of building schemes that are both secure and usable. However, the aim still far from reached. The reasons why most of graphical password researchers cannot concentrate on systems with balanced security and usability features are, first, the researchers tend to focus more on the ability of attackers to break or crack the password solutions for authentication with modest prominence on the usability features necessities [9, 10]. Second, the researchers focus more on users' satisfaction by increasing the usability features (especially the password memorability) with little attention on implementation of security features [11].

The aforementioned problems in existing graphical password schemes have motivated the need of providing a scheme that is stable and balanced in usability and security. We believe that by achieving such condition, the scheme will be usable, secure, effective and most importantly able to satisfy the users' needs and requirements.

3. Graphical Password Classifications

3.1. Recognition-based Techniques

Jensen et al. [12] proposed a graphical password scheme based on “picture password”. This scheme was designed especially for mobile devices such as PDAs. Throughout the password creation, the user has to select the theme first (e.g. sea and shore, cat and dog and etc) which consists of thumbnail photos. The user then selects and registers a sequence of the selected thumbnail photo to form a password (Figure 1). The user needs to recognize and identify the previously seen photos and touch it using a stylus in the correct sequence in order to be authenticated.

However, as the numbers of thumbnail photos are limited only to 30, the size of the password space is considered small. A numerical value is assigned for each thumbnail photo and the sequence of selection will produce a numerical password. This numerical password is shorter than the length of textual password. To overcome this problem a user can select one or two thumbnail photos as one single action in order to create and enlarge the size of the password space. However, this will make the memorability of the created password become more complex and difficult.

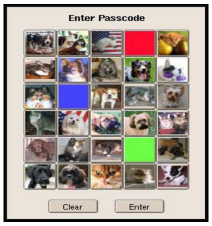


Figure 1: Cats and dog theme

Based on the assumption that human can recall human faces easier than other pictures, Real User Corporation has developed their own commercial product named Passfaces ^{TM} [13]. Basically, Passfaces works as follows, users are required to select the previously seen human face from a grid of nine faces one of which is known while the rest are decoys (Figure 2). This step is continuously repeated until all the four faces are identified.

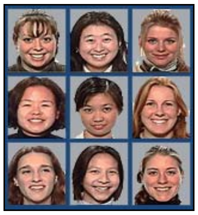


Figure 2: Passfaces ^{TM}

A comparative study conducted by Brostoff and Sasse [14] in which 34 subjects involved in the test showed that, the Passfaces password is easier to remember compared to textual passwords. Results also showed that Passfaces took a much longer login time than textual passwords. Empirical and comparative studies by Davis et al. [15] showed that, in Passfaces the user's choice is highly affected by race, the gender of the user and the attractiveness of the faces. This will make the Passfaces password somewhat predictable.

Sobrado and Birget [16] proposed graphical passwords schemes that overcome shoulder-surfing attacks. In their first scheme which they called “triangle scheme”, a user needs to select their pass-object among many displayed object. To be authenticated, a user needs to recognize all the pre-selected pass-object which was selected during the registration phase. Users are required to click inside the convex-hull which is formed by the pass-object (Figure

3). To make the password space large enough and difficult to guess, Sobrado and Birget suggested using 1000 objects on the login process. However, by increasing the number of objects, the display becomes more crowded and making it difficult to find the pass-object. On the other hand if the number of objects is reduced, the size of password space will become smaller thus making it easier to crack and guess.

Sobrado and Birget also produced a second scheme called "moveable frame scheme". This scheme is similar to their previous scheme but, only three pass-objects were involved in this technique. One of the pass-objects is placed into the moveable frame. To be authenticated, the user needs to rotate the frame until all the pass-object is located in a straight line (Figure 4). To minimize the likelihood of logging, Sobrado and Birget suggest repeating the process several times by clicking or rotating it randomly. However, this step is unpleasant, confusing and time consuming since there are too many non-pass objects.

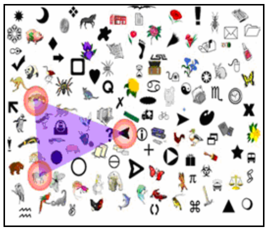


Figure 3: Convex-hull shoulder-surfing resistant

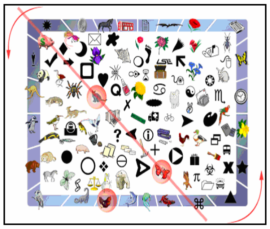


Figure 4: Moveable frame scheme

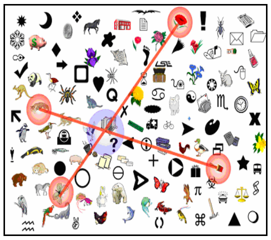


Figure 5: The special geometric configuration

Sobrado and Birget last scheme is called "special geometric configuration". In this scheme four pass-objects are involved to form an intersection point (Figure 5). To be authenticated, user only required to click the object nearest to the intersection point.

Hong et al. [17] proposed a scheme called Pict-O-Lock as shown in Figure 6. For the purpose of picture memorability, Hong et al. allowed users to choose their own words to associate with each pass-object variant. For example, "3" can be used to be associated with a pass-object variant which exhibits a shape similar to the shape of "3"; this facilitates the task of password recall. However, this significantly extends the process of password registration.

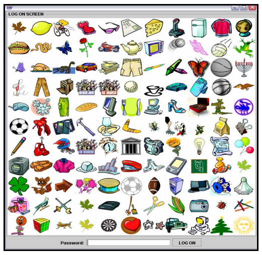


Figure 6: Pict-O-Lock scheme

To arrange the pictures systematically, Hong et al. used a grid based picture arrangement and each time the login process began, the images displayed on the screen are generated randomly by the program. To protect against brute force attacks, Hong et al. used many decoy images in their scheme. To prevent shoulder-surfing attacks, this scheme requires several verification processes. Apparently this process is significantly time consuming and tedious, therefore might not be a choice for users.

Dhamija and Perrig [18] proposed a scheme using a hash visualization technique on the abstract images. The scheme is called "Déjà vu" (Figure 7). 20 participants were involved in this study. The participants were asked to create the Déjà vu password by selecting 5 images from a challenge set of 25 images. At the same time, the participants were required to create the text-based password which is at least 6 characters long. After the password creations were finished, participants need to authenticate themselves using both techniques. According to their studies, the result showed that it took more time to create a graphical password compared to traditional approach. Besides that, 90% of the authentication using Déjà vu succeeded compared to 70% using the traditional approach. However, due to the larger amount of pictures stored on the server side, the authentication process can be slow due to network traffic delay. Even though the size of the password space of Déjà vu is much smaller compared to text-based password, it cannot be concluded that Déjà vu scheme is easy to remember.

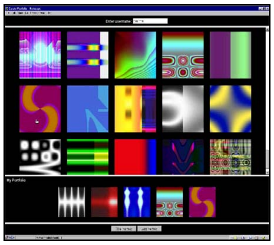


Figure 7: Déjà vu scheme

3.2. Recall-based Techniques

G. E. Blonder [7] the founder of graphical password scheme, designed a scheme in which a user is presented with one predetermined image. A user has to locate one or more tap regions on the displayed image as their password. To be authenticated, user has to click on the approximate areas of those tapped regions with the selective order (Figure 8).

The major problem with this scheme is related to the memorable password space. Since Blonder not particular studied this area, the memorable password space is still uncertain. Apart from that, users cannot randomly click the background of the image since it will make the created password difficult to recall because of the simple background of the image.

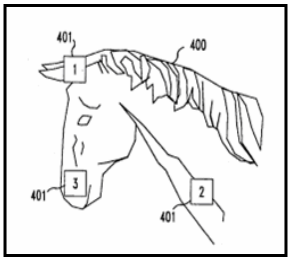


Figure 8: Blonder scheme

VisKey is a recall-based authentication scheme that currently has been commercialized by SFR Company in Germany [19]. This software was designed specifically for mobile devices such as PDAs. To form a password, users need to tap their spots in sequence (Figure 9).

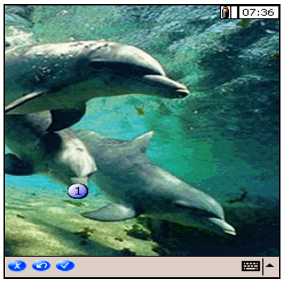


Figure 9: VisKey SFR

The problem with this technique is the input tolerance. Since it is difficult to point to the exact spots on the picture, Viskey permits all input within a certain tolerance area around it. The size of this area can be pre-defined by users. Nonetheless, some precautions related to the input precision needs to be set carefully, as it will directly influence the security and the usability of the password. For a practical setting of parameters, a four spot VisKey can offer theoretically almost 1 billion possibilities to define a password. However, is not large enough to avoid the off-line attacks by a high-speed computer. At least seven defined spots is needed in order to overcome the brute-force attacks.

Passlogix Inc. [20] is a commercial security company located in New York City USA. Their scheme called Passlogix v-Go uses a technique known as "Repeating a sequence of actions" which means creating a password by a chronological situation. In this scheme, user can select their background images based on the environment, for example in the kitchen, bathroom, bedroom or etc (Figure 10). To enter a password, user can click and/or drag on a series of items within that image. For example in the kitchen environment, user can prepare a meal by selecting cooking ingredients, take fast food from fridge and put it in the microwave oven, select some fruits and wash it in washbasin and then put it in the clean bowl.

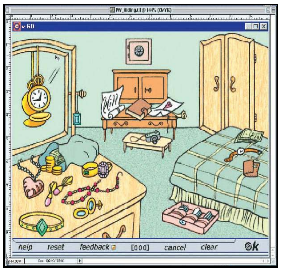


Figure 10: Passlogix scheme

Other environments such as cocktail lounge allow users to select their favorite vodka, brandy or whiskey and mix it with other cocktails. This type of authentication is easy to remember and fun to use. Nevertheless, there are some disadvantages such as the size of password space is small. There are limited places that one can take vegetables, fruits or food from and put into, therefore causing the passwords to be somewhat guessable or predictable.

Empirical studies by Wiedenbeck et al [21, 22] extended Blonder's design. Their scheme called "PassPoints" expanded the clickable area of the traditional image background introduced by Blonder.

As a result, users can click anywhere on an image to form a password (Figure 11). The tolerance area of each selected location is also calculated to ensure it fulfills the usability and security requirements. A user is authenticated if he or she accurately clicks all the selected locations within the tolerance of each selected area. Since the authors allow the usage of any types of images, the amount of memorable password space is relatively large compared to textual passwords. The authors also conducted a comparative users study between the users of alphanumeric password and graphical passwords. The result showed that the PassPoints users had more difficulties to learn the password and it also took more time to input their passwords compared to alphanumeric users.

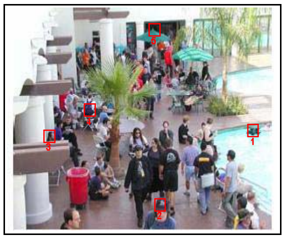
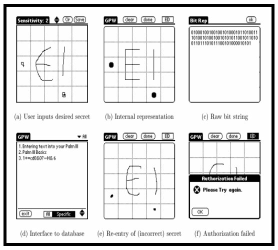


Figure 11: PassPoints scheme

Jermyn et al. [23] proposed a scheme, known as "Draw-A-Secret (DAS)". This scheme is based on a two dimensional grid, users have to draw something to represent their password. Each of the grids coordinates from the drawn pictures is stored in the order of the drawing. To be authenticated, user needs to redraw the picture again. If the drawing lines up at the same grids coordinates with the proper sequence, then the user is authenticated (Figure 12). There are some advantages when using a grid as the background for the drawing. First, the users can draw a password as long as they wish. Second, grid based techniques also lessens the need for the graphical database storage on the server side and reduced the traffic loads without transferring an images through network. Furthermore, the full password space for a grid based schemes is much better than traditional textual passwords.



(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 12: Jermyn et al. DAS scheme

4. Usability Features in Graphical Password Schemes

Currently, there are number of existing graphical password schemes available on the Internet. Some of them have already been commercialized. In this paper, twelve schemes are studied and compared using the comparative study method. The selected schemes are shown in Table 1.

Table 1: The usability features on graphical password

Graphical Password Schemes	Techniques		Usability Features on Graphical Password												
			Memorability												
	Recognition	**Recall**	Meaningfulness	Human faces	Organized by theme	User assign image	Icon based	Abstract image	Navigating image	Freedom of choice	**Efficiency**	**Input reliability & accuracy**	**Easy and fun to use**	**Grid based**	**Drawing password**
Jansen et al.	√		√		√						**X**		√	√	
Passfaces ™	√			√		√					**X**	√	√	√	
Triagle	√						√				**X**		√		
Movable Frame	√						√				**X**		√		
Intersection	√						√				**X**		√		
Pict-O-Lock	√						√				**X**	√		√	
Déjà Vu	√							√			**X**		√	√	
Blonder		√	√			√				√	**X**				
VisKey SFR		√	√			√				√	**X**	√			
Passlogix v-Go		√	√		√				√		**X**		√		
PassPoints		√	√			√				√	√	√	√	√	
DAS		√	√									**X**		√	√
√ = Yes **X** = No Blank = not mentioned															

There are various characteristics studied to find the similarities and the differences of usability features among each of the schemes. As depicted in Table 1, there are six main usability features that have been used on the existing graphical password schemes. The memorability of the password is categorized into eight sub-features: meaningfulness, human faces, organized by theme, user assigned image, icon based, abstract image and freedom of choice. The "√" symbol denotes that the scheme has that particular feature. Meanwhile, the "**X**" symbol shows that the scheme does not have the particular feature.

By analyzing Table 1, it is found that seven of the existing schemes are recognition-based technique while the remaining five are recall-based. To make the pictures more memorable, six of the schemes used picture meaningfulness which is a sub-feature of picture memorability and five of these are recall-based. Icon based image and user assigned image is used by four schemes, while freedom of choice is adopted by three. Two schemes use the organized by theme sub-feature in which user can select their graphical password based on the theme. The remaining sub-features which are human faces, abstract image and navigating through image have single adoption.

The PassPoints scheme is the only scheme that can be considered as an efficient scheme due to low time consumption in authenticating users. The password input reliability and accuracy is one of the enabling features that increases the usability of graphical password scheme. As can be seen a total of four schemes implemented this feature. To make the picture displays well arranged six schemes applied the grid based picture arrangement. As is well-known, pictures crowded together will affect the usability of the scheme. Draw-A-Secret (DAS) also applied the grid based feature; the only difference is that DAS draws the password and it is implemented on a canvas which uses coordinates behind the grid line. Eight of these schemes are considered as easy and fun to use; six recognition-based and two are recall-based.

Among all of the features, the highly selected feature is the easy and fun to use. Hence, this feature needs to be included in the development of our graphical password scheme. The developer must ensure the scheme easy and fun to use, for example in the password creation and input phase, the developer can use the challenge-respond or training session technique in order to provide a feasible and user friendly platform of creating password. To increase the password memorability, only the meaningfulness, human image, organize by theme and freedom of choice sub-features will be implemented on our scheme. To make the selected area accurately pointed, we will divide the selected picture into a grid based arrangement. The time factor (efficiency) will not be considered in the development of the graphical password scheme. As we can see, almost all of the available schemes are time consuming. However, we will try to minimize the time factor by giving a training session especially in the process of creating and learning the password.

5. Security Features in Graphical Password Schemes

There are six main security features that are used on existing graphical password schemes. The features are shown in Table 2. The possible attack method is not classified as the security feature, it is only for the guidance and supporting reason of why the security features is needed. The possible attack method is divided into six types of attacks which are brute force, dictionary, guessing, spyware, shoulder-surfing and social engineering. These are the current active attack methods in graphical authentication environment. From Table 2, it can be concluded that all of the existing schemes are vulnerable to brute force, guessing and shoulder-surfing attack. As we can see, the Draw-A-Secret (DAS) scheme is the only scheme that is capable of defending against brute force attack. This is because DAS provides the largest password space compared to other schemes [23]. The Pict-O-Lock scheme has a strong resistance to guessing. This scheme used the image variation where a same image is displayed in different colors. Overall, the existing schemes have strong security mechanisms to counter dictionary, spyware and social engineering attacks. In order to protect against brute force and guessing, the scheme needs to provide a large password space. The larger the password space, the harder for brute force and guessing to succeed. As depicted in Table 2, seven schemes provide a large size of password space to their scheme. To increase the security of graphical authentication, seven schemes used randomly assigned image and decoy images features. The purpose of using these features is mainly to defend against shoulder-surfing attacks. As we can see, almost all of the schemes using these features are less susceptible to shoulder-surfing attacks. A total of four schemes used the hash visualization function. In order to strengthen the security of the selected password, some of these schemes combined hash and salt functions.

Among all of these recognition and recall based security features, we will select the large password space, hash function and decoy images features to protect against the possible attack methods in graphical authentication environment. The repeat verifications, randomly assign images and image variation will not be used in the development of our scheme. As we can see, by repeating the process of verification it will make the authentication process slower which will affect scheme usability. We strongly agree that applying the image variation feature, users (especially those with weak vision), will have difficulty to recognize or recall their passwords. We agreed not to implement the randomly assigned images because it will decrease the memorability of the password, for example in the case of the appeared images are not suitable or disliked by the users.

Table 2: The attacks and security features on graphical password

Graphical Password Scheme	Techniques		Possible Attack Methods						Security Features on Graphical Password					
	Recognition	**Recall**	Brute force	Dictionary	Guessing	Spyware	Shoulder-surfing	Social	**Large password space**	**Randomly assign images**	**Hash function**	**Image variation**	**Decoy images**	**Repeat verification**
Jansen et al.	√		√	**X**	√	**X**	√	**X**	✗	✓	✓		✓	
Passfaces ™	√		√	√	√	**X**	√	**X**	✗	✓			✓	
Triagle	√		√	**X**	√	**X**	**X**	**X**	✓	✓			✓	
Movable Frame	√		√	**X**	√	**X**	**X**	**X**	✓	✓			✓	
Intersection	√		√	**X**	√	**X**	**X**	**X**	✓	✓			✓	
Pict-O-Lock	√		√	**X**	**X**	√	**X**	**X**	✓	✓		✓	✓	✓
Déjà Vu	√		√	**X**	√	**X**	√	**X**	✗	✓	✓		✓	
Blonder		√	√	**X**	√	**X**	√	**X**	✓					
VisKey SFR		√	√	**X**	√	**X**	√	**X**	✗					
Passlogix v-Go		√	√	**X**	√	**X**	√	**X**	✗					
PassPoints		√	√	**X**	√	**X**	√	**X**	✓		✓			
DAS		√	**X**	√	√	**X**	√	**X**	✓		✓			
√ = Yes **X** = No Blank = not mentioned														

6. Approach

Our approach is to provide a system with balanced usability and security features. The word balanced does not refer to the equal number of usability and security features, but based on the system itself. The system must not focus too much on either usability or security. Our system will be implemented in a controlled lab environment. There are 63 participants involve in this experiment. The participants are staffs, undergraduate and postgraduate students of Faculty of Computer Science and Information Systems (FSKSM) University of Technology Malaysia. To validate the password memorability, we will use the longitudinal trial testing method. The memorability testing will take approximately six weeks to finish. During this time, participants are required to input their password at different time intervals, to test their memorability and retention. The memorability of the password will be evaluated based on the number of failure and successful login into the system. The validation of the security features will be based on the capability of the scheme to thwart the six possible attack methods. We will apply the large password space, hash function and decoy images security features in order to fight against these attacks. Since a user will be locked out after five unsuccessful attempts, we strongly believe that the number of combinations will make it difficult for manual password guessing and brute force attacks. To fight against dictionary attacks, we will employ hash visualization function with the combination of salt technique. To overcome the shoulder-surfing attack, we will adopt decoy images into the login process.

7. Conclusions and Future Work

In this paper, we have conducted a comprehensive study of existing graphical password techniques. We classified the current graphical password techniques into two categories; recognition-based and recall-based techniques.

We have found that the graphical passwords schemes is more difficult to be cracked by using the traditional attack methods such as brute force search, dictionary, social engineering and spyware attack. Some user and empirical study have proven that human are better at memorizing graphical passwords compared to textual characters passwords [5, 14, 18]. Our approach is to provide a scheme that will be able to satisfy the users' needs and requirements. We strongly believe that, to achieve such condition the usability and security features must be balanced.

Acknowledgement

The authors would like to thank University of Technology Malaysia (UTM) and Ministry of Higher Education Malaysia (MOHE) for funding this work and the involving research.

References

[1] A. Adams and M. A. Sasse, "Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures", *Communications of the ACM*, vol. 42, 1999, pp. 41-46.

[2] K. Gilhooly, "Biometrics: Getting Back to Business", in Computerworld, May 2005.

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

[4] M. Kotadia, "Microsoft: Write down your passwords", *In ZDNet*, Australia, 2005.

[5] R. N. Shepard, "Recognition memory for words, sentences, and pictures", *Journal of Verbal Learning and Verbal Behavior*, vol. 6, 1967, pp. 156-163.

[6] L. F. Cranor and S. Garfinkel, "Secure or Usable?", *IEEE Privacy and Security*, Vol. 2, 2004, pp. 16-18.

[7] G. Blonder, "Graphical Password", *In Lucent Technologies, Inc.*, Murray Hill, NJ, United States Patent 5559961, 1996.

[8] Furkan Tari, A. Ant Ozok, Stephen H. Holden, "A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords", *Proceedings of the second symposium on Usable privacy and security SOUPS '06*. 2006.

[9] B. Ives, K.R. Walsh and H. Schneider, "The Domino Effect of Password Reuse," *Communications of the ACM*, Vol. 47, 2004, pp. 75-78.

[10] L. O' Gorman, "Comparing Passwords, Token and Biometrics for User Authentication," *In Proceedings of the IEEE*, Vol. 91, 2003, pp. 2021-2039.

[11] J. Yan. A. Blackwell, R. Anderson and A. Grant, "Password Memorability and Security: Empirical Result", *IEEE Privacy and Security*, Vol. 2, 2004, pp. 25-31.

[12] Jansen, W., Gavrila, S., Korolev, V., Ayers, R., Swanstrom, R., "Picture Password: A Visual Login Technique for Mobile Devices", *NISTt NISTIR 7030*, 2003.

[13] Real User Corporation, Passfaces ™, http//:www.realuser.com, Accessed on January 2007.

[14] S. Brostoff and M. A. Sasse, "Are Passfaces more usable than passwords: A Field Trial Investigation", *In People and Computers XIV – Usability or Else: Proceedings of HCI*. Sunderland, U.K.: Springer –Verlag, 2000.

[15] D. Davis, F. Monrose and M.K. Reiter, "On User Choice in Graphical Password Schemes", *In Proceedings of the 13th USENIX Security Symposium*. California, 2004.

[16] Sobrado, L and Birget, J. *"Graphical Passwords,"* The Rutgers Scholar , An Electronic Bulletin of Undergraduate Research, Rutgers University, New Jersey, Vol. 4 (2002), http://rutgersscholar.rutgers.edu/volume04/sobrbirg/sobrbirg.htm, Accessed on January 2007.

[17] 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.

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

[19] SFR IT - Engineering, http://www.sfr-software.de/cms/EN/pocketpc/viskey/, Accessed on January 2007.

[20] Passlogix, http://www.passlogix.com, Accessed on February 2007.

[21] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "Authentication Using Graphical Passwords: Basic Results", *In Human-Computer Interaction International (HCII 2005)*, Las Vegas, NV, 2005.

[22] Wiedenbeck, S., Waters, J., Birget, J. C., Brodskiy, A., Memon, N., "PassPoints: Design and Longitudinal Evaluation of a Graphical Password System", *International Journal of Human-Computer Studies*, 63, 2005, pp. 102-127.

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