Graphic-Text Authentication of a Window-based Application

Ayannuga Olanrewaju O.
Dept. of Computer Technology
Yaba College of Technology
PMB 2011 Yaba, Lagos, Nigeria.

Folorunso Olusegun
Dept. of Computer Science
University of Agriculture
Abeokuta, Nigeria.

ABSTRACT
Password systems have fallen under several attacks in the last decade. Shoulder surfing, key logging, brute force attack and many others have been identified as threats for the security of systems. The conventional (traditional text passwords) are often forgotten by users. In view of this, users often write them down on sheet of paper or any other surface for memorability. Users tend to choose short and simple passwords in place of long and complex passwords. Graphical passwords have been introduced as an alternative to text passwords. This is because humans tend to remember visuals better than text. This paper attempt to highlight the existing graphical password schemes noting their strength and weaknesses, their usability features and then develop a new graphical password system that combines both graphic and texts passwords to fortify the authentication process on desktop systems.

General Terms
Security, Authentication

Keywords
Brute force, Key logging, Password, Shoulder surfing

1 INTRODUCTION
The advent of information and communication technology has brought a great change in the way information is handled. Our businesses, educational systems, manufacturing industries, tourism and even governance have been positively affected by IT. A large percentage of the world's data is being managed by platforms provided by Information Technology. Speed, reliability, high performance, robustness etc. have been highlighted as advantages of using these platforms.

However, the increasing dependence on Information and communication technology to create, access, process and transmit data has brought about a wide range of security threats. Illegal access to data by various means has been a hard nut to crack for system developers, programmers and even the end users. All hands must be on deck to ensure that information be guarded jealously for it not to get into the wrong hands. Hence, need for authentication.

Authentication plays an important role in protecting resources against unauthorized use. Authentication is a function where a user presents some credentials to the system. If the system recognizes this set of credentials or the credentials match a given set on the system, then the user is said to be authorized otherwise the user is not authorized *[Michael Burrows, Martin Abadi, Roger Needham, 1990]*. Kurose and Ross, 2003 define authentication as the process of proving one's identity to someone else. Authentication is needed to let the system perform some tasks for the user. The user needs to be authorized to request services from the system.

Many authentication processes exist from simple password based authentication system to costly and computation intensive Biometric authentication systems. Still, the most widely used authentication system is based on the use of text passwords (Art Conklin, Glenn Dietrich, Diane Walz, 2004). The password is a very good and strong authentication method still used up to now but because of the huge advance in the uses of computer in many applications as data transfer, sharing data, login to emails or internet, some drawbacks of conventional password appears like stolen the password, forgetting the password, weak password, etc so a big necessity to have a strong authentication way is needed to secure all our application as possible, so a researches come out with advanced password called graphical password where they tried to improve the security and avoid the weakness of conventional password (Ali Mohammed, 2008).

Text based passwords are not secure enough for many applications that enforce security by access control mechanisms. Authentication based on text-based passwords has major drawbacks. Text passwords are subject to dictionary attacks; and text passwords can be stolen by malicious software (e.g. key loggers) when being entered from keyboards.

In addition, a user could be persuaded to visit a forged website and enter their passwords. The site captures the login details. This is called phishing. Such an attack is made possible in part due to the fact that text passwords do not allow users to authenticate a server; by design they provide only one-way user authentication, and server authentication is not a design objective of text passwords alone.

To combat the various security inadequacies, graphical password systems have been proposed as a possible alternative to text-based passwords, motivated particularly by the fact that humans can remember pictures better than text. Psychological studies have shown that people can remember pictures better than text (R.N Shepard, 1967). Pictures are generally easier to be remembered or recognized than text, especially photos, which are even easier to be remembered than random pictures (Xiaoyuav Suo 2006).

The increasing threats to computer systems have called for a more focused effort to attend to security requirements for the underlying systems. Over the years, security practitioners and researchers have made studies in protecting systems, individual users and digital assets. However, the problem arises that, until recently, security was treated wholly as a technical problem, and the system user was not factored into the equation.

Users interact with security technologies either passively or actively. For passive use, understandability may be sufficient for users. For active use, people need much more from their security solutions and usability solutions such as ease of use, memorability, usability, efficiency, effectiveness and satisfaction (Ali Mohammed, 2008).

Nowadays there is an increasing recognition that security problems are also fundamentally human-computer interaction issues (Dourish, 2004 and Patrick *et al* 2004).

Traditional text passwords are used widely for authentication, but other methods are also available today, including biometrics and smart cards. However, there are problems of these alternative authentication technologies.

Biometrics raise privacy concerns and smart cards usually need a Personal Identification Number (PIN) because cards can be lost. As a result, passwords are still dominant and are expected to continue to remain so for some time as an authentication process (Coventry *et al* 2003, Jain *et al* 2000 and Brostoff *et al* 2000). In addition, the high cost of implementing other authentication systems (i.e. smart cards, token and biometrics) has made the textual passwords the preferable choice on middle-level systems.

However, the conventional text passwords have usability challenges, and these challenges tend to translate directly into security problems. That is, users who fail to choose and handle passwords securely open holes that attackers can exploit Brown *et al.* 2004, Sasse *et al*. 2001,Dhamija *et al* 2000, Feldmeier *et al.* 1990, Klein *et al* 1990 and Morris *et al.*1979)

Generally, password systems are faced by problem of conflicting requirements. First is the fact that passwords should be usable and easy to remember. The second requirement is for it to be secure (i.e. they should be hard to guess, be changed frequently, it should not be written down.)

Largely, the password problem arises from the inability of humans to store things in memory for a long time. "There is no doubt that over time, people are going to rely less and less on passwords. People use the same password on different systems, they write them down and they just don't meet the challenge for anything you really want to secure" (Bill Gates, 2006)

This password vulnerability is related in part to the practices of users, and in part to inherent weaknesses in the passwords themselves, such as the ease with which passwords may be shared or stolen (Adams & Sasse, 1999; Besnard & Arief, 2004; Ensor *et al.*, 2004).
In addition to the weaknesses of password properties and usage, regulatory pressures look set to render simple username plus password protocols obsolete. For example, the US banking regulator, the FFIEC, published guidelines making 'strong authentication' mandatory for identity verification on all regulated institutions' web sites (FDIC 2005). Inertia may lead institutions and users to regret change, but the *status quo* with passwords is no longer an option; conventional username and password protocols must be changed or augmented to meet regulatory requirements.

Once a password has been chosen and learned the user must be able to recall it to log in. But, people regularly forget their passwords. Breakdown and interference explain why people forget their passwords. Items in memory may compete with a password and prevent its accurate recall (Wixted *et al* 2004).

If a password is not used frequently, it will be even more susceptible to forgetting. A further complication is that users have many passwords for computers, networks, and web sites. The large number of passwords increases interference and is likely to lead to forgetting or confusing conventional passwords (Wixted *et al* 2004).

Graphical Passwords are been developed to address the aforementioned problems. This passwords system demands the user to click on certain points on an image, a set of images to gain access to be actually authenticated.

Topical issues emanating from the graphical password idea is the creation and learning of the graphical password because from a human viewpoint, the problem of creating a password is making it memorable so that the user can retrieve it later.

In a graphical password system, a user choosing click locations in an image needs to choose memorable locations since there are two issues in memorability, the nature of the image itself and the sequence of click locations, the memory because most existing graphical password systems can be classified as being based on either recognition or cued recall. Recognition involves identifying whether one has encountered an item before. In a graphical password system based on recognition, the user has to be able only to recognize previously seen images. By contrast, pure recall is retrieval without external cues to aid memory, e.g. remembering a textual password that one has not written down and the efficiency and perception of efficiency are important in password systems because users want quick access to systems.

2 LITERATURE REVIEW

Depending on the type of graphical background being used, graphical password schemes can be divided into two categories, which are, the **Image Based Scheme** and **Grid Based Scheme**. Image based scheme uses single image or multiple images to construct graphical passwords, whereas grid based scheme uses grid as the background in composing of graphical passwords.

The first graphical password scheme was introduced by Greg Blonder (1996). In his scheme, a user is offered with one preset image, which is displayed on screen. The user is then required to select one or more fixed positions, which is recognised as "tap regions" on the displayed image, in a particular order to access the system. This scheme was not resistant to shoulder surfing because as the users clicking on the image may make the users' actions easier to capture and the attacker can gain the access to the system with the same password.

Draw – A – Secret (DAS) was suggested by Jermyn *et al.* (1999). DAS requires a user to draw a secret design on a grid as a way to input a password. 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.

To improve the security of Draw-A-Secret technique, Thorpe and van Oorschot (2004) proposed a "Grid Selection" technique. The selection grid is an initially large, fine grained grid from which the user selects a drawing grid, a rectangular region to zoom in on, in which they may enter their password. This would significantly increase the DAS password space. But this technique also not resistant to shoulder surfing because as the users re-draw the picture on the grid may make the users' actions easier to capture and the attacker can gain the access to the system with the same password.

Syukri *et al* (1998) proposes a system where authentication is conducted by having users drawing their signature, using mouse. Their technique included two stages, registration and verification. During the registration stage: user will first be asked to draw their signature with mouse, and then the system will extract the signature area and either enlarge or scale-down signatures, rotates if needed, (also known as normalizing). The information will later be saved into the database. The verification stage first takes the user input, 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 database. According to the paper, the rate of successful verification was satisfying. The biggest advantage of this approach is that there is no need to memorize one's signature and signatures are hard to fake. However, not everybody is familiar with using mouse as a writing device; the signature can therefore be hard to drawn. One possible solution to this problem would be to use a pen-like input device, but such devices are not widely used, and adding new hardware to the current system can be expensive. We believe such technique is more useful to small devices such as PD. A.F.Syukri *et al* (1998).

Birget et al. (2003) introduced Passpoints. Pass points allow a user to click on any point inside a background image as an indication of his or her password entry. Story scheme was suggested by Davis *et al.* (2004), in which the user's password is a sequence of images selected by the user through storytelling.

Déjà Vu was proposed as a graphical authentication scheme based on Hash Visualization technique. In their system, user will be asked to select certain number of images from a set of random pictures generated by a program. Later, user will be required to identify the pre-selected images to be authenticated. The results showed that 90% of all participants succeeded in the authentication using their technique, while only 70% succeeded using text-based passwords and PINS. The average login time, however, is longer than the traditional approach, but has a much smaller failure rate.

A drawback is that the server needs to store a large amount of pictures, which may have to be transferred over the network, delaying the authentication process. Another weakness of this system is that the server needs to store the seeds of the portfolio images of each user in plain text. Interface-wise, the process of selecting a picture from picture database can be tedious and time consuming for the user. (Dhamija *et al* 2000).

"Picture password" was suggested by Jansen *et al.* (2003) In creation of a picture password, a user is requires to select a predefined theme, such as 'seashore', 'kitten' and so on, which consists of thumbnail photos. The user are then required to selects a sequence of thumbnail photos as a password.

Man *et al.* (2003) suggested another shoulder surfing resistant solution. In creation of a password, a user has to choose a number of pass-objects, and has to remember the textual characters that are related to each variant of their pass-objects. During login, the pass-objects, which are randomly generated, are displayed on the screen with about 400 to 500 decoy objects. The user has to input a string of textual characters, in accordance to the order of the pass-objects.

V-GO is commercial authentication software by Passlogix Inc. (2004). V-GO allows a user to create graphical password by navigating through an image. To set or enter a password, a user can click and/or drag on a series of items within that image.

In 2008, this model is proposed based on trying to gather all the usability features, like ease of use, ease to create, ease to memorize, and ease to learn and acceptable design and layout in one algorithm, during registration, the user will select three pictures as a password and then sort them according to the way he wanted to see them in login phase.

In login phase the password of the user will mixed with seventeen color pictures to create more usability. Around thirty people participate in trial version. According to them, 40% believed the algorithm is ease to use, 50% believed on ease to creation, 55% found the new algorithm easy to memorize, 57% user agree the algorithm is easy to learn and at last around 53% found the design and screen layout acceptable. As the algorithm is very new, there is no special drawback in any survey until now.

3 USABILITY COMPARISONS ON RECOGNITION-BASED ALGORITHMS

There are several surveys, which concentrate on usability of different graphical scheme, which the latest one related to one survey which has been done by University Technology Malaysia (Ali Mohammed, 2008). According to this research, the items of usability are easy to use, easy to create, easy to memorize and easy to learn. As the techniques which is been used by recognition, pure and cued schemes are different, so the features in their usability table is not the same. For example, in recognition-based scheme the usage of different pictures is one of the main items. Therefore, the "pleasant picture" is a meaningful item in their usability table.

Row	Recognition Based Scheme	Usability Features										
		Satisfaction									Efficiency	Effectiveness
		Mouse Usgae	Create Simply	Meaningful	Assignable Image	Memorability	Simple Steps	Nice Interface	Training Simply	Pleasant Picture	Applicable	R&A
1	PassFace	Y	Y	N	Y	Y	Y	Y	Y	Y	N	Y
2	Dejavu	Y	Y	N	Y	N	Y	N	Y	N	N	Y
3	Triangle	Y	Y	N	N	Y	Y	N	N	N	N	Y
4	Moveable frame	Y	Y	N	N	Y	Y	N	N	N	N	Y
5	Picture password	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	N
6	Story	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	N
7	Man	N	Y	N	Y	Y	Y	N	Y	N	Y	N
8	Jetafida	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	N

Table 1. Usability Table

4 SYSTEM DESIGN

This paper adopts the combination of both graphic and text password schemes as means of authentication. At the point of login in the interface is shown below

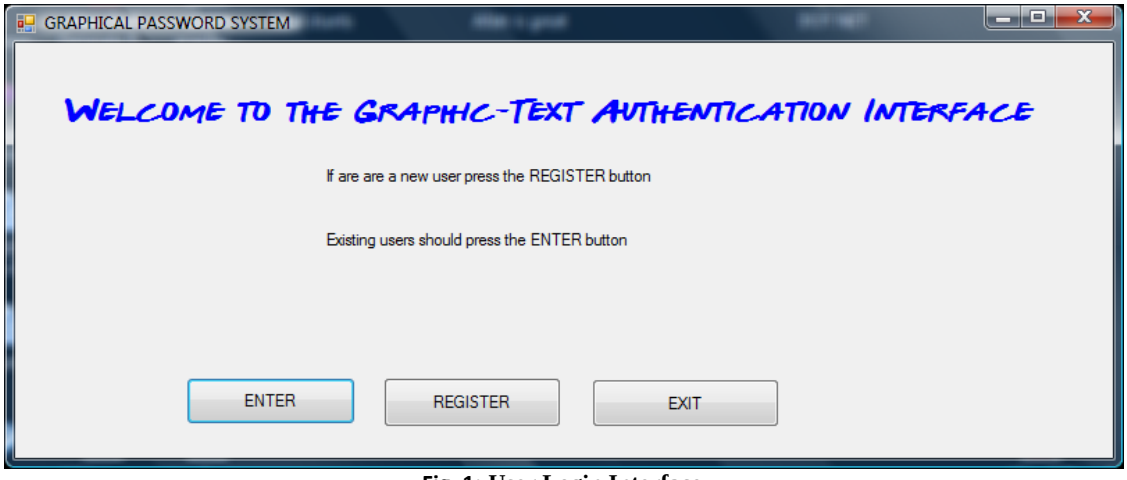

Fig. 1: User Login Interface

A new User will press the REGISTER button for registration process, which allow the new user to register his/her user name which is text password, this cannot be seen by other users but just display ****** for security reason and also display nine images from which the user will select three from as his/her graphic password, the text password is encrypted and then stored into a database while in the other hand the selected images are stored in another database.

Existing Users will press the ENTER button for login process, which display the nine images for graphic password along with the space for the username as shown below

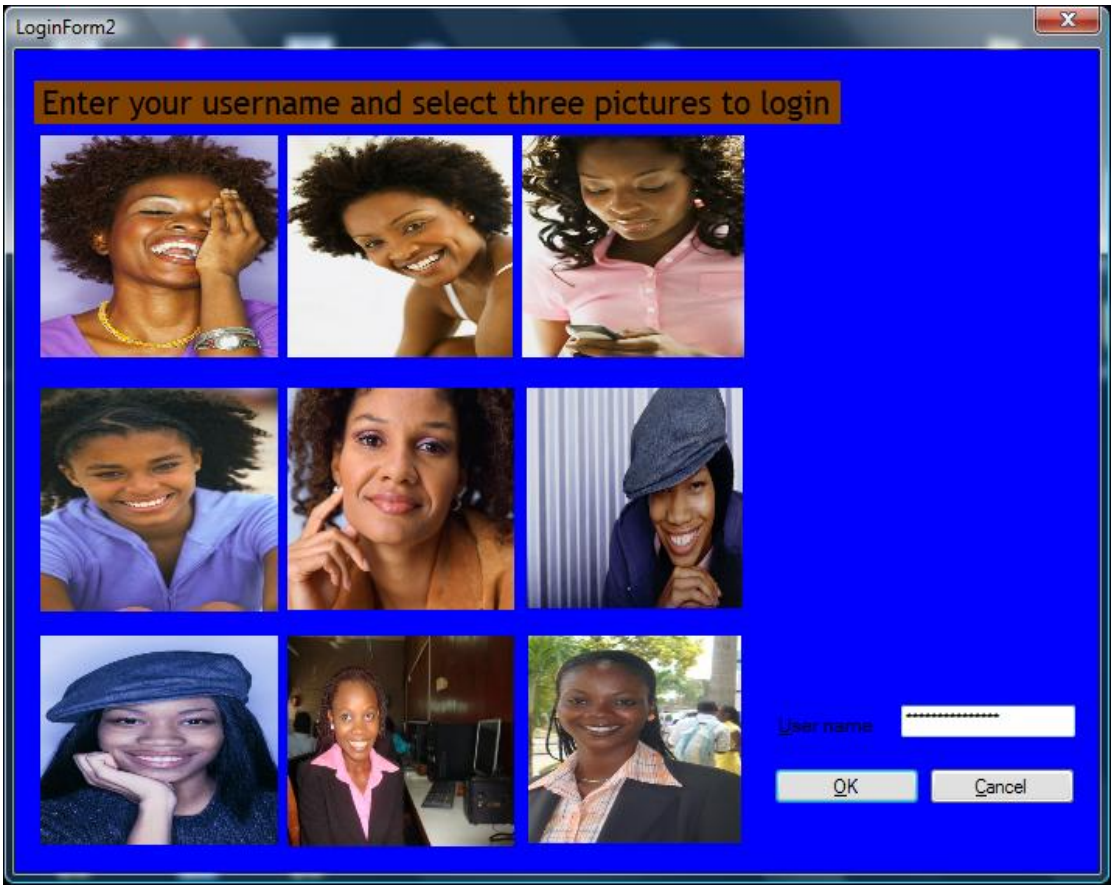

Fig. 2: User Authentication Interface

The User supplies his/her password and then select three images to login into the system

The research adopts the graphical scheme for authentication as a result of its user friendly and security features which makes it more advantageous than the traditional textual passwords. The system is designed based on the recognition-based algorithm. A user is required to login with a username and three picture passwords, which would be selected from a group of ten pictures arranged in rows and columns on the password interface. The password is compared to an encrypted password, which was saved at point of registration. If the password is correct then, the user is granted access to the system.

The registration process requires the intending user to select three pictures, and a username. The password is encrypted and saved to database.

5 RESEARCH MOTIVATION

This project is driven by the fact that there are many weaknesses for existing alphanumeric passwords authentication system. Most problems associated with alphanumeric passwords are related to the recollection of secure passwords.

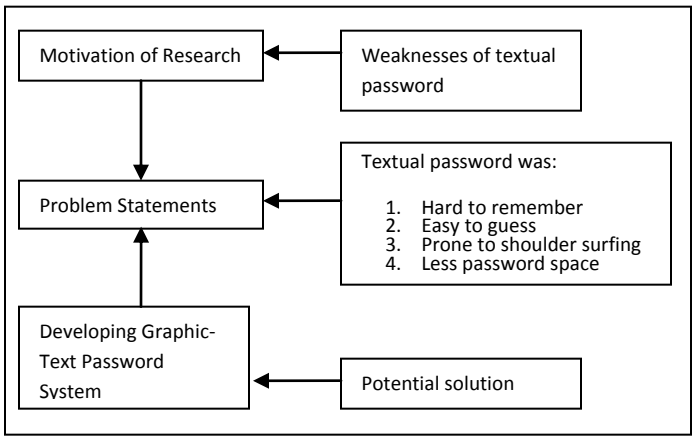

Fig. 3: Research motivation flowchart

6 APPLICATION OF RESEARCH

This research is a model that can be applied to any desktop (window-based) application. Examples include:

- Point of sale applications
- Accounting applications
- Inventory applications
- School management applications
- Result Processing application.

It can also be adapted to log in interface of operating system e.g. windows, Linux.

7 CONCLUSIONS

It has been shown that combining graphics and text can enhance the security of systems while also making it more user friendlier than the traditional passwords systems.

Designing two step user authentication method combine both graphical password and to offer some advantages in countering common attacks against text passwords, such as naive key logging and phishing. Also it counter common attacks usually against graphical password standing alone such as shoulder surfing, eavesdropping and many others as well as counter to passphrase stand alone, this combine strategy method is more usable because the user get familiar with the two steps during training.

This design method will balance the tradeoff between security and usability because it will be difficult for attackers because passphrase question is not known to anybody expect to the real user while it is easier for the real user and that make it more usable, for future work we intend to implement the design to compare it login success rate with other design, check it time of training and getting familiar as well as time of login and compare it with other designs.

8 REFERENCES

[1] Perrig and D. Song, "Hash Visualization: A New Technique to Improve Real- world Security," in *Proceedings of the 1999 International Workshop on Cryptography Techniques and E-Commerce*, 1999.

[2] 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.

[3] Ali Mohamed Eljetlawi, Norafida Ithnin. "Graphical password: comprehensive study of the usability features of the recognition base graphical password methods," Third 2008 International Conference on Convergence and Hybrid Information Technology. 1137-1143. 2008

[4] Brostoff, S. and Sasse, M.A. Are Passfaces more usable than passwords: A field trial investigation. In *People and Computers XIV - Usability or Else: Proceedings of HCI 2000 (Bath, U.K., Sept. 8-12, 2000).* Springer Verlag, 405-424.

[5] Brown, A.S., Bracken, E., Zoccoli, S. and Douglas, K. Generating and remembering passwords. *Applied Cognitive Psychology 18* (2004), 641-651.

[6] Berger, M.A., (2003), "Password Security is a Must for Any Organisation", *Computers in Libraries* 23(5), May2003, p41.6- Coventry, L., De Angeli, A. and Johnson, G. Usability and biometric verification at the ATM interface. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI'03)* (Fort Lauderdale, FL, USA, April 5-10, 2003). ACM Press, New York, NY, 153-160.

[7] Bailey, R. 2001. How reliable is usability performance testing? UI design update

[8] newsletter.http://www.webusability.com/article_reliability_of_usability_testing_10-2001.htm [14 Jan 2008].

[9] Dourish, P. Security as experience and practice: Supporting everyday security. Talk given at the *DIMACS Workshop on Usable Privacy and Security Software*, July 7, 2004.

[10] Dhamija, R. and Perrig, A. Déjà Vu: User study using images for authentication. In

[11] *Ninth Usenix Security Symposium* (Denver, CO, USA, Aug. 14-17, 2000).

[12] http://www.usenix.org/publications/library/proceedings/sec2000/dhamija.html, accessed: Feb. 20, 2005.

[13] D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password

[14] schemes," in *Proceedings of the 13th Usenix Security Symposium*. San Diego, CA, 2004.

[15] Feldmeier, D.C. and Karn, P.R. UNIX password security – ten years later. In *Advances in Cryptology – CRYPTO'89*, Lecture Notes in Computer Science 435, Springer Verlag (1990), 44-63.

[16] Faulkner, L. 2003. Beyond the five-user assumption: Benefits of increased sample sizes in usability testing. *Behaviour Research Methods, Instruments, & Computers, 35(3)*, pp. 379-383.

[17] G. E. Blonder, "Graphical passwords," in *Lucent Technologies, Inc., Murray Hill*,

[18] *NJ*, U. S. Patent, Ed. United States, 1996.

[19] Google (2007) http://www.usabilitypartners.se/usability/what.shtml.

[20] Google (2007) http://www.usabilitypartners.se/usability/standards.shtml

[21] Google(2007) http://www.baychi.org/calendar/files/ISO-Standards-for- Usability/ISO- Standards-for-Usability.pdf

[22] 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.

[23] Jain, A., Hong, L. and Pankanti, S. Biometric identification. *CACM 43*, 2 (2000), 91- 98 28- J. Goldberg, J. Hagman, and V. Sazawal, "Doodling Our Way to Better

Authentication," presented at Proceedings of Human Factors in Computing

[24] Systems (CHI), Minneapolis, Minnesota, USA., 2002.

[25] J.-C. Birget, D. Hong, and N. Memon, "Robust discretization, with an application to graphical passwords," Cryptology ePrint archive 2003.

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

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

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

[29] Sasse, M.A., Brostoff, S. and Weirich, D. Transforming the 'weakest link'– a human/computer interaction approach to usable and effective security. *BT Technical Journal 19* (2001), 122-131.

[30] S. Man, D. Hong, and M. Mathews, "A shoulder-surfing resistant graphical password scheme," in *Proceedings of International conference on security and management*. Las Vegas, NV, 2003.

[31] T. Takada and H. Koike, "Awase-E: Image-based Authentication for Mobile Phones

[32] using User's Favorite Images," in *Human-Computer Interaction with Mobile Devices and Services*, vol. 2795 / 2003: Springer-Verlag GmbH, 2003, pp. pp. 347 - 351.