Evaluating Web-Based User Authentication using Graphical Techniques

M.Z. Jali[1], S.M. Furnell[1,2] and P.S. Dowland[1]

[1]Centre for Information Security & Network Research,
University of Plymouth, Plymouth, UK
[2]School of Computer and Information Science, Edith Cowan University,
Perth, Western Australia
e-mail: info@cisnr.org

Abstract

Graphical techniques are one of the many alternatives proposed to address the weaknesses in the conventional authentication based upon username and passwords. In this paper, two methods of graphical technique, namely ‘click-based’ and ‘choice-based’ are studied in term of their usability for web-based authentication. A total of 21 participants were asked to use prototype implementations and provide feedback. From the data analysed in terms of number of attempts, accuracy, time, pattern and user feedback, it was found that the choice-based method performed better. However, with regard to security, participants rated the choice-based method as weak. Overall, it was found that although both methods have advantages and could be used for authentication, more work needs to be done to balance the issues of security and usability.

Keywords

Graphical Technique, Usability, Security, Web Authentication

1. Introduction

There are many forms of user authentication, but the username/password combination is still the most widely used and accepted method by end-users. This is because the username/password authentication is simple and easy to deploy, involves less cost, and requires no additional hardware. However, this method of authentication is potentially vulnerable to compromise through a variety of means, including dictionary attacks, shoulder surfing, spyware, phishing and even social engineering. In addition to above, there are also problems with users forgetting their passwords, using the same ones for different applications, writing them down in discoverable locations, and generally facing usability issues when required to remember long and complex strings (Brostoff, 2004; Yan *et al.* 2005).

The aim of this study was to investigate the usability of graphical techniques for user authentication in a web-based environment. A user trial was conducted in which participants were asked to use the prototype implementations and provide feedback. The key elements of usability in this study were in terms of users’ accuracy while entering their secrets, the time taken to enter them, patterns of the chosen secrets and users' feedback about the methods.

The paper is arranged as follows. The next section outlines the current state of the art in graphical technique. It highlights the psychological studies about the 'picture superiority effect' and then continues to explain the current research trends for both types used in the study. Section three discusses methodologies used in the study, with section four presenting the results from practical evaluation. Finally, the conclusion and thoughts towards future work are described in section 5.

2. Graphical Technique

The fundamental idea of graphical technique is using images or pictures rather than strings of characters as the basis for the user's secret. From the literature, it was found that among an early attempt to use pictures during authentication was described in the paper by King (1991), entitled 'Rebus Password'. Rebus is a method of association using images or graphics in order to aid remembering sequences of nonsense passwords. In this paper, graphical techniques were grouped into two categories; namely 'click-based' and 'choice-based'. These categories were solely based on the users' actions while carrying out authentication tasks. Briefly, click-based refers to the users' action clicking on areas within a given image, whereas choice-based refers to the action of selecting a series of images from among a larger set of images. Another variation of these graphical techniques is the 'draw-based' method, in which users draw their secret in order to be authenticated.

From various psychological studies, it was found that participants are better at recognising and recalling images compared with recognising and recalling words, phrases or even sentences (Shepard, 1967; Nickerson, 1968; Standing, 1970). It was also claimed that graphical techniques are more secure than conventional passwords since they offer larger secret spaces (Blonder, 1996).

In the click-based method, Blonder (1996) patented his graphical scheme where users' click or tap on the predetermined areas of the given image which is already defined within the system. Following this the 'Passpoints' systems (Wiedenbeck *et al.* 2005a) was developed, which enhanced the original scheme from Blonder by giving users the opportunity to choose their own images and the system itself does not need any predefined click-region or well-marked boundaries. Chiasson *et al.* (2007a) evaluated 'Passpoints' and determined that the scheme was less effective as users had problems while entering their passwords. As a result, Chiasson *et al.* (2007b) introduced the 'Cued Click Point' (CCP). CCP addresses the 'Passpoints' problem by letting users to click once on a series of images with the current click determines the next images. Another variation of CCP was the Persuasive CCP (Chiasson *et al.* 2008a), where a method of persuasion is used in order to advise users to choose more secure passwords. Among the usability studies carried out for click-based method were investigating the level of memorisation (Wiedenbeck *et al.* 2005a; Chiasson *et al.* 2007a), assessing the effect of having multiple passwords (Chiasson *et al.* 2008b), investigating the use of different images (Wiedenbeck *et al.*

2005b; Chiasson *et al.* 2007a), and predicting the click points chosen by users (Golofit, 2007; Thorpe and Oorchot, 2007).

The most familiar choice-based method was the scheme known as 'Passfaces' (Passfaces, 2003). Users have to select images of peoples' faces in order to authenticate. Djamila and Perrig (2000) introduced 'Dejavu', which uses images deployed from the Andrej Bauer's Random Art algorithm, an algorithm where bits of strings are converted into interesting abstract images. Users of this scheme have to remember a number of images and the authentication rounds are dependent on the total number of images chosen by users. De Angeli *et al.* (2003) introduced 'Visual Identification Protocol' (VIP), an ATM-based pictorial password and conducted a usability study to compare it with the conventional ATM-style. Other schemes that could be considered to be in this category are 'Story' by Davis *et al.* (2004), 'PassImages' by Charruau *et al.* (2005) and 'ToonPasswords' by Hinds and Ekwueme (2007). Among the usability studies carried out for this method were the level of memorisation and recall (Djamija and Perrig, 2000; De Angeli *et al.* 2003), image types and effect on screen size (De Angeli *et al.* 2005; Davis *et al.* 2004; Renaud, 2009), the effect of having multiple passwords (Moncur and Lepatre, 2007), and the security against 'description' attack (Dunphy *et al.* 2008).

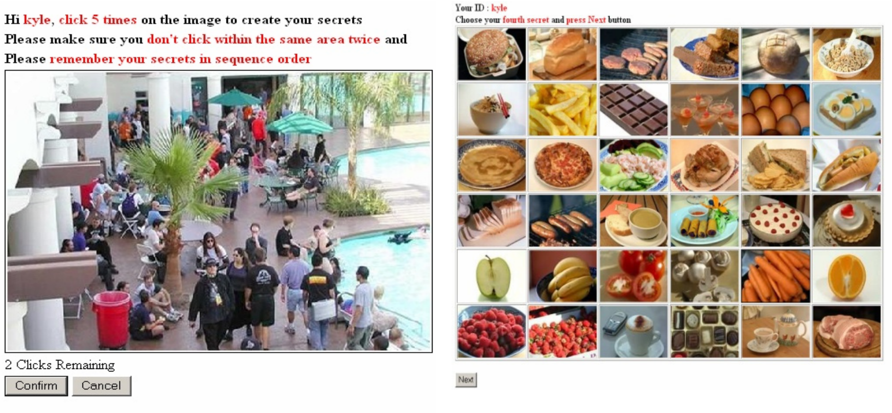
3. Methodology

As far as the prior research is concerned, no study is reported to have investigated the alternative graphical techniques by using the same user sample. With this in mind, a study was undertaken with 21 participants evaluating both the click-based and choice-based methods in terms of performance and user acceptance. Participants needed to complete five main tasks. These started with registering and confirming their 'passwords' for both methods, playing a spot the difference activity (explained below), then re-authenticating using their chosen passwords for both methods, and finally providing feedback by answering a questionnaire. The questionnaire and game activities were done on paper, while the remaining tasks were conducted online using the Internet Explorer (IE 7) browser, with all of the materials (and the trial method itself) having received prior ethics approval.

The development of the click-based method prototype was similar to the original scheme proposed by Wiedenbeck *et al.* (2005), while the choice-based method prototype was developed with consideration and references from 'Passfaces' (2003), Djamila and Perrig, (2000) and De Angeli *et al.* (2003). Both prototypes were developed using a combination of PHP and JavaScript as the interface and MySQL as the platform for storing data.

In the click-based method, the type of image used was similar to those used in Wiedenbeck *et al.* (2005a). The display scale of the image was 450x330 pixels with a selection tolerance (areas in which the click is still valid) of 18x18 pixels. The small tolerance was used as Chiasson *et al.* (2007a) proved that the click-based method would still be usable even with the smaller tolerance. Participants were required to create their passwords by choosing and clicking upon five different points in the given image. They were told not to click their passwords in the same place or within the same tolerance areas and remember their secret in sequences order.

For the choice-based method, the majority of images were taken from FreeFoto (2008) and personal collections. Similar to the click-based method, participants needed to remember five different images grouped within five different themes; namely ‘Animal’, ‘Transport’, ‘Nature’, ‘Food’ and ‘Other’. These categories were chosen because they were common everyday images, easy to recognise and remember. All of these images were manually chosen in order to prevent redundancy. During the registration, a total of 180 images (arranged in 5 separate 6x6 grids) were displayed to the participant, who then needed to choose one image from each theme. This process (displaying 36 images for each category) would continue until participants finished choosing their five images. When it came to the confirmation of their images, only 16 images (arranged in 4x4 grids) were randomly displayed to them, one of which their chosen images. This process continued for the other themes until they finished choosing all of their images within all the themes. The screen shots of both methods are shown in Figure 1.



Hi kyle, click 5 times on the image to create your secrets
Please make sure you don't click within the same area twice and
Please remember your secrets in sequence order

2 Clicks Remaining

Your ID : kyle
Choose your fourth secret and press Next button

Figure 1: Screen shot from the click-based (left) and the choice-based (right) methods

The purpose of the ‘spot the difference’ activity was to provide participants with a mental distraction between the registration and login tasks. This gave them something to do other than to focus on remembering their chosen secrets. It was anticipated that it could take between 3 to 5 minutes to find all 28 differences (eight for each image). After completing the authentication tasks, the participants were asked to complete a three-part questionnaire. The first two parts were about the authentication methods, while the last one was about general opinions and the prototype itself. Among the questions asked were whether it was easy to remember the secrets, whether they had problems during login, whether they would use these methods, and whether they would prefer using their own images as their secrets.

4. Results and Findings

A total of 21 participants (16 males and 5 females) volunteered to participate, all of whom were university students doing various courses, with an average age of 26 years old (Standard Deviation (SD) = 3.9, sample range from 21 to 36 years) and up to 7 years experience of using computers. Since the number of participants is small, the results might not be conclusive. However, with the idea of getting participants to use and evaluate the both methods simultaneously, the results can still be used as an early indication for evaluating the both methods empirically.

The discussion of the results is categorised into five areas, namely number of attempts, timing, accuracy, patterns and user feedback.

4.1. Number of attempts

With the way the study was designed, all participants successfully completed all the authentication tasks (register, confirm and login) and they did not have any major problems creating their secrets. Moreover, as the total number of attempts created by the participants was quite low (with only 21 participants), only general findings will be highlighted here. First, for the choice-based method, all participants were able to complete all of the authentication tasks with only one attempt. Second, for both methods the number of attempts starting from the registration to the login was reduced significantly. This suggested the participants' level of familiarity as high.

By contrast, it was found that the number of recorded attempts for the click-based method was significantly higher, particularly during registration and confirmation. These results were predicted as participants had to carefully click on their secret areas, which sometimes they did not manage to do. When compared with the choice-based method, the above finding could be biased as in the click-based method, participants needed to be accurate while entering their details and they had to remember the information in sequence, but for the choice-based method participants only needed to remember the images themselves.

4.2. Timing

Each participant's registration, confirmation and login duration was recorded to calculate their average time while entering their passwords. The time was measured from the first chosen click/image until the last. Table 1 gives the mean and the SD for each task.

N=21		**Register**	**Confirm**	**Login**
Choice-based	**mean**	38.4	16.4	15.1
	SD	19.5	4.9	4.7
Click-based	**mean**	12.9	8.6	7.7
	SD	6.7	3.9	2.5

Table 1: Mean and SD of time for entering secrets

For the choice-based method, it was clear that participants took longer during registration compared with the confirmation and login tasks. This is because during the registration, participants needed to familiarise (scanning 180 images) and carefully choose their images. As they became familiar with their chosen images, the time for confirmation and login was reduced considerably. For the click-based method, it was found that the mean time for each task was marginal to each other. To summarise, although these times are greater than the time for username/passwords method, they are still likely to be within bounds that are acceptable to users.

4.3. Accuracy

This section measures the correctness of the chosen images and the precision between clicks. For the choice-based method, since all of the participants managed to create their secrets during their first attempt, it could be summarised that the accuracy for both registration and login were very high.

For the click-based method, accuracy refers to how far the original click points during registration are from the click points during confirmation and login (Chiasson *et al.* 2007a). As explained in previous section, the tolerance of 18x18 pixels was used. As long as participants clicked within their secret tolerance area, the click will be accepted. Figure 2 illustrates the distribution of accuracy for all participants during both registration and login tasks (considering only the successful attempts), followed by Table 2 showing the mean and SD of accuracy for successful attempts during both tasks.

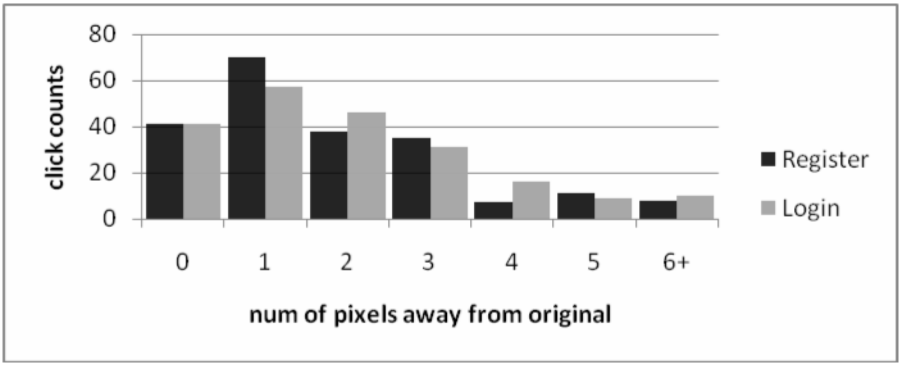


Figure 2: Accuracy during Registration and Login tasks

N=210	**Register**	**Login**
Mean	1.8	2.1
SD	1.7	1.9

Table 2: Mean and SD of Accuracy for Register and Login Tasks

Based upon Figure 2, it was found that participants were good and relatively accurate in entering their secrets within 3 pixels of their original click point. Taking the results of both into consideration, it could be suggested that the click-based method is still usable if it is designed with a tolerance as low as 6x6 pixels (note that the method would be more secure if the smaller tolerance is used, as it produces a larger secret space).

4.4. Patterns

This section highlights the types of images chosen and areas in the image clicked by the participants. The purposes are to investigate and further finding any relationships or patterns while creating the secrets.

For the choice-based method, among of the chosen images were sport cars, flags, eggs, burgers, lion and cat. No relationship was found between the chosen images but it was found that one participant had chosen his images based on the sequences of a story (**car – key – road – coffee - bird**). With regard to patterns, it was found that nearly all of the participants had chosen the images that related to their name. For example, one participant used 'JP' as his username and chosen image letter 'J' as one of his secret images. On top of that, it was found the male participants normally chosen sport cars while the female participants chosen mini cars. Based on observation and informal interviews, it could be summarised that the chosen images were based on two main things; their personal preferences and the recognisability of the image itself. The table below shows the example of secrets (list of images) chosen by them.

Theme	Transport	Other	Nature	Food	Animal
User A	Helicopter	Cutlery	Clock	Eggs	Cow
User B	Mini Cooper	Letter	Bridge	Chocolate	Dog
User C	Sport car	Letter	London	Chips	Penguin
User D	Sport car	Flag	Bridge	Carrot	Lion
User E	Sport car	Letter	Autumn	Cereal	Peacock
User F	Sport car	Letter	Bridge	Raspberry	Bird

Table 3: Example of images chosen by the participants

For the click-based method, the start point of the click and the shape of the clicks are reported. For the start click point, it was found that majority of the participants started their first click in the bottom area of the image where 6 participants clicked on the 'bottom left' area, 4 participants clicked on the 'bottom middle' area and 3 participants clicked on 'bottom right' area. Other preferences for starting the first click were the 'top left' (3 participants) and the 'top middle' (2 participants) of the image, whereas others clicked randomly. With regard to the image used, it could be anticipated that such chosen areas were obvious and recognisable (e.g. people wandering around, beams, umbrellas and etc.). After the first click, no interesting patterns were found since participants likely to click everywhere but one noticeable finding was that participants chosen to click on the objects, as explained earlier. Examples of clicks created by 6 of the participants are shown in Figure 3.

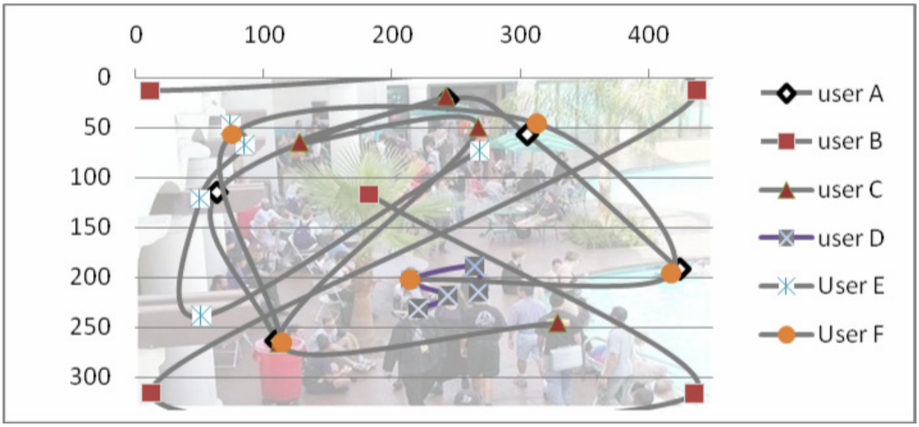


Figure 3: Example of the clicks created by participants

From the distribution of the clicks drawn by the participants, it was found that the shapes of click could be mapped into shapes like ‘U or V’, ‘Z or N’ and ‘L’. Here, it is obvious that the majority of them tended to click on recognisable objects (e.g. beams, bin, people faces, etc.) and the forms of shapes created were also straightforward and predictable. Although clicking on recognisable objects and forming straightforward shapes would make it easy to remember their secrets, if these habits continue it is not possible to build more dictionaries based upon the users’ click points and click patterns and conduct an attack based on these; as already discussed in Thorpe and van Oorschot (2007).

4.5. User Feedback

For the choice-based method, 19 out of 21 participants agreed that they could remember their chosen images well, with all of them did not have any major problems while carrying out the authentication tasks and 16 of them would consider using the method on the web. On the other question, 12 participants think that the method would be vulnerable if they explained their secret images to others and 15 of them preferred the themes to appear in a random order during the login (whereas in the trial themes had been presented in a fixed order) in order to tighten the security of the method.

For the click-based method, 16 participants agreed that they could easily remember their click points in sequence. During the registration and the login tasks, between 11 to 13 participants rated the method was easy to use while the rest rated the method as difficult (note that no training was provided at the start of trial; only description on how both methods work was outlined in the participant briefing sheet). For other questions, 13 out of 21 participants would consider using this method on the web and importantly, the vast majority of them (17 participants) agreed that it is difficult for others to reproduce their login details if they just explain briefly what their secrets were.

Participants agreed the prototypes as suitable to be used for graphical authentication purposes, the usage of images and text as clear, and considered that the instructions during the trial were concise and understandable. The majority of them (20 participants) preferred using their own images rather than the images provided in the prototype, as they claimed it would be more memorable. Encouragingly, participants who did not manage to complete their authentication tasks on their first attempt and rated the click-based method as difficult to use agreed that they would perform better if enough training was provided beforehand. Finally, participants preferred using the click-based method (11 participants) as opposed to the choice-based method (6 participants) for replacing username and password authentication; whereas the remaining rated 'unsure' about it. Overall, it could be summarised that all participants provided positive response with regard to the suitability of the prototype to be used in the web-based environment.

5. Conclusions

There are numbers of lessons to be learnt from the conduct of this study. First and foremost, the number of attempts for the click-based method was rather high compared to the choice-based method. This is perhaps due to the nature of the click-based method itself whereby participants needed to be accurate when clicking on their chosen areas (which they sometimes missed). Second for both methods, participants took longer during the registration (as they want to carefully look and choose their images) but then during the confirmation and login tasks, they performed significantly better. Third, participants had chosen/clicked images or objects that were easy to recognise and formed shapes that were easy to predict. Here, it could be summarised that participants preferred convenience rather than security. Last but not least, participants always gave positive feedback, as well as suggestions on how to improve the methods for future use.

This study confirmed that the problems identified were identical to other studies, regardless of the methods and prototypes used. However, the contribution of this paper is the comparison of both methods within a single study, using a common population of test subjects. With regards to the results and findings, it seems that both are complementary to each other and there is potential for both methods should be combined in order to create a graphical password that is not only usable but also secure. Combining the nature of the click-based method, which can be summarised as 'secure but unusable', and the choice-based method, which can be summarised as 'usable but unsecure', will be the main focus of ongoing research. Appropriate evaluation in terms of usability and security will then be conducted in order to validate the enhanced scheme.

6. References

Blonder, G. (1996) *Graphical password.* 5.559.961. [online]. Available at: http://www.patentstorm.us/patents/5559961.html (Accessed: 10 March 2008).

Brostoff, A. (2004) *Improving password system effectiveness*. PhD. University College London.

Chiasson, S., Biddle, R. and Oorschot, P.C.v. (2007a) 'A second look at the usability of click-based graphical password'. *Symposium On Usable Privacy and Security 2007*. Pittsburgh, USA: July 18-20, 2007.

Chiasson, S., Oorschot, P.C.v. and Biddle, R. (2007b) 'Graphical password authentication using Cued Click-points', Biskup, J. and Lopez, J. (Eds.). *ESORICS 2007, 12th European Symposium On Research In Computer Security*. Dresden, Germany September 24-26, 2007. Springer, pp. 359-374.

Chiasson, S., Forget, A., Biddle, R. and Oorschot, P.C.v. (2008a) 'Influencing users towards better passwords: Persuasive cued click-point'. *HCI 2008*, September 1-5, Liverpool, UK.

Chiasson, S., Forget, A., Stobert, E., Oorschot, P.C.v. and Biddle, R. (2008b) 'Multiple password inteference in text and click-based graphical passwords'. [Technical Report TR-08-20] School of Computer Science, Carleton University.

Charruau, D., Furnell, S. & Dowland, P. (2005) 'PassImages: an alternatives method of user authentication', *ISOneWorld 2005*. Las Vegas, USA March 30 - April 1, 2005.

Davis, D., Monrose, F. and Reiter, M.K. (2004) 'On user choice in graphical password schemes'. *Proceedings of the 13th USENIX security symposium*. California, USA: August 9-13, 2004 USENIX Association, pp. 1-11.

Djamila, R. and Perrig, A. (2000) 'Deja Vu: A user study using images for authentication', *Proceedings of the 9th USENIX Security Symposium*. Denver, Colorado, USA August 14-17, 2000. USENIX Association, pp. 45-58.

De Angeli, A., Coventry, L., Johnson, G. and Coutts, M. (2003) 'Usability and user authentication: Pictorial passwords vs. pin'. in McCabe, P.T. (ed.) *Contemporary Ergonomics 2003*. Taylor & Francis, pp. 253–258.

De Angeli, A., Coventry, L., Johnson, G. and Renaud, K. (2005) 'Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems'. *International Journal of Human Computer Studies*, 63 pp. 128-152.

Dunphy, P., Nicholson, J. and Olivier, P. (2008) 'Securing Passfaces for description', *Proceedings of the 4th symposium on Usable privacy and security (SOUPS 2008)*. Pittsburgh, Pennsylvania, USA July 23-25, 2008. ACM, pp. 24-35.

FreeFoto (2008) 'Free Pictures'. [Online]. Available at: http://www.freefoto.com/index.jsp (Accessed: 10 March 2008).

Golofit, K. (2007) 'Click passwords under investigation'. in Biskup, J. and Lopez, J. (eds.) *Computer Security - ESORICS 2007*. Springer Berlin/Heidelberg, pp 343-358.

Hinds, C. and Ekwueme, C. (2007) 'Increasing security and usability of computer systems with graphical password', *ACM Southeast Regional Conference*. Winston-Salem, North Carolina, USA ACM New York, USA, pp 529-530.

King, M. M. (1991) 'Rebus Passwords', *Computer Security Applications Conference*. San Antonio, TX, USA IEEE, pp 239-243.

Moncur, W. and Leplatre, G. (2007) 'Pictures at the ATM: Exploring the usability of multiple graphical password', *CHI '07: Proceedings of the SIGCHI conference on Human factors in computing systems*. San Jose, USA April 28- May 3, 2007. ACM, pp. 887-894.

Nickerson, R.S. (1968) 'A note on long-term recognition memory for pictorial material'. *Psychonomic Science*, 11 (2) pp. 58.

Passfaces (2003) 'Next generation graphical authentication'. [Online]. Available at: http://www.realuser.com/personal/index.htm (Accessed: 15 March 2008).

Renaud, K. (2009) 'On user involvement in production of images used in visual authentication'. *Journal of Visual Languages and Computing*, 20 (1) pp. 1-15.

Shepard, R.N. (1967) 'Recogition memory for words, sentences and pictures'. *Journal of Verbal Learning and Verbal Behavior*, 6 pp. 156-163.

Standing, L., Conezio, J. and Baher, R. N. (1970) 'Perception and memory for pictures: Single-trial learning of 2500 visual stimuli'. *Psychonomic Science*, 19 (2) pp. 73-74.

Thorpe, J. and Oorschot, P.C.v. (2007) 'Human-seeded attacks and exploiting hot-spot in graphical passwords', *16th USENIX Security Symposium*. Boston, USA. USENIX, pp. 102-118.

Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A. and Memon, N. (2005a) 'PassPoints: design and longitudinal evaluation of a graphical password system'. *International Journal of Human Computer Studies*, 63 pp. 102-127.

Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A. and Memon, N. (2005b) 'Authentication using graphical passwords: effects on tolerance and image choice'. *Symposium On Privacy and Security*. Pittsburgh, USA: July 6-8, 2005.

Yan, J., Blackwell, A., Anderson, R. and Grant, A. (2005) 'The memorability and security of passwords'. in Cranor, L.F. and Garfinkel, S. (eds.) *Security and Usability: Designing secure systems that people can use.* O'Reilly, pp. 129-142.