A Survey of User Opinions and Preference Towards Graphical Authentication

M.Z.Jali, S.M.Furnell, P.S.Dowland and F.Reid

Centre for Information Security and Network Research, University of Plymouth, UK
e-mail: mohd.jali@plymouth.ac.uk

Abstract

User authentication is a process of proving a user's identity to the services or systems that they wish to use. The traditional way of using authentication is the combination of username and password. This paper presents a study carried out to investigate users' opinions and preferences towards the use of images/pictures as an alternative method of authentication. A survey was carried out within a university environment and participants were asked to use a standalone graphical authentication prototype and provide feedback. Overall, preliminary results of the study showed that although participants initially had problem using the prototype, they enjoyed using it after a few attempts. This indication and other positive results suggested that user authentication using pictures/images could be used as one of the alternatives for balancing the weaknesses in traditional username/passwords.

Keywords

Graphical password, Authentication, Usability

1. Introduction

User authentication is the first layer of interaction between human and machines. Generally, the purposes of user authentication are to confirm or validate the person and as the next steps from him/her to use the services offered. Today, the use of passwords, or other secret or knowledge-based methods (e.g. what is your mother's maiden name, what is the name of your pet) are still the most widely used. Despite of this widespread use, traditional user authentication has many issues and problems. Adams and Sasse (2005) summarised that people normally had problems remembering long and complex passwords, that passwords chosen were vulnerable to various types of attacks and problems with the usability of passwords themselves.

As a result of these problems, among the solutions that have been developed so far are using Single-Sign-On, Multi-factor authentication and the use of biometric-based approaches such as retina, hand, iris, voice, thumbprint and the patterns of mouse and keyboard movements (O'Gorman, 2003), with each of these solutions having their own strengths and weaknesses.

The objective of this paper is to report an initial study evaluating users' opinions and preferences on the use of images/pictures as an alternatives means for user authentication. The paper begins with an explanation of the background areas of the

study and is followed by an explanation of how the study was approached together with the results and findings. The paper ends by highlighting the conclusions and future work that the authors are planning to conduct.

2. Background

This section briefly discusses the issues of authentication and graphical password.

2.1. Authentication

Authentication can be defined as a process of proving who you are or claim to be. There are two main types of authentication; user authentication and machine authentication. User authentication deals with the interaction of a human (as the user) with the computer while machine authentication deals with the interaction between computers. This paper only discusses user-based authentication.

Users often confuse the concept of authentication with other services or processes such as access control, auditing and administration. Generally, auditing is a process of recording all of the activities conducted by users (as either legitimate or not), access control is to limit or restrict the actions and operations the legitimate users should perform; and administration is the process of managing the system services (Sandhu, 1997).

There are many approaches for user authentication. O'Gorman (2003) categorised user authentication into three; something you have or object-based (e.g. tokens), something you know or knowledge-based (e.g. password or other secret) and something you are in terms of psychology and/or behaviour (e.g. biometrics).

Even though many authentication methods have emerged, no single method is applicable for all applications. For instance, the use of biometrics is not practical when used with the current ATM machines and the use of long and complex passwords could pose difficulties to certain members of the community (e.g. the elderly or people with learning difficulties). That is why research into user authentication is still important and has gained much interest from the psychology and security domains.

2.2. Graphical Authentication

The idea of using graphics to aid with remembering passwords is not new, however the idea of using graphics as a replacement for passwords has emerged with the work patented by Blonder (1996), to offer better usability and security as opposed to the traditional username/password approach, claiming that using pictures/images could offer a larger password space and thus offer greater security. It was also suggested that the problem of remembering long and complex passwords could be addressed by recognising images/pictures, as humans are very good at recognising and recalling images as opposed to words, sentences or phrases (Shepard, 1967).

In this paper, graphical authentication methods are grouped into three categories, based on the type of user interaction required: Choice-based, Click-based and Draw-based. The idea of each type is as follows:

Choice-based requires users to select their chosen images from a set of decoy images. The image selection can be continued for several rounds depending on the system settings.

Click-based requires users to click anywhere they prefer in the image. These clicks are actually their password. There are two further variations in this type; users click all locations in one image or users click once for each image.

Draw-based requires users to draw their secret/password on the provided grid/screen. In this case, the drawing is interpreted as the password in order to be authenticated.

The Choice-based type taking place with the product known as Passfaces (Passfaces, 2003) in which, users needed to choose the image of faces in order to be authenticated. Later, Dejavu was introduced by Djamija and Perrig (2000). This used abstract images deployed from the Andrej Bauer's Random Art algorithm, an algorithm where bit of strings converted into the form of interesting abstract images. Overall, the Choice-based type is the most well-known because of its ease and simplicity while still maintaining the level of security. Other work within this group include ToonPasswords (Hinds and Ekwueme, 2007), VIP (De Angeli *et al.* 2003) and PassImages (Charruau *et al.* 2005).

The Click-based type was first developed and patented by Blonder (1996). In this scheme, users clicked on the predetermined areas of the image. As the password of this approach is easy to guess, Wiedenbeck *et al.* (2005) introduced an enhanced scheme known as Passpoints. In this approach, users are required to click on anywhere they prefer on the image. From all the usability studies carried out by the authors, they concluded that participants satisfied with the approach and it could be one of the alternatives for future user authentication. Recently, Chiasson *et al.* (2007) introduced the Cued Click Point (CCP) in which users are required to click once per image on a sequence of images. The next image is based on the previous click-point. The authors claimed that the approach could reduce the burden of memorising a sequence of click points as in Passpoints while at the same time enhancing the usability and security.

The first Draw-based scheme was Draw-A-Secret (DAS), developed by Jermyn *et al.* (1999). Another scheme in this group is Pass-Go (Tao, 2006). Recently, Yan and Dunply (2007) introduced the Background-DAS, claiming that this could eliminate the problem of accuracy of user drawings and also offered larger password space and enhanced usability. Most of the schemes within this type were developed to be used in restricted environments such as phones and handheld devices.

In addition to the above schemes, graphical authentication is also being introduced to tackle the problem of shoulder-surfing and spyware (Li *et al.* 2005; Malek *et al.* 2006; Man *et al.* 2003). Overall, it was found that only a small number of approaches

were actually tested for their usability, the others simply explain their idea and describe how their schemes would be able to prevent shoulder-surfing and spyware.

3. Methodology

The objectives of this study were to investigate users' opinions and preferences towards three types of graphical authentication, as explained in the earlier section. The study made an assumption that users would choose Click-based and Choice-based methods as their preferences for web authentication. This is based on the point of view where both are easy to use, memorable, offer an appropriate level of security and more importantly, can be used directly on the web without needing any additional hardware/software.

A survey was conducted in order to investigate the objectives. In this survey, participants were asked to use the prototype and then answer a related questionnaire. This activity took approximately 10 to 15 minutes to complete depending on the participants' experiences using computers. The following sections explain the prototype, questionnaire and outline the steps and procedures the participants had to follow.

3.1. Prototype

The prototype of three graphical authentication techniques was developed using Microsoft Visual Studio. All three schemes were developed and bundled in one application. The developed prototype was analogous in context with the Passpoints, Passfaces and DAS approaches. The purpose of this prototype was to give participants a brief hands-on experience and to demonstrate how graphical authentications could work in the real world.

Initially, the main intention of this study was to get participants opinions on web authentication using a graphical approach; however after considering many factors like accessibility, mobility and time, it was decided not to develop the prototype in a web environment but simply to have a small standalone application. The designs of three schemes were basically similar to the original Passfaces, Passpoint and DAS but simplified in terms of the number of passwords they need to register or use. This is due to the fact that the study only needed the participants to get an impression of using graphical approaches and did not want to burden them by remembering up to five click points and five to six images.

There were two main modules in the prototype; Register and Login. In the register module, participants needed to register their passwords by clicking four times on the image for the click-based type, choosing two images for the Choice-based type and drawing freely for the draw-based type. Here, the drawing will take into account the location of mouse *click-down* and the location of mouse *click-up*. The types, shapes and number of drawings were left to the participants' preferences. Example screenshots for the prototype are shown in Figures 1, 2 and 3.

Figure 1: Screen shot of the click-based type

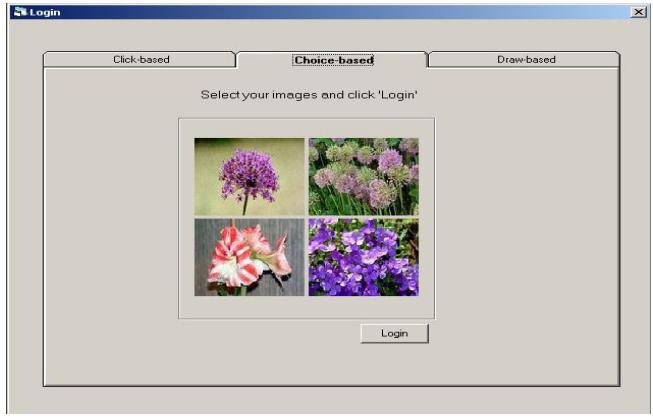

Figure 2: Screen shot of the choice-based type

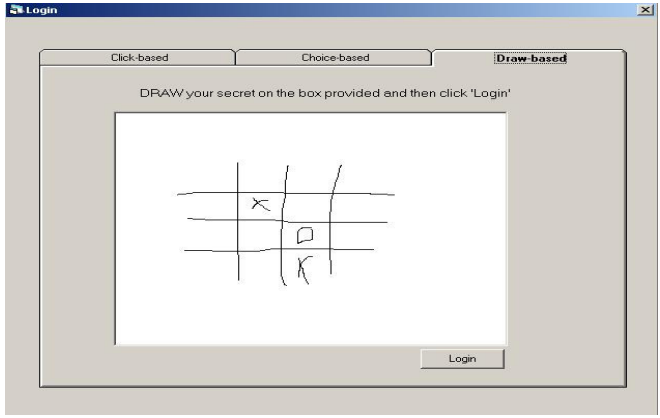

Figure 3: Screen shot of the draw-based type with an example of a secret drawn by one of the participants

3.2. Questionnaire

There were two sections in the questionnaire. Part A asked the participants to give their demographic information such as their age, gender, nationality, highest level of education, current job, years of using computers and asked their awareness and knowledge regarding the use of images/pictures as a means of alternative user authentication.

In part B, participants were asked to answer four questions after they finished using the prototype. The first question was about their opinion on the ease of use of each method, how easily they remembered their secret, how easily they could reproduce their password and whether they felt that the methods could be used in a web-based environment. The second question asked participants to select the method they would most strongly prefer to use for web-based authentication. For the third question, participants were asked their opinion about whether they would consider each method to be 'Safe' or 'Unsafe' against the following security threats: observer or shoulder-surfer, guessing by close family or friends and brute-force attack. The final question asked participants to give any comments and suggestions regarding image authentication.

In order to validate users' understanding and to reduce errors during the subsequent implementation, five participants took part in pilot testing where the prototype was evaluated. Appropriate changes and amendments were then made prior to the full run of the study.

3.3. Procedures and Steps

Participants were asked to use the prototype displayed on a 14-inch laptop screen with a wireless mouse as their input device. They were first to register their password and later, reproduce it or login by using the same password/secret they had chosen earlier. During the registration and login, appropriate messages were displayed in order to alert and give them information. After using the prototype, they were asked to answer the provided questionnaire. Upon using the prototype, all of the participants' actions and behaviour were observed for monitoring purposes. As this was an 'uncontrolled' type of survey, participants were allowed to use the prototype as many times as they wanted.

4. Results and Findings

A total of 25 volunteers took part in this initial study (12 males and 13 females). The minimum age of the participants was 30 years old. The majority of the participants were university staff (e.g. students, researchers, administrators and lecturers) and all of them had more than 6 years experience using computers.

When asked about their familiarity with the use of images/pictures for authentication purposes, only 11 participants indicated that they were aware of it. Accordingly, from the observation, it was found that participants were initially quite 'confused' with the 'state-of-the-art' of graphical authentication. For example in the Click-based

type, the majority of them had problems reproducing their passwords. This is possibly due to their misunderstanding of this approach because when they clicked on particular points (for example clicking on the person's hand); they were assuming the whole image (in this case, the whole body of the person) was chosen. Only the point or the area in which they clicked would be taken into account as their password and not the whole object**.** Overall, only 12 participants managed to complete all the tasks successfully. This demonstrates that for the graphical password to be effective, appropriate training should be provided beforehand.

Users' preferences on the suitability of graphical scheme towards web authentication showed that participants preferred click-based (13 participants) and choice-based (12 participants) with no participants indicating a preference for the draw-based method. From the informal interview, the main reason why such schemes were preferable was because of their convenience and simplicity. However, the majority of the participants pointed 'unsure' or 'doubt' for the level of security of the choice-based method.

When using the prototype, it was found that all of the participants preferred using the choice-based method. They felt that the passwords were quite easy to remember and they had no problem reproducing their passwords during login. However, although the draw-based type was easy to use, participants had difficulty remembering and reproducing their drawings. It is likely that this was due to the usage of the mouse and if participants were to use some sort of special device such as a stylus or a drawing pad, they would perform better. The results of ease of use, ease of recollection, ease of reproduction and suitability to be used in web environments were shown in Figure 4.

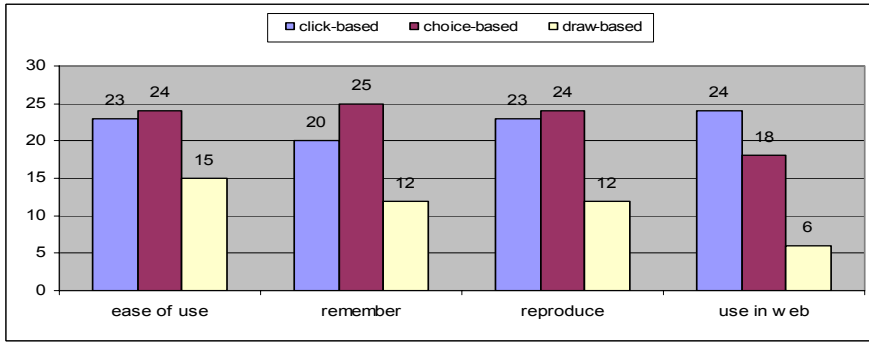

Figure 4: Users' opinion towards ease of use, remembrance, reproduction and use in web

The users' opinion towards the level of security the methods might offer, the majority of the participants believed that the draw-based method offered better security. This is due to the fact that it is impossible for users to draw alike. Conversely, more than half of the participants felt that choice-based would be vulnerable to guessing, brute-force and information harvesting vulnerabilities and interestingly although they felt that the choice-based type was not secure enough;

they still choose it as their preferred method for web authentication. The detailed results on users' opinions towards security issues are presented in Figure 5.

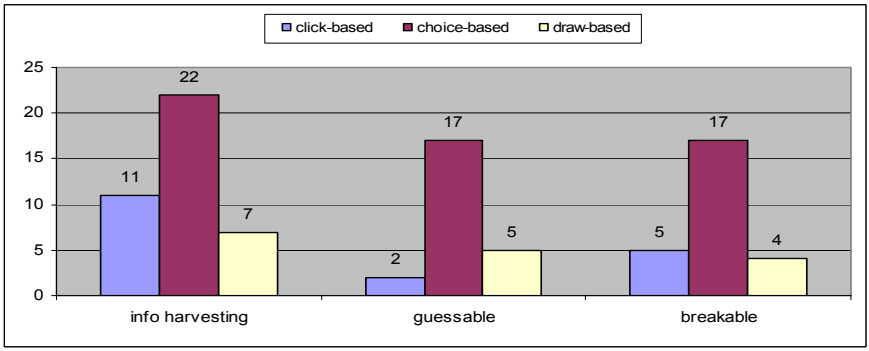

Figure 5: Users' opinion towards security issues like information harvesting, 'guessability' and 'breakability'

Here, the term 'information harvesting' refers to the vulnerability or actions done by the observer or shoulder-surfer. 'Guessable' refers to the vulnerability or guessing actions perform by closed family or friends, while the term 'breakable' deals with the vulnerability to some sort of educated guess, dictionary attack and/or computer algorithms. Although users may not have been able to offer truly informed opinions about these aspects, their views were still a valid reflection of what they perceived the security to be (which would therefore influence their confidence in using the approaches

In summary, the assumption that participants would prefer choice-based and click-based types for web authentication was confirmed in this study. The contribution of this study when compared to earlier works is that it asked users to consider and compare all three types of graphical schemes (whereas others typically compared a single form of graphical authentication against traditional username/password methods).

5. Conclusion and the future

This paper presented an initial study on user opinions and preferences towards authentication using images/pictures. From the results and findings from 25 participants, it has shown that the level of familiarity and awareness towards graphical authentications were balanced; participants preferred the click-based and choice-based methods for web usage and they provided mixed opinions towards the issues of security and usability. Overall, the study concludes and suggests that using images and pictures could by some means be one of the alternatives for user authentication, especially in the web-environment.

However with the current state of graphical authentication, the authors feel that it is still too immature to be implemented on a large-scale and thus more work needs to be done in the areas of security and usability. The authors plan to extend this study with additional participants in order to obtain more conclusive and representative

findings. In addition, a fully working prototype of graphical web authentication will be developed, enabling a series of experiments (both in-lab and field trial) to be carried out in order to more comprehensively assess user experiences in practice.

6. References

Adams, A. and Sasse, M.A. (2005), "Users are not the enemy", in Cranor, L.F. and Garfinkel, S. (eds.) *Security and Usability: Designing secure systems that people can use,* O'Reilly Media Inc, CA, pp619-630, ISBN: 0-596-00827-9.

Blonder, G. (1996), *Graphical password,* 5.559.961, available at: http://www.patentstorm.us/patents/5559961.html, (accessed: 10 March 2008).

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

Chiasson, S., Oorschot, P.C.V. and Biddle, R. (2007), "Graphical password authentication using Cued Click-points", In Biskup, J. and Lopez, J. (eds.) *ESORICS 2007, 12th European Symposium On Research In Computer Security*. Dresden, Germany September 24-26. Springer, pp359-374.

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, pp253–258.

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, pp45-58.

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, pp529-530.

Jermyn, I., Mayer, A., Monrose, F., Reiter, M.K. and Rubin, A.D. (1999), "The design and analysis of graphical password", *Proceedings of the 8th USENIX Security Symposium*. Washington DC, USA, August 23-26, pp1-14.

Li, Z., Sun, Q., Lian, Y. and Giusto, D.D. (2005), "An association-based graphical password design resistant to shoulder-surfing attack", *IEEE International Conference on Multimedia and Expo 2005*. July 6-8, pp245-248.

Malek, B., Orozco, M. and Saddik, A.E. (2006), "Novel shoulder-surfing resistant haptic-based graphical password", *Proceedings of Eurohaptics 2006*, Paris, France, July 3-6.

Man, S., Hong, D. and Matthews, M. (2003), "A shoulder-surfing resistant graphical password scheme - WIW", *Proceedings of the International Conference on Security and Management 2003*. Las Vegas, USA, pp105-111.

O'Gorman, L. (2003), "Comparing passwords, tokens, and biometrics for user authentication", *Proceedings of the IEEE*, 91 (12), pp2019 - 2040.

Passfaces (2003), "Next generation graphical authentication", available at: http://www.realuser.com/personal/index.htm (accessed: 15 March 2008).

Sandhu, R.S. and Samarati, P. (1997), "Authentication, access control, and intrusion detection", in Tucker, A.B. (ed.) *The Computer Science and Engineering Handbook,* CRC Press, pp1929-1948.

Shepard, R.N. (1967), "Recogition memory for words, sentences and pictures", *Journal of Verbal Learning and Verbal Behavior*, 6(0), pp156-163.

Tao, H. (2006), *Pass-Go: A new graphical password scheme*. MSc. University of Ottawa, Canada, available at: http://www.site.uottawa.ca/~cadams/papers/HaiTaoThesis.pdf (accessed: 8 May 2008).

Wiedenbeck, S., Waters, J., Birget, J.-C., Brodskiy, A. and Memon, N. (2005), "PassPoints: design and longitudinal evaluation of a graphical password system", *International Journal of Human Computer Studies*, 63(0), pp102-127.

Yan, J. and Dunply, P. (2007), "*Background Draw A Secret*", available at: http://homepages.cs.ncl.ac.uk/jeff.yan/bdas.htm, (accessed: 10 March 2008).