PassImages : An alternative method of user authentication

D. Charruau, S.M. Furnell & P.S. Dowland
Network Research Group, University of Plymouth, Plymouth, UK
info@network-research-group.org

Abstract

This paper presents an assessment of an alternative to the predominant password and PIN-based methods of user authentication. Although these approaches are in widespread use, there are many recognised problems in terms of their usage and the consequent protection that they actually provide. Therefore a graphical method using PassImages has been created in which users are authenticated from the selection of six images, chosen from a set of one hundred. A trial of the technique has been conducted via a prototype implementation of a web-based authentication process. This assessment shows that the PassImage approach provides a high level of effectiveness, with 29 trial users achieving 95% successful authentication.

Keywords: *Security, Authentication, Passwords, Graphical Passwords*

Introduction

In modern society it is not unusual to have to authenticate ourselves on several IT systems. Most of the time, these systems require a password or a PIN, but faced with the requirement to remember such information, many users encounter difficulties, which tends to result in poor choices or other bad practices. For example, passwords are often based upon dictionary words or personal information, resulting in vulnerability to attack by brute force cracking tools or social engineering (VeriSign, 2000). By contrast, enforcing better selection practices may simply lead to compromise in other ways, such as passwords being written down and left nearby the computer (often in plain sight) for the legitimate user's reference. All the while, of course, they are equally visible to potential impostors. In view of such problems, alternative methods are desirable, and common recommendations include the use of token-based or biometric approaches (Smith, 2002). However, one of the inherently attractive characteristics of a password is its low cost, and the aforementioned alternatives will typically incur additional expense. In addition, if a web-based service operator wished to authenticate users on the basis of such techniques, there would be no guarantee that the users possessed appropriate hardware. As such, the use of alternative secret-knowledge approaches may remain preferable in many contexts. Therefore, an experiment has been conducted in an attempt to evaluate an alternative method based upon selection of images rather than the recall of text sequences. This method is based on the conclusions of two previous studies conducted by Irakleous *et al.* (2001) and Furnell *et al.* (2004).

The paper begins by presenting an outline of the problems with existing password-based approaches, as well as previous attempts to utilise image-based methods as an alternative. It then proceeds to discuss the design and implementation of an alternative approach, and the results observed from a practical user trial. The implications of these results are then discussed, along with opinion-based feedback from the trial participants, leading to the suggestion of future research directions in the concluding section of the paper.

Background

The vast majority of user authentication methods in operating systems, applications and websites involve the use of passwords. Indeed, passwords remain the method of choice in spite of recognised vulnerabilities, many of which arise from the behaviour of users. Passwords have been the way to authenticate on IT systems since the first computers were created in the early 1960's (Morris and Thompson, 1979). In the last two decades, other aspects of computer interfaces have changed significantly (e.g. the arrival of Graphical User Interface (GUI) environments), but people are reluctant to change their security systems for something new (Bensinger, 1998). As a result, an authentication method inherited from the command line age is still in use. Studies have shown that the end users' behaviour introduced the majority of the password weaknesses, by sharing their password or by choosing passwords that are easy to remember. For an intruder these passwords became easy to guess (Boroditsky, 1998). For example, a previous study has shown that on a sample of 15,000 passwords 21% of them have been cracked in less than a week and 2.7% in less than 15 minutes (Klein 1990). This suggests that allowing end users to choose their passwords effectively introduces weaknesses in the security system. In order to increase the security, administrators tend to provide passwords to the users, but then other problems arise: because the password is no longer simple to remember, people start to write it down, and the effect is even worse (Boroditsky, 1998). By the early 1990's an Internet Engineering Task Force (IETF) request for comments (RFC) was already taking the matter as a serious security threat, and proposing the minimum requirements that a password must comply with – namely being at least 6 characters long, and composed of characters drawn from mixed case alphabetic, punctuation symbols and digits (Holbrook and Reynolds,1991).

In many ways GUI-based authentication methods using images are considered better than passwords. The reason is that images are easier to remember than a string of letters. This is due to the fact that the human brain has difficulty remembering information when it is not part of a context. On the other hand, an image can easily provide a context by itself (Bensinger, 1998). According to psychology researchers, the human brain is good at recognising images. Two studies are used as references to explore this ability. In the first test, 2,560 photos were presented to an audience, with each image shown for a few seconds. The users then had to examine a set of images composed of new and already seen images. During the test, participants had to indicate the images seen before. The result of this experiment was a 90% recognition rate (Standing *et al.*, 1970). Another study was carried out and followed a similar principle. The audience saw 10,000 pictures in two days and performed a recognition rate of 60% (Standing, 1973).

In addition to this ability to easily recognize images, a study has shown that image pin based methods were easy to use: in a study involving 27 participants, 63% were successfully able to authenticate. In parallel to this experiment, password authentication was studied and gave approximately the same rate of success (Irakleous *et al.*, 2002a). Other methods have also been developed such as the "Déjà Vu" authentication method created by Dhamija and Perrig (2000). This method is based on the memory of images, but does not require a precise sequence. Two types of images have been used to evaluate this method, namely photos and random art images. The photos are complex sceneries and the random art images are images drawn by a computer using random parameters inserted into a mathematical formula. The probability to be able to masquerade as another person with this method is unlikely to occur since a sequence of 5 images on a matrix composed of 25 images is required to authenticate. However, as described below, this still yields notably fewer combinations than a (correctly used) six character password.

The aim of the research at this stage was to devise a potential replacement for password-based authentication, while retaining a secret-knowledge based approach and providing a comparable level of protection to a password selected on the basis of the recommendations in RFC 1244 (Holbrook and Reynolds, 1991). A new method (hereafter referred to as the PassImage method) was devised that attempted to provide a user-friendly authentication approach based upon the selection of on-screen images.

Methodology

The guidelines of the aforementioned RFC 1244 indicate a total of 95^6 possible password combinations. Therefore it has been decided to create a method that allows the user to choose six images from a total of 100 images. In order to prevent "shoulder surfing" the images are displayed randomly on four different grids each time the process is launched. The images themselves all depict objects from everyday life, as illustrated in Figure 1. It is therefore hoped that users will be able to recognise the objects, and select six that they are most comfortable with.

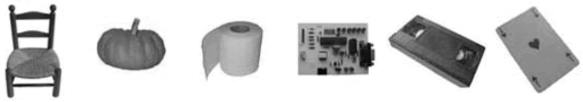

Figure 1: PassImage example

In order to create a method that can be used by the largest number of potential users it was decided to design a web-based authentication procedure. The use of a web interface had many advantages compared to other means of assessment, since there was no need to distribute software to potential participants, and most operating systems can support the method as it was written in JavaScript.

The authentication process was made as simple and secure as possible. Therefore in order to select an image, the user is only required to do a simple click on the image that they want to choose. For security purposes, images chosen are not displayed since it would be easy for prying eyes to catch the selection. Therefore a system of 'traffic lights' was implemented. Each selection from the user switches on an amber light (see figure 2). Once all selections have been made, and if the user achieves authentication, all the traffic lights become green (see figure 3), on the other hand if the user fails, the traffic lights become red. Users can change the grid and cancel the last selection either with the button provided or with keyboard keys. Shortcut keys are useful to accelerate the choice of the images by reducing the need for moving the mouse pointer from the grid to the buttons and back to the grid.

In order to simplify the authentication procedure it was decided that the system will assist the legitimate user in recalling the correct sequence of images. To achieve this, the six pictures that comprise the PassImage are always displayed back in the right order on the login grids. For example if a user chose the PassImage shown in Figure 1, then in all subsequent authentication sessions these would appear in the grids in this order (i.e. the image of the chair will always be the first one that the user will encounter when looking through the choices available). This enables the user to scan each grid from left to right, top to bottom, with no requirement to hunt back and forth between the grids (i.e. unless the user inadvertently misses one of their images, they should only need to advance forward to the next grid, rather than back to a previous one).

The concept is illustrated in figures 2 and 3, which depict the PassImage login in operation. The required selections are indicated by the shaded images, along with a number indicating the sequence in which each image has to be chosen (note: the shading and numbering do not appear in the live operation of the system, and have been added to the screenshots to help clarify the process involved). It should be noted that although the example depicts the user's images being spread over two different grids, this will not always be the case. Apart from ensuring that the images appear in order, their placement is done randomly; so on different occasions they may be spread over up to four different grids.

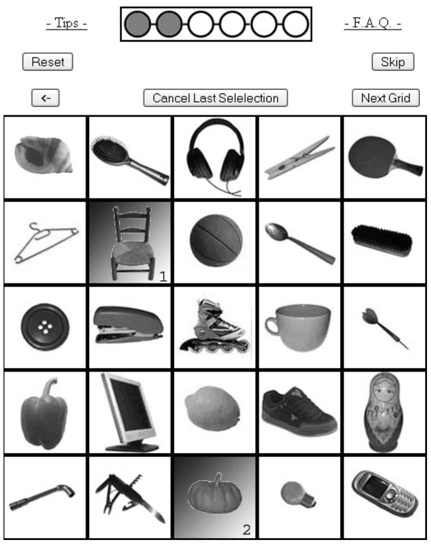

Figure 2: Authentication Process

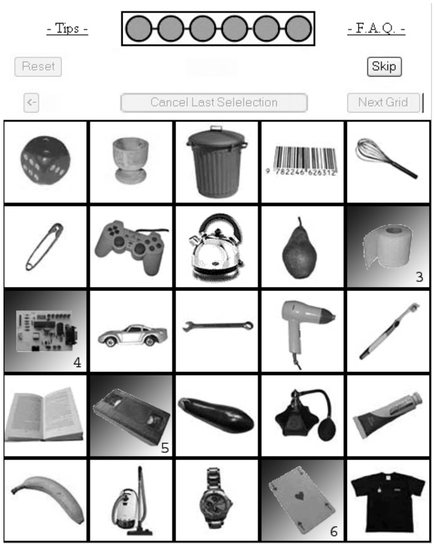

Figure 3: Authentication achieved

In addition to measuring the success or failure of authentication attempts, the system used for the trial was also able to log the time that users took to choose the images composing the PassImage, the number of access attempts they made during the trial period, and the time taken for each authentication attempt. At the end of the trial period, a small survey of the participants was conducted via an online questionnaire, in order to collect user opinions regarding the PassImage method.

4. Experimental results

Twenty-nine users were involved in assessing the method, during a total period of 90 days. During this time, the PassImage website was set as the new homepage for each participant's web browser. As such, each time they loaded the browser, they were prompted to provide their user identity and then authenticate themselves via PassImage. Successful authentication then initiated automatic redirection to their original browser homepage. In order to foster goodwill amongst the trialists, they were not obliged to use the method each and every time they loaded the browser, and a 'skip' button was offered as a quick route to their normal homepage. For participants who had forgotten their PassImage, the system offered an option for it to be recovered.

None of the trialists used the authentication method for the full 90 days of the study period. The average period of usage was 38 days, with users having performed an average of 31 trials. The numbers of trials varied considerably from one user to another. For example, the maximum of trials was 213, while the minimum was six.

The result shows that the users achieved a high rate of authentication. From a total 911 trials, the users were able to authenticate on 867 occasions. This gives an authentication rate of 95%, and a rejection rate of only 5%. However, in addition to this result it should be noted that users had to retrieve their PassImage on only three occasions. Therefore if only the retrievals are taken into account to calculate the number of authentication failures, the authentication success becomes 99.6%. Another interesting point is that there was only one occasion during the trial in which a user made three errors in a row. This suggests that a standard security policy of blocking the account after three consecutive rejections is likely to have low impact upon the activities of legitimate users.

A measurement, which is very important for such techniques, is the time spent by the users to set up an account and then to authenticate during subsequent logins. The selection of the PassImage was a relatively long process, and on average, users spent two minutes to perform this task. This is, however, justifiable in the sense that users should consider their choices carefully in order to ensure that they remember them later. Figure 4 illustrates that as users made more use of the system, the time taken to authenticate steadily decreased. The results of the measurements made on the time spent to authenticate, show that after a short usage period, users are, on average, able to authenticate in around twenty seconds. This is still somewhat longer than the typical time taken for password-based authentication, but this could arguably be set against the potential security benefits of the new approach.

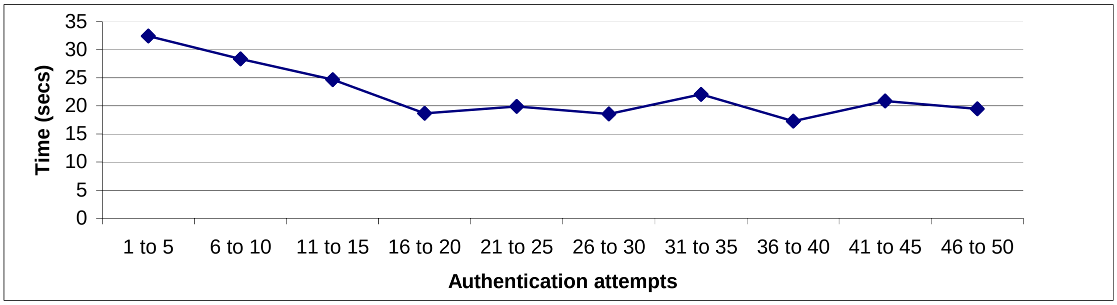

Figure 4: Average time taken to authenticate

Since security was one of the main objectives of the experimentation, the choice of PassImage has been scrutinised in order to find weaknesses implied from a poor set of image selections. Although the selection process did impose some restrictions upon the users' choices (e.g. they were not permitted to choose multiple instances of the same image), there were other ways in which potentially weak choices could be made. For example, users could conceivably choose all six of their images from the same category of pictured object (e.g. food and drink, clothing and footwear, etc.). Therefore all the images were categorised and all the PassImages were parsed to see if they met such criteria. This revealed that, out of 37 PassImages chosen by users during the trial, 5 were classed as weak choices because the constituent images all belonged to the same category. Also related to the issue of image choices is that the post-trial comments from one participant suggested that two of his relatives had nearly found his PassImage. This suggests that the method may face some potential for attack through social engineering.

Discussion

In addition to the analysis performed, the users were asked to provide their opinions about the method. All users felt that the implementation using a web-based interface was appropriate, 89% of the users felt that the method operated quickly, and 8% of the users found that the images were hard to recognise. Despite the high rate of successful authentication, almost a quarter (23%) considered it hard to use (against 27% who found it 'very easy' and 39% who classed it 'easy'). From the users' perspective, the perceived ease of use of the method was closely tied to their ability to remember the necessary images - 27% thought that remembering the six images was very easy, 39% thought it was easy and 23% thought it was hard. The theoretical chance for an impostor to guess the correct PassImage is one in 858,277,728,000 (based upon six images chosen from 100, without duplicates). To determine how the security was perceived by users, they were asked to rate the chances of a person remembering their PassImage witnessed during the authentication process, 42% thought that it would be very hard, 35% that it would be hard and only 4% of the users thought that it would be easy. A question on how many images users would have chosen was also asked; it showed that 54% of the users would choose six images. This result is not surprising since the experiment was based on the same choice. However 34% of the users preferred to choose fewer images and only 11% of the users would choose more than six images. Even though the analysis of the authentication time showed that users, on average, were able to authenticate in around twenty seconds, 39% of the users thought that the method was too time consuming.

The last question asked if the users thought that this alternative method could replace the present means of authentication, 73% believed that it could, while 27% considered that it would not be feasible. The main reason expressed in the latter case was the time taken for authentication when compared with typing a password. A secondary factor was the difficultly in remembering the images.

When comparing the results to earlier studies, some further positive observations can be made. In the study conducted by Irakleous, a similar technique only achieved 63% success. The present method has also achieved a better effectiveness than the study carried out by Furnell *et al.* (2004), which had an effectiveness of 84% from 378 attempts. The measurements resulting from this analysis can also be compared with results from the "déjà vu" research performed by Dhamija and Perrig (2000). In the "déjà vu" research, users only spent a minute to choose their images whereas in this method results show that the choice of the PassImage is quite a long process since users, on average, took more than two minutes to make their selections. The "déjà vu" research also showed that the users were able to authenticate in an average of twenty-seven seconds, whereas with the current experimentation users spent an average time of twenty seconds after a short usage period, and that the average time taken over the whole experiment was twenty three seconds. Furthermore it should be noted that the requirement for the authentication was not the same. In the "déjà vu" experiment, the users were asked to select five photos from amongst twenty other photos on the same screen. Therefore it can be concluded that the choice of displaying simple objects rather than complex images may simplify the user's choice.

Conclusion

The practical study revealed a good approval rate of the PassImage method, and a high level of effectiveness (albeit amongst a relatively small user population). However, some issues need to be addressed. Even though users considered the web-based interface to be appropriate, some imperfections have to be addressed, such as more attention to the production of a better set of images. It is believed that if better images can be produced, the difficulties remembering them may decrease, as well as avoiding obvious categorisation issues. In order to prevent social engineering, a possible way would be to create a larger image database and to filter the images that the user can choose in accordance with a questionnaire about his/her work and hobbies.

In terms of the implementation, a better way to assess such a method would be to integrate it into a system in which users traditionally expect to login, rather than as a voluntary additional layer within an application that normally proceeds without authenticating the user. Another necessary evaluation would be to perform the assessment with trialists using several accounts. Therefore the effect of having to remember multiple PassImages could be studied, revealing whether it is possible to use the PassImage as intensively as the PIN and passwords that are currently used across many different systems. Other techniques to reduce the time spent in order to authenticate have to be found since it will lead to a better acceptance of the method.

Once these issues have been addressed, the method would benefit from a larger scale trial (without the option for the users to skip the authentication process – which would help to yield a more accurate impression of their acceptance of the technique).

References

Bensinger, D. (1998) "Human Memory and the Graphical Password", p.2. www.PassLogix.com (accessed 10/12/03).

Boroditsky, M. (1998) "Passwords Security Weaknesses & User Limitations", p.2. www.PassLogix.com (accessed 10/12/03).

Dhamija, R. and Perrig, A. (2000) "Déjà Vu: A User Study Using Images for Authentication", In *Proceedings of the 9th USENIX Security Symposium*, August 2000.

Furnell, S.M., Papadopoulos, I. and Dowland, P. (2004) "A long-term trial of alternative user authentication technologies", *Information Management & Computer Security*, vol. 12, no. 2: pp178-190.

Holbrook, P and Reynolds, J. (1991) "RFC 1244 Site Security Policy Handbook Working Group", p.58, www.ietf.org (accessed 10/12/03).

Irakleous I., Furnell S.M., Dowland P.S. and Papadaki M., (2002) "An experimental comparison of secret-based user authentication technologies", *Information Management & Computer Security*, vol. 10, no. 3, pp100-108

Klein, D. (1990) "Foiling the Cracker: A Survey of, and Improvements to, Password Security", in *Proceedings of the Second USENIX Security Workshop*, Portland, Oregon, August 1990, pp5-14.

Morris, R. and Thompson, K. (1979) "Password Security: A Case History", *Communications of the ACM*, vol.22, no.11, pp594-597

Smith, R.E. (2002) *Authentication. From Passwords to Public Keys*. Addison Wesley.

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

Standing, L. (1973) "Learning 10,000 pictures", *Quarterly journal of Experimental Psychology*, 25:207-222, 1973.

VeriSign. (2000) *The Security Risks of Using Passwords*, VeriSign White Paper, available online: itpapers.news.com (accessed 1/10/2004).