Authentication based upon secret knowledge and its resilience to impostors

L.Zekri and S.M.Furnell

Network Research Group, University of Plymouth, Plymouth, United Kingdom
e-mail: info@network-research-group.org

Abstract

This paper presents an assessment made on an alternative to the present password and PIN-based methods of user authentication. In the recent years, many alternative authentication methods emerged, but none of them seems to have been a major breakthrough. Nevertheless, two techniques emerged as potentially efficient: image-based authentication and cognitive question and answer techniques. Even if the viability of these techniques has been proved, little research has assessed the resilience of the methods to impostors. Therefore, an environment has been created to test the robustness of the alternative techniques. The evaluation comprises both a theoretical and a pragmatic analysis to rate the robustness of the methods. The results show that the methods are vulnerable in different ways, with PassImages susceptible to phishing and shoulder surfing, whereas cognitive questions can be targeted via social engineering.

Keywords

Security, Authentication, Graphical Passwords, Cognitive Questions, Robustness.

1. Introduction

Passwords are the most commonly used method for identifying users in computer and communication systems. They were introduced first in the early 1960s as an authentication solution with the emergence of the first multi-users operating systems. Since that date, users relied more and more on passwords as computer and networks spread, and especially the Internet. According to a study (Danchev, 2005), almost 99% of the home users rely heavily on passwords as a basic form of authentication to sensitive and personal resources.

On average, we need to remember about 10 passwords, and this average increase up to 16 passwords for IT workers (Brostoff, 2004). Moreover, we can add to our list of passwords a list of PIN (Personal Identification Number) codes. This huge amount of passwords and PINs that we have to remember threatens our security. For security reasons, the best password would be a random one. However, it is widely recognised that, in order to remember all these passwords, we tend to use dictionary words or other words that have special meaning for us. We also tend to use the same password everywhere, allowing a hacker that discovered a password in one account to gain access to others.

Because humans live in an environment where their sense of sight is extremely active, we have acquired an amazing ability to treat and store large amounts of graphical information easily. These recent years, many studies tried to exploit this ability in the context of user authentication. Three of them, performed by Irakleous et al. (2002), Papadopoulos (2001), and Charruau (2004) were the building blocks of this research. The subject of these studies was to assess the viability and the efficiency of image-based authentication, and also some other secret-knowledge techniques. None of them assessed the robustness of the methods to impostors. In order to be adopted in a large scale, the potential alternative techniques should be first assessed from a security point of view. It is from this perspective that this study has been developed.

The paper begins by presenting the weaknesses of the existing password-based approaches, as well as an outline of the previous attempts to utilise image-based methods as an alternative. It then discusses the adopted methodology, the implementation of the tests conducted on the alternative techniques, and the results observed from the experimentation. The implications of these results are then discussed, leading to the suggestion of future research directions in the concluding section of the paper.

2. Background

Passwords were a viable way to implement an authentication process that could work with the rudimentary and simple command line interface. By using passwords, it was simple for system designers to provide an efficient authentication, and it was easy for users to adopt it.

However, it is the users themselves that often compromised the password-based protection. Simple passwords are easy to remember, but vulnerable to attacks, whereas complex passwords are more secure, but hard to remember. Many studies have been carried out during the past decades investigating the roots and the impact of the weaknesses of password-based methods on authentication. A study, conducted in the early 70's (with a population of 3829 users) presented quite interesting results: about 15% of the passwords had length no more than three characters and 85% of the passwords were dictionary words (Morris and Thompson, 1970). Another study (1990) conducted on a population of 15,000 persons showed that 21% of the passwords have been cracked in less than a week (Klein, 1990).

The problem with passwords is due to the fact that they rely on a precise recall of the secret information, which is not a strong point of human cognition. Thus, other secret-knowledge based authentication techniques have been developed recently, and they rely on recognition rather than a precise recall of memory. Image-based authentication consists on the recognition of previously seen images, a skill at which humans are amazingly talented. Many studies have shown that humans can remember and recognise thousands of pictures very rapidly. In an experiment, a sequence of about 2,600 pictures was presented to an audience which realised, in a second step, an interesting 90% recognition rate (Standing et al, 1970).

In addition, it seems that image-based authentication is viable and efficient. In fact, two earlier studies established the high authentication rate of these alternatives. The first one involved 27 persons and presented a 63% authentication rate (Irakleous et al. 2002). In the second one, from a total 911 trials, the users were able to authenticate 867 times. This gives an authentication rate of 95% (Charuau et al. 2004).

In addition to the graphical authentication techniques, researchers have developed other alternative methods. For instance, cognitive passwords are based on specific questions where the answers depend on user's opinions, interests and life history.

The purpose of this study is to assess the robustness and the resilience of some alternative techniques to impostors. The two chosen methods to be assessed are PassImages and Cognitive questions. In fact, three previous studies assessing the effectiveness of alternative methods have previously been performed by Irakleous et al. (2002), Papadopoulos (2002) and Charuau (2003). The first study established that a technique based upon associative questions (i.e. using word association as the basis for challenge-response pairs) suffer from a low authentication rate (4%) and thus it will not be considered for further research. In the opposite side, it established that successful authentication methods could potentially be cognitive questions techniques (59% of successful authentication) and PassImages (63%). Thus, and according to these results, this study will mainly focus on the robustness of these two techniques.

3. Methodology

The goal of this project is to assess the robustness of both PassImages and Cognitive Questions (see Figure 1 & 2). Thus, what should be considered is the potential of these methods to be compromised by impostors. To do so, tests have been conducted to investigate their resilience to would-be masqueraders, to determine whether the replacement methods might be more easily compromised then traditional passwords. To be as realistic as possible, the first challenge was to perform in a realistic way the impostors' behaviour. Thus, two persons were asked to behave like impostors by contacting the legitimate users in different ways and trying to obtain information that could help impersonation.

To assess the robustness of PassImages and, in a second step, cognitive questions, two approaches have been adopted: a theoretical analysis and practical tests. The aim of this dual analysis is to provide both mathematical analysis as well as pragmatic conclusions, and then try to compare them.

The aim of the theoretical analysis is to measure the ability of an impostor to guess the secret knowledge. Davis et al. (2004) conducted a study on graphical password schemes in which they used a measure that indicates this ability: termed the "guessing entropy". In order to compute it, the computer randomly selects a set of "test PassImages". Then the computer generates a random PassImages and checks whether it belongs to the test set. Then it selects another random one and so on. Once

all the PassImages of the test set are guessed, the computer returns the total number of attempts he performed. It then performs the same operation with another non-overlapping set of PassImages, until all the passwords distribution is covered. Finally, it calculates the average number of attempts, which is the average entropy.

Figure 1: PassImages authentication

Please answer carefully the following questions:

1. What is your mother's maiden name?	Kefi
2. Where were you born?	Tunis
3. What is your favourite colour?	Blue
4. What was the name of your best friend at school?	Mourad
5. What is your favourite music?	Jazz
6. What is your favourite food?	Coucous
7. What was the name of your first pet?	
8. Which primary school did you go to?	La Goulette
9. What is your favourite sport?	Volleyball
10. Where was your first house?	La Goulette
11. What make was your family's first car?	Peugeot
12. How old were you when you had your first kiss?	17
13. What is your favourite film?	
14. Where was the first place you remember going on holiday?	Rafraf
15. What was your favourite subject at school?	Maths
16. What is the most important part of your body?	
17. What is your favourite type of animal?	

Figure 2: Cognitive questions authentication

In addition to the theoretical study, it was decided that a practical test on authentication methods robustness would be performed in order to measure, in a pragmatic manner, the ability of an impostor to guess the secret knowledge. The first test consisted of physical and virtual meetings between would-be impostors and their targets. The challenge in physical meetings was to remember the conversation and especially details that can be useful for guessing the secret knowledge. Virtual discussions were performed with the help of Internet messengers, and are easier to remember since all the discussions are stored in a historic of conversation.

The second test was phishing. When setting up their passwords, an email containing all the secret knowledge was sent to the users and they were supposed to save it. The phishing strategy was to send them another email asking them to send back the subscription email. The trap was that the destination address was a forged one.

The third test was shoulder surfing. As its name implies, this refers to watching over people's shoulders as they perform authentication. The assessed users were asked to authenticate themselves with a person sitting behind them. The test was performed once with each of the users who agreed to the request.

Results of these tests would be compared with the theoretical ones in order to determine whether the theoretical robustness of some PassImages corresponds to real difficulties when trying to guess robust PassImages.

4. Results

The results of the statistical analysis were obtained with the help of a simulation made with a computer (Table 1). In order to get any significance from the numbers presented in this table they should be compared to the number of possible passwords. In fact, in order to select a PassImage a user should select the first image of his PassImage from one hundred ones, then the second image of his PassImage from the following ones and so on. According to a calculation made in this manner with the help of a computer, there are 1,192,052,400 possible PassImages for a maximum guessing entropy of 596 $*10^6$. The results show that the worst 10% of passwords can be guessed only after 980,297 attempts, and the worst 25% ones after more than four millions attempts. This result states that with an adequate brute force attack tool, the attacker would spend hours and even days to abduct the authentication process.

G (Average)	**286990167,2**
G median	**143490375**
G 10%	**980297**
G 25%	**4901487**

Table 1: Guessing Entropy for PassImages

It is also interesting to note that the average Entropy G^{Avg} is higher than the median G^{Med}. This means that there are many good passwords in the dataset that, by increasing the average number of guesses, they make it harder for an attacker to guess the PassImages.

Concerning the practical assessment, forty-three users received two emails asking them to send back or to communicate personal data. The results show that twenty-five persons succumbed to phishing (58%), from which twenty persons (46%) sent back the subscription email they received few weeks ago and sixteen (37%) persons dropped in the trap of the second email (asking them to re-authenticate to avoid account expiration). Finally, eleven persons succumbed to both traps (25%).

For a social engineering attempts, in order to be considered as successful, the impostor should be able to correctly answer at least 75% of the target's cognitive questions. In fact, cognitive questions techniques are considered too time consuming (Papadopoulos, 2002) and usually, the administrators implements a system that selects randomly from three to five cognitive questions, in spite of listing the twenty questions. By acquiring the answers for at least 15 questions, the impostor could typically expect to come across a set of questions he can answer. Forty-three users participated in this test, and were divided into categories as follow: 18% were close relatives, 28% were friends, 30% were colleagues or classmates and 23% had a non-significant relationship with the impostors. The most interesting thing here is the fact that the stronger the relationship with the user is, the more successful is social engineering. The success rate grows from 33% for strangers to 38% for colleagues and flatmates, then 66% for friends, and finally 87% for relatives. Globally, social

engineering is an efficient method to compromise the robustness of cognitive questions techniques, with a success rate of 53%.

The "shoulder surfing" test consisted of evaluating the ability of an impostor, sitting behind the legitimate user, to capture the password when the users are authenticating themselves, either with PassImages or with cognitive questions. Despite the small number of users assessed (20), some interesting conclusions emerge from the results. Eleven (55%) PassImages were held by the impostors, when only three successful attempts (15%) to retain answers of cognitive questions have been realised. The inefficiency of shoulder surfing with cognitive questions is obvious.

5. Discussion

According to the findings, PassImages and cognitive questions are unequally sensitive to the different attacks performed to assess their robustness. When social engineering seems to be efficient to bypass cognitive questions method (with a success rate of 53 %), its effectiveness to compromise the robustness of PassImages is less evident. In fact, and according to the comments of the impostors, trying to link the user's choice of images to their hobbies, activities or their past is simply inefficient. The impostors observed: "for instance, a user declaring he plays volleyball avoided the volley ball and selected the tennis one. He was not a smoker but selected a lighter and a cup of coffee. His favourite meal was a French meal made with peppers and minced meat, but he selected a picture of a lemon. Examples of such a contradictions between the users' profiles and their selections are various." In a rare case, an impostor successfully guessed the PassImages of his sister ("I just thought that for PassImages she would has chosen an easy context. I thought about selecting the images referring to his breakfast, and I succeed!").

In the other side, PassImages seems to be far more vulnerable to shoulder surfing (55% of success rate) than cognitive questions (15%). This can be explained by the fact that, in order to remember answers to cognitive questions, the impostors need to retain a large amount of information in a very short time. In addition, as the only five questions were displayed randomly each time, the information caught by the impostor is simply incomplete. It also shows that it is more easily to remember graphical information than the written one, which works in favour of shoulder surfing and against the technique. However, what must be remembered with this study is the fact that shoulder surfing was performed once with each user. In the real life, a diligent impostor may perform shoulder surfing more frequently in order to get all the information he needs.

Finally, we can conclude that the two techniques are complementary. In fact, in actual means of authentication, and more especially on Internet, many service providers portals and banks (e.g. yahoo, Gmail, HSBC) have adopted cognitive questions (for password recovery) coupled with traditional passwords in order to authenticate their customers. What could be suggested is to use a more efficient PassImages plus cognitive questions strategy.

Another important objective was to accept or disprove the hypothesis stating that the theoretical analysis of the dataset could be enough and avoid the need to perform practical assessments on authentication methods.

The success rate for guessing PassImages with practical tests was 58% (phishing), 55% (shoulder surfing) and 2.5% (social engineering). When balanced with the total number of participants for each test, the overall success rate of the practical tests is 30.25%. According to the theoretical study, the guessing entropy $G^{25\%}$ corresponding to the effort that an impostor should provide in order to guess the 25% weakest PassImages is 4,901,487 attempts. It is clear that the two persons acting as impostors have made far less efforts in order to achieve their results. In fact, what could be reproached to the theoretical study is the fact that, by its nature, it is a quantitative test and not a qualitative one: it is based on the analysis of the information the dataset contains, and not the way of extracting it. In addition, the statistical distribution of the images has shown that the most recurrent image represents only 2% of the overall selections which implies that no weakness have been revealed by the users' choice of a PassImages. In practice, the user's behaviour was insecure, careless and naïve in a general manner, and the theoretical analysis could not uncover it.

Finally, PassImages can be considered more robust than passwords in many aspects. First, passwords are more vulnerable to social engineering than PassImages and cognitive questions. Secondly, passwords are not more robust to phishing than the two alternative techniques: phishing relies more on the carelessness of the users than the authentication technique itself and we can state that all the listed authentication methods are equally vulnerable to phishing. Thirdly, unlike passwords, PassImages are more robust against sniffing: there are no alphanumeric data entered, and even if the hacker guesses the mouse movement, he could not repeat identically the authentication process since the images are refreshed randomly every time. By contrast, cognitive questions rely on alphanumeric data and thus, they are as vulnerable to sniffing as passwords unless encrypted. Nevertheless, PassImages are more vulnerable to shoulder surfing than passwords. In fact, by its nature, graphical information is more easily memorable than alphanumeric one, and this was established when comparing the vulnerability of PassImages to shoulder surfing confronted to the cognitive question one.

6. Conclusion

The experimentation produced many interesting results on the robustness of PassImage and cognitive question techniques. On one side, the theoretical assessment states that the number of attempts that an impostor should perform in order to get access to the system is astronomical and then the system can be considered as secure enough against brute force attacks. On the other side, the findings that emerged from the practical tests have shown that the theoretical study by its own is not sufficient to assess the robustness of authentication methods. In fact, the average success rate to bypass the process was a significant 30.25%. This

reflects the fact that, by its nature, the theoretical study is based on the analysis of the information that the dataset contains, and not the way of extracting it.

Despite the fact that the methods remove many weaknesses compared to passwords, they still suffer from some inherited ones. PassImages techniques are easily compromised with shoulder surfing when cognitive questions seriously suffers from the effects of social engineering. Moreover, both methods are prey to phishing. Nevertheless, the complementary nature of these techniques has been identified, and further studies should consider this aspect.

Another aspect of assessment could also be performed. In our study, only two impostors were volunteers to assess the robustness of the methods. Providing an environment on which more participants will be willing to act as impostors is an issue to consider for future researches.

Finally, this study suffers from a missing direct comparison of the assessed authentication methods compared to passwords. Future works should consider this issue in their conception.

7. References

Brostoff, S. (2004), *Improving Password System Effectiveness*, PhD Thesis, Department of Computer Science, University College London.

Charruau, D. (2004), *Assessing the Viability of alternative authentication methods*, MSc Thesis, University of Plymouth, UK.

Charruau, D., Furnell, S.M. and Dowland, P.S. (2004), "PassImages: an alternative method of user authentication", in *Advances in Network and Communications Engineering 2*, ISBN: 1-84102-140-7.

Danchev, D. (2005), "Passwords - Common Attacks and Possible Solutions", www.windowsecurity.com (accessed 03/09/2005).

Davis, D., Monrose, F. and Reiter, M.K. (2004), "On user choice in graphical password schemes", *Proceedings of the 13th USENIX Security Symposium*, San Diego, August 2004.

Irakleous, I., Furnell, S.M. and Dowland, P.S (2002), "An experimental comparison of secret-based user authentication technologies", *Information Management & Computer Security*, vol. 10, no. 3, p103.

Klein, D. (1990), "Foiling the Cracker: A Survey of, and Improvements to, Password Security", *Proceedings of the USENIX Second Security Workshop*, Portland, Oregon, 1990, p.3.

Morris, R. and Thompson, K. (1979), "Password Security: A Case History", *Communications of the ACM*, 22(11), Nov 1979.

Papadopoulos, I. (2002), *User Acceptance of Alternative Authentication Technologies*, MSc Thesis, University of Plymouth, UK.

Real User Corp., (2005), “Technology and products”, www.realuser.com, access [10/12/2005].

Standing, L., Conezio, J. and Haber, R. (1970), “Perception and memory for pictures: Single-trial learning of 2500 visual stimuli”, Psychonomic Science, Vol 2, p73-74.