

Chapter 2

IPAS: User Test Phase and Evaluation

Sadiq Almuairfi, Prakash Veeraraghavan and Naveen Chilamkurti

Abstract User authentication is one of the most important topics in information security. A text-based strong password scheme can provide a certain degree of security. However, as strong passwords are difficult to memorize, users often write them down on a piece of paper or even save them in a computer file. An image-based authentication scheme has been proposed as a possible alternative solution to text-based authentication, motivated particularly by the fact that humans can remember images better than text. Recently, many networks, computer systems and electronic-commerce environments have tried using a graphical technique for user authentication. All graphical and image algorithms comprise two different aspects: usability and security. Unfortunately, none of the graphical algorithms are able to cover both these aspects at the same time. In this paper, we evaluate the usability and security of different authentication schemes and compare them with our proposed scheme, which is the Implicit Password Authentication System (IPAS) by an experiment and a questionnaire survey.

Keywords Authentication • IPAS • Graphical password • Security • Usability

S. Almuairfi (✉) · P. Veeraraghavan · N. Chilamkurti
Department of Computer Science and Computer Engineering, La Trobe University,
Melbourne 3086, Australia
e-mail: sadiqjafar@students.latrobe.edu.au

P. Veeraraghavan
e-mail: p.veera@latrobe.edu.au

N. Chilamkurti
e-mail: n.chilamkurti@latrobe.edu.au

2.1 Introduction

In recent years, computer and network security have been seen as extremely important issues. A key factor in security research is authentication which is the determination of whether a user should be allowed access to a given system or resource. In this respect, the password is a common and widely authentication method still used currently.

Although traditional alphanumeric passwords are used widely, they have problems such as being hard to remember, vulnerable to guessing, dictionary attacks, key-loggers, shoulder-surfing and social engineering [1]. In addition to these types of attacks, a user may tend to choose a weak password or record his password. This may further weaken the authentication schemes. As an alternative to the traditional password-based scheme, the biometric system was introduced. This relies upon unique features unchanged during the life time of a human, such as finger prints, iris etc. The major problem of biometric as an authentication scheme is the high cost of additional devices needed for identification process [2]. The false-positive and false-negative rate may also be high if the devices are not robust. Biometric systems are vulnerable to replay attack (by the use of a sticky residue left by a finger on the device), which reduces the security and usability levels. Thus, recent developments have attempted to overcome biometric shortcomings by introducing token-based authentication schemes which relies on the use of a physical device such as smartcards or electronic-key.

Graphical-based password techniques have been proposed as a potential alternative to text-based techniques, supported partially by the fact that humans can remember images better than text [3]. Therefore, graphical-based authentication schemes have higher usability than other authentication techniques. It is also difficult to break graphical passwords using normal attacks such as dictionary attack, brute force and spyware which have affected text-based and token-based authentication [4]. Thus, the security level of graphical-based authentication schemes is higher than other authentication techniques as we proved in our experiment.

In this paper, we start with an overview of current authentication schemes in Sect. 2.2. Then, Sects. 2.3 and 2.4 describe the IPAS user test phase which is the core of this paper. Sections 2.5 and 2.6 explain IPAS usability and security levels from the user's perspective and provides user feedback. Finally, we present the conclusion and future directions in Sect. 2.7.

2.2 Related Work

In general, graphical password techniques can be classified into two: recognition-based and recall-based graphical techniques [5].

2.2.1 Recognition-Based Systems

In recognition-based systems, a group of images is displayed to the user and accepted authentication requires a correct image being clicked or touched in a particular order. Some examples of recognition-based system are Awase-E system, AuthentiGraph, and Passfaces system, one may refer to [2] for more details.

Although a recognition-based graphical password seems to be easy to remember, which increases the usability, it is not completely secure. It needs several rounds of image recognition for authentication to provide a reasonably large password space, which is tedious [6]. Also, it is obvious that recognition-based systems are vulnerable to replay attack and mouse tracking because of the use of a fixed image as a password. Thus, we consider these drawbacks in our IPAS system, which overcomes the problems of recall-based schemes too.

Pure Recall-Based Technique. With these types of systems, users need to reproduce their passwords without any help or reminder by the system. Draw-A-Secret technique and Passdoodle system are common examples of pure recall-based techniques. We have evaluated and discussed pure recall-based systems in our paper [2].

Cued-Recall Based Technique. With this technique, the system provides hints which help users to reproduce their passwords with high accuracy. These hints are presented as hot spots (regions) within an image. The user has to choose some of these regions to register their password and they have to choose the same region following the same order to log into the system. The user must remember the “chosen click spots” and keep them secret. There are many implementations, such as the Blonder algorithm and the PassPoint scheme which we covered in [1, 2].

2.3 IPAS Overview and its Advantages

IPAS is an intelligent imaged-based authentication framework that falls under the “What you know” type of authentication. In a traditional “what you know” type of authentication, either the password phrase or the image (in the case of an image-based password) is static and the user is expected to return the exact phrase (in the case of a textual password) or “click” on the exact location in an image (in the case of an image-based password) to the server for authentication. Since the user is expected to provide the same static information during every authentication cycle, it has a number of security pitfalls, including replay attack and shoulder surfing. IPAS is the most generalized authentication scheme that eliminates all the security pitfalls.

IPAS creates an intelligent user personalization profile for every individual user during the registration stage. The profile is based on the information (like pastime

hobbies, likes/dislikes, favourite movie stars etc.) provided by the user at the time of registration. The authentication server may have several images and each image may have more than one clickable area. Each clickable area may represent an object and have several text attributes associated with it. During the authentication process, the system presents to the user one or more pieces of information in an implicit image form. The user is expected to “click” on the correct area that represents the “expected information” in an implicit form to complete the authentication process. For example, if the user likes apples, the system may present an image of “Sir Isaac Newton” or a Macintosh computer. Since different information is expected from the user every time they log in through different images implicitly representing the information, IPAS is immune to the problems suffered by the “What you know” type of authentication schemes. Since IPAS may be configured to present to the user static information every time they log in (including static textual images), it may also act like other static authentication schemes.

2.3.1 IPAS Domains

Registered IPAS users can be categorized, in relation to their interaction behaviour, into two domains: region/state domain and word space/distance domain.

Various kinds of users in a system can, at times, have a different perspective of their needs. For instance, the perception of someone in America may not be the same as someone who is in Australia. Therefore, the system will consider the area/region where the user is during the creation of the user’s password and will link their information to the region domain. As a result, the objects in an authentication image will be related to the user’s region. For example, if the keyword or the information is opera, then users from Australia may easily recognize the Sydney Opera House; whereas users from Europe may more easily recognize the London Coliseum Theatre than the Sydney Opera house (some may not even recognize it at all). Thus, the system under this domain will be country/region dependent which should be considered during the production roll-out of the module.

In the space domain, we measure implicit level between word and object in an image. For example, let the chosen keyword be *apple*. An image which contains an *apple pie* will represent a closer relation to the word *apple*, while an image of *Steve Jobs* will represent a more distant relation to the word *apple*. The semantic variants of this concept can be developed quickly and with little effort by the system developer. We test these domains during our IPAS experiment and survey as below.

2.4 IPAS User Test Phase

2.4.1 Methodology

In our experiment, we tested IPAS using a number of participants from different backgrounds and with different experience in using authentication techniques. Participants include IT students, nurses, bankers, and miscellaneous workers. All participants engaged in the IPAS experiment and then answered our survey questionnaire.

2.4.2 IPAS Experiment

In our experiment, the participants were asked to read a given story/keywords, however, in the real-life implementation of IPAS, this would be provided by the user. The participants were then asked to match the keywords (password) with the object(s) in an image. The objects in the image implicitly represent one or more keywords. Three different stories and images were distributed randomly to the participants. We fetch the keywords of one story which was used in the IPAS experiment as follows:

Keywords selected in advance are: “*Unkempt Hair, Skyscrapers, Homeless, Dollar, Eagle, and Rat*”.

Training Phase. At the beginning of the experiment, we informed participants of its main purpose and what they would do before, during, and after the experiment. Then, we explained the definitions of the different authentication schemes: text, biometric, token, graphical and image-based password schemes with simple examples and figures. After this, an overview of IPAS, the experiment steps, and the survey questions were discussed. We also showed them several images and the way to link keywords with the object in the image.

We clarified the difference between IPAS and PassPoint as follows: PassPoint uses one image with different click points (passwords) for all users during the authentication process, while IPAS uses a new image with different objects to represent the password every time. The IPAS image is changed with every authentication process to avoid replay attacks or shoulder surfing. Also, IPAS is a one-to-many relation which means one word (password) is represented by many implicit objects within the image while the Question Hint scheme is a one-to-one relation between the password and its question. For example, the word *apple* in IPAS could be represented as apple pie, apple juice, Steve Jobs etc. while in the Question Hint scheme; the word *apple* will be the direct answer for a question “What is your favourite fruit?”. In this stage of the IPAS experiment, we answered any questions and concerns which were raised by the participants.

Experiment Phase. To begin with, we asked the participants about the circled objects in the given image as in Fig. 2.1. The most common answers were direct or

Fig. 2.1 IPAS sample image with implicit objects



explicit words *comb* and *drink bottle*. After this, we asked the user to read the above story and keywords and then to implicitly match the keywords and objects with the given image by marking the correct object. Most users were able to implicitly link the keywords *unkempt hair* and *skyscrapers* with the correct objects within the image which means that they were able to recall the password correctly. After this, the users were asked to answer the survey questions which compared IPAS with other well-known authentication schemes from a usability and security perspective.

The motivation for this survey is multifold. First, we analyze the authentication schemes based on usability and security parameters. Then, we compare IPAS with current authentication schemes in relation to usability and security issues.

2.4.3 Survey Questions

In this section, we give an overview of our survey questions. In the section on demographic information, we ask two questions: one about age and the other about gender. Then, the survey is divided into two main categories: general information about authentication schemes and IPAS evaluation after performing the experiment. The last part of the survey asks users to make comments and suggestions.

The category on general information about authentication schemes included the three following questions: Question# 1 “How frequently do you deal with the below authentication schemes? Tick one box for each scheme”. Response options for this question were “Always”, “Usually”, “Often”, “Rarely”, and “Never”. The second question was “How do you evaluate the below authentication schemes from an ease-of-use perspective?” Response options for this question were a rating from 1 to 5 where 1 is easy and 5 is difficult. The third question was “How do you evaluate the below authentication schemes from a security perspective?” Response

options for this question were a rating from 1 to 5 where 1 is not secure at all and 5 is strongly secure.

The IPAS evaluation category includes six questions which cover the main and minor factors as follows:

(1) How do you evaluate IPAS from an easy-to-use perspective? (2) How do you evaluate IPAS from a security perspective? (3) What do you think about the story in the IPAS experiment? (4) Do you prefer a close or a distant relation between the key word and object in the image? (5) What kinds of stories do you prefer? (6) Do you like stories in your native language? (This question is for non-English speakers.)

The response options for questions 1 and 2 were similar to those for questions 1 and 2 in category one. For the third question about the IPAS story, the participants were required to respond with a rating from 1 to 5 where 1 is too short and 5 is too long to indicate their opinion about the length of the IPAS story. In question 4, the participants were asked about the relationship between keywords and the object in the image. Response options for this question were a rating from 1 to 5 where 1 indicates a direct/explicit relationship and 5 is an indirect/implicit relationship. To enhance IPAS domain objectives and to evaluate the effects of the minor factors, we asked the participants in question 5 about the type of story they preferred. The responses for this question were Regional, International, or Both. The last question in this category was a specific question to evaluate the language in the IPAS story, especially for non-English speakers. The responses for this question were either yes or no.

At the end of the survey, we included an open-ended question for participants' comments and suggestions about the IPAS experiment and the survey on the authentication schemes.

2.4.4 Survey Analysis

The responses to the demographic information showed that 29 % of the participants were female and 71 % were male. In relation to the age of the participants, 54 % were aged from 18 to 30 years, 45 % were aged from 31 to 50 and 1 % were more than 50 years old. The authentication schemes which were included in our survey are: the test-based authentication scheme, the biometric-based authentication scheme, the token-based authentication scheme, the graphical-based authentication scheme, and the image-based authentication based.

Our first question asked how frequently the participants used the authentication schemes, with five response options being always, usually, often, rarely, and never. In response to the question as to how frequently the participants used the authentication schemes, the survey respondents answered 75 % always, 14 % usually, 6 % often, and 2 % for each rarely and never, respectively.

The participants indicated that the second most popular authentication scheme was the token-based scheme with 22 % responding always, 15 % usually, 14 %

often, 16 % rarely, and 33 % never. The biometric authentication scheme was the third most popular, with 24 % of respondents reporting (always and usually) above average, 16 % average (Often), and 60 % below average. Finally, graphical-based passwords and image-based password were the least popular of the authentication schemes with only 7 % of respondents indicating they had dealt with image-based passwords and 86 % indicating they had either rarely or never used an image-based authentication scheme.

The results indicate that a text-based password is still the most common form of authentication preferred by most participants. Conversely, an image-based password is almost unknown to most of the participants, therefore there needs to be greater awareness of and research into this type of authentication scheme.

The next questions were designed to evaluate the usability and security of the current authentication schemes in order to compare them with IPAS, which is the aim of our survey.

2.5 Usability of IPAS

Usability refers to the degree to which a system is easy to learn, use, and meets the user's needs. Even though many authentication schemes have been proposed to improve password strength, the responses to the usability of these systems indicate that yet another improved scheme needs to be introduced. Therefore, in our survey, we use a scale to study user's feedback on the different authentication schemes.

The scale in this area was divided into five stages: easy, a little easy, acceptable, a little difficult, and difficult. In this question, we include IPAS and other authentication schemes to measure which is considered to be an easy method of authentication by participants.

The five abovementioned stages were revised into three stages as follows:

Acceptable = Average, Easy, a little easy = Above Average, Difficult, a little difficult = Below average.

As a result, a total of 81 % (63 % easy and 18 % a little easy) of participants said that it was easy to use a text-based password, 13 % indicated it was acceptable (average), and only 6 % considered a text-based password scheme difficult to use as a way of authentication. Usability of biometric, token-based, and graphical-based authentication schemes are 46, 48, and 38 % respectively. Thus, most users consider them as difficult to be used.

The responses to image-based password schemes were as follows: 30 % indicated that they are easy to use, 21 % indicated acceptable, and 49 % considered them difficult to use as an authentication scheme. In general, image-based passwords were considered difficult to use by the majority of participants.

In relation to IPAS, most participants (54 %) indicated it was easy to use, 25 % indicated it was acceptable, and 21 % indicated it was difficult to use as an authentication scheme. Therefore, according to the participants' feedback, IPAS is easier to use than other image-based authentication schemes.

The majority of participants (81 %) indicated that text-based password schemes were the most usable, IPAS was the second most usable authentication scheme (54 %), the token-based scheme was the third most usable at (48 %), followed by the biometric (46 %), graphical (38 %) and image-based schemes, (30 %) respectively.

2.6 Security of IPAS

In this question, we analyze participants' opinions regarding the security level of different authentication schemes. The response options to this question were "Not Secure at all", "Less Secure", "Acceptable", "Secure", and "Strongly Secure" for each scheme. Also, we included IPAS with other authentication schemes to measure which authentication scheme was considered the most secure scheme.

The five abovementioned stages were revised into the three stages as follows: *Acceptable = Average, Secure and Strongly Secure = Above Average, Not secure at all & less secure = below average.*

We selected above average (secure and strongly secure) values to evaluate the security level of the given schemes. Most of the participants (65 %) considered biometric-based authentication scheme as the most secure scheme, with the second most secure authentication scheme being IPAS (58 %), followed by the image-based password (55 %), token-based (53 %), and graphical-based (52 %). Only 27 % of the participants thought that the text-based password scheme was a secure scheme.

The responses showed that overall, the participants felt that IPAS was the second most secure of the authentication schemes. Furthermore, they indicated that the image-based password scheme had an acceptable level of security which implies that password entropy in image-based password schemes is longer than text-based password schemes. Therefore, IPAS achieved the required balance of usability and security to be used as a primary authentication scheme.

2.7 Conclusion and Future Directions

In this paper, we compared IPAS with other authentication schemes by performing two experiments and asking participants to answer a questionnaire. We then explained the usability and security of IPAS from the users' point of view. In our subsequent papers, we will try to present the dynamic IPAS as a new version of IPAS with more features to obtain a better balance between usability and security.

References

1. Almuairfi S, Veeraraghavan P, Chilamkurti N (2011) IPAS: implicit password authentication system. In: Advanced information networking and applications (WAINA), 2011 IEEE workshops of international conference on advanced information networking and applications
2. Almuairfi S, Veeraraghavan P, Chilamkurti N (2013) A novel image-based implicit password authentication system (IPAS) for mobile and non-mobile devices. *Math Comput Model* 58(1–2):108–116. ISSN 0895-7177, [10.1016/j.mcm.2012.07.005](https://doi.org/10.1016/j.mcm.2012.07.005)
3. Xiaoyuan S, Ying Z et al (2005) Graphical passwords: a survey. In: 21st annual computer security applications conference, pp 463–472
4. Wells J, Hutchinson D, Pierce J (2008) Enhanced security for preventing man-in-the-middle attacks in authentication, data entry and transaction verification. In: Australian information security management conference. Paper 58
5. Xiaoyuan S, Ying Z et al (2005) Graphical passwords: a survey. In: Computer security applications conference, 21st annual
6. Pierce JD, Wells JG, Warren MJ, Mackay DR (2003) A conceptual model for graphical authentication. In: 1st Australian information security management conference, 24 Sept. Perth, Western Australia, paper 16

Frontier and Innovation in Future Computing and
Communications

Park, J.H.; Zomaya, A.; Jeong, H.-Y.; Obaidat, M.S. (Eds.)

2014, XXVIII, 923 p. 427 illus., Hardcover

ISBN: 978-94-017-8797-0