'H-IBAS-H' - Authentication System for University Student Portal Using Images

Haitham Al-Sinani[1], Chi Nguyen [1], Branislav Vuksanovic [1]

Abstract— **Nowadays, most of the authentication systems rely on a precise recall of passwords and/or personal identifier numbers (PINs). As the number of on-line services requiring authentication continues to rise sharply, the number of passwords needed continues to also rise! The burden on users to remember such an increasing number of passwords leads to poor and predictable choices as users seek passwords that they can readily remember. This has a potential security risk that could endanger users' privacy, e.g. identity theft. For certain applications, research suggests that the use of images may be a more effective combination of both security and ease of use. This is because humans are, by far, better at recognising images that they have previously seen than they are at remembering passwords. In addition, it may well be possible to improve the usability of authentication systems through the use of images. In this paper, an experimental authentication system, called H-IBAS-H, has been developed for use by students when authenticating to their University student portal. H-IBAS-H authenticates students based on their ability to recognise previously seen images.**

Prior to presenting H-IBAS-H to users, a user questionnaire was developed. H-IBAS-H was, then, tested on three experiments; a pilot survey, a one-time experiment and a four-week experiment with more than 100 members (both staff and students) of the Department of the Electronic and Computer Engineering (ECE) at the University of Portsmouth and their feedback has been collected and, subsequently, analysed. One of the astonishing results of the user testing is that about 94% of the participants succeeded in authenticating with H-IBAS-H. This is despite the previous hypothesis that only about 50% to 60% were expected to succeed. The H-IBAS-H findings illustrate some *novel* theories that are of significance to the study of image-based authentication systems. An example of this is that "flexibility in key generation" is significant to achieve high success in image-based authentication systems.

Index Terms— **Authentication, challenge-set, decoy-images, image-based authentication, pass-images, sampling.**

1. INTRODUCTION

1.1. Authentication definitions

AUTHENTICATION can be defined as the process of verification that someone is actually who they claim they are [1]. In other words, authentication is the act of establishing or confirming something (or someone) as authentic, i.e., that claims made by or about the thing or the one are true [2]. In another resource, authentication is defined as the process of determining whether someone or something is, in fact, who or what it is declared to be [3]. Authentication is needed to let the system perform some tasks for the user. The user needs to be authorized to request services from the system"[4]. Thus, it could be concluded that the authentication is simply the process of establishing a level of confidence regarding a claim [5].

Since the authentication basically **verifies** a **claim**, it can be rightly assumed that the authentication is made up of two main parties; a claimer and a verifier (usually this is the issuer as well)[5].

1.2. Authentication types

Human authentication factors are generally classified into three cases; something the user knows (e.g. password), something the user has (e.g. ID card) and something the user is or does (e.g. fingerprint [5, 7]). Hence, the authentication can take the form of one or more of the following:

1. "Knowledge-based systems".
2. "Biometric-based systems".
3. "Token-based systems" [6].

Often a combination of these methods is used, in which case the term "two-factor authentication" is used. [5] A traditional example of this is the use of a bank card and a PIN at the ATM machines.

1.3. Weaknesses of existing authentication systems

By far the most common form of authentication is knowledge-based systems, of which the most widely used type is text-based authentication systems [4, 6, 8, 9, 10]. Although biometrics can demonstrate valuable use for user authentication, it yet to suffer from a number of drawbacks such as that if it is not totally unchangeable, then it is difficult to change and maintain[4]. In addition, many biometric systems require specialised devices and can be unpleasant to use. Additional hardware undoubtedly means additional cost, which raises questions about whether they are affordable, in particular to the every day users.

Token-based systems are, also, not perfect solutions since they can be easily lost or stolen. Therefore, many token-based systems employ knowledge-based authentication systems to prevent impersonation through theft or loss of the token [6].

Despite their common use and their world-wide popularity, text-based systems, particularly passwords and PINs, experience a number of shortcomings. On the one hand, simple, short and/or meaningful passwords are easier to remember but vulnerable to attacks. These attacks can be as a result of a guess due to the **predictability** of the humans' behaviour or can be as a result of the technology using brute force attacks like attempting different passwords (on-line attacks) or by off-line attacks on the password hash file. On the other hand, arbitrary and complex passwords are more secure but, however, they are more difficult to remember. Yet, brute force attacks are still applicable here. Since users can only remember a limited number of passwords, they tend to write them down. What is even more disastrous, which can result in a total fiasco, is that some users would simply and foolishly use almost similar if not exactly identical passwords for applications which require a higher level of security such as bank accounts and for applications which are not very critical such as the infrequently-visited websites.

1.4. Proposed countermeasures for passwords weaknesses

Almost countless attempts have been made to suggest solutions that are capable of addressing the weaknesses of the passwords. The majority of these solutions can be grouped in a number of distinct

[1] Department of Electronic and Computer Engineering, Faculty of Technology, University of Portsmouth, Anglesea Building, Anglesea Road, Portsmouth, Hants, PO1 3DJ, United Kingdom (website: www.oman4ever.org, e-mail: ece50148@port.ac.uk)

categorizes. The first being the employment of strict password polices where users are, for example, required to update their passwords on a weekly basis. In many situations, this technique miserably backfired to its proposers since users started to come up with some tricks to counter such strict policies. For instance, whenever there is a requirement for updating passwords, they would just make a variation on the old password or reuse some other older passwords or simply swap them with their friends or family or they would go all the way to write them down if necessary.

The other solution is the usage of proactive security measures that aim to identify weak passwords by constantly running password cracking programs, such as 'John the ripper, JTR'. Another approach, which is still technical in nature, utilizes techniques to increase the computational overhead of cracking passwords. Furthermore, another group of solutions includes user training and education to increase security awareness and to establish security guidelines and rules for users to follow. “Unfortunately, all these proposed solutions do not remedy the main cause of password insecurity, which is the human limitation in terms of memory for secure passwords” [6].

1.5. Authentication systems and idealism

The reality is that no one could, at least currently, claim that a particular authentication system is the ideal system that can perfectly fit all environments, wonderfully serve all purposes, or work best under all circumstances. The reasonable argument is that a particular authentication system should work the best to its potential when specifically designed to serve a particular environment under certain and predefined conditions.

1.6. The case of image-based authentication systems

Analysing the solutions that are intended to address the weaknesses that the character-based authentication systems suffer from lead to one obvious conclusion; those solutions have a common weakness shared between all of them and that is their negligence of the significance of the human limitation in terms of memory. This negligence negatively and severely impacts on humans' ability to remember the character-based passwords [6]. From this, a relatively recent wave of solutions has erupted. What makes these solutions special is the fact that they signify the principle that humans have a limitation in terms of memory and have, therefore, introduced a newer way of coping with the passwords' weaknesses and that is; *recognise rather than remember!* Such systems are known as “recognition-based systems” and their idea has originated from an interesting but a scientifically-proven fact, which simply states that humans have a far greater capacity for recognition than they do for recall. In other words, a user is far more adept at recognising an image that they have previously seen than recalling a word or a phrase that they have attempted to commit to memory [6, 7, 8, 9, 11].

On the top of them being easy on humans in terms of reducing the need to memorise more passwords, other advantages which make the use of image-based authentication systems attractive is that they are simple enough, cost effective, do not require any additional hardware and more interestingly they are fun to use [6]!

2. H-IBAS-H

This paper proposes an experimental authentication system, named as **H-IBAS-H**. The name ‘H-IBAS-H’ is simple enough that it comes from the first letters of “**I**mage **B**ased **A**uthentication **S**ystem”, which make up IBAS, and the two Hs represent the first letter of the system developer, i.e. “**H**aitham”. H-IBAS-H is designed so that it aims to achieve the following:

- Minimise the user's cognitive load.
- Help the user make fewer mistakes.
- Prevent users from choosing weak passwords.
- Make it difficult to write passwords down or share passwords or describe passwords with or to others.
- Provide more pleasant experience, i.e. Make H-IBAS-H fun to use!

2.1. Primary user of H-IBAS-H

H-IBAS-H is designed primarily to be the login system authenticating the University students to their student portals.

2.2. H-IBAS-H stages

H-IBAS-H is made up of two main stages; the first is the registration stage, which is considered to include the training part, and the second stage is the authentication stage.

2.2.1. The registration stage

At the registration stage, the users are required to fill in their details such as their 'unique' username, their 'valid' e-mail addresses and any other details marked with *. They, also, have to select the correct amount of pass-images. If the offered images do not appeal them, they can refresh the registration page as many times as they wish to view more and more images, until they find images that they are comfortable with. Then, upon entering their details and choosing their images, they may click 'submit' to move on to the training phase where they have to correctly identify their pass-images from among a mixture of decoy images.

2.2.2. The authentication stage

H-IBAS-H puts forward **a novel authentication algorithm** such that the pass-images are randomly distributed on the login rounds. Therefore, every round may have all, some or none of the pass-images. At least, one login round must contain no pass-images, to battle the intersection attack.

2.3. H-IBAS-H modes

H-IBAS-H can work on a pre-set and/or a flexible mode.

2.3.1. Pre-set mode

The H-IBAS-H administrator, in this mode, takes responsibility in setting the number of the *pass-images* and the number of the *training* and the *login* rounds that the student must go through as well as setting the number of the *permissible attempts* to retry to authenticate in case of failure.

2.3.2. Flexible mode

All the features included in the pre-set mode are, also, applicable here but to provide maximum flexibility, the settings for the number of the *pass-images*, the *login* and the *training* rounds lay within the users' responsibilities.

3. H-IBAS-H JUSTIFICATIONS

3.1. The use of random art

H-IBAS-H uses random art images as they have the advantage that whilst they are identifiable, they are extremely hard to describe.

3.2. H-IBAS-H is made configurable

Given the flexibility provided by H-IBAS-H's flexible mode, and with the additional facts that the size of the challenge-sets as well as the number of allowable login attempts could be configured upon the user's request, it could be stated that H-IBAS-H has the additional benefit of providing a flexible authentication framework that can handle various situations.

3.3. Adaptation of the multiple-round technique

H-IBAS-H attempts to improve the security by adopting some methods, in which, there are no necessity to further increase either the size of the challenge-set or the number of the pass-images. One such method is the use of more than one authentication round. In this case, the authentication is split up into multiple rounds. Each round presents a challenge-set including all or some or none of the pass-images. The probability of a random attack succeeding would then be given by the combined probability of successes in each round.

3.4. Keeping the number of the login rounds configurable

If the system "H-IBAS-H" is restricted to have one image per login round, an attacker would easily be able to deduce the number of the pass-images since the number of the login rounds is equal to the number of the pass-images. As a countermeasure, the approach of keeping the number of authentication rounds configurable is proposed. It attempts to blur the correlation between the number of the login rounds and the number of the user-images.

3.5. Variation of the number of user images in each round

The number of the pass-images included in the challenge-set differs for each authentication round. It is, also, possible that the challenge-set may not include any user-images, i.e. pass-images, at all. Through the introduction of such additional unknowns, not only does an attacker have to determine whether this particular round includes any pass-images but, if they assume it does, they would have to guess how many of the user's images were presented in the challenge-set in that round and they would have to decide what those images were.

3.6. Inclusion of 'no pass-image(s) is/are presented'

This is a *two-in-one* approach that while it aims to solve the restriction in humans' memory, it also helps to fight the intersection attack [8, 11].

3.7. Randomization of the image positions on each round

H-IBAS-H randomly varies the location of images within the challenge-set and varies the decoy images in the challenge-set itself on every authentication round. This would mean that the system could not be attacked by recording a student's responses and attempting to replay them at later times.

3.8. Proceeding on error

If a student fails to correctly identify their pass-images in any single round of authentication, H-IBAS-H does not terminate and neither does it inform the students/users of their error(s) but the authentication process proceeds as normal. H-IBAS-H tells the users whether their authentication is successful only at the end of the authentication process. This would ensure that a malicious entity cannot exactly determine the point of failure.

3.9. Retry sessions and locking accounts

To minimise brute force attacks, H-IBAS-H denies access after a number of unsuccessful attempts to authenticate. However, care should be taken when blocking students' accounts as not to open the doors to the denial of service attacks. Legitimate users can reactivate their accounts through emails or through their administrators.

3.10. Reverse to previous login rounds is prohibited

H-IBAS-H does not allow going back to the previous rounds/pages. This is to eliminate a possibility that the attackers could brute-force attack the images presented on the challenge-set.

3.11. Refreshing at the login rounds means continuation

If a login round is refreshed; H-IBAS-H takes the user to the next login round. It is obvious that this technique helps fight the intersection attack as well.

4. USER STUDY

Following the implementation of H-IBAS-H, a user study was conducted which involved three phases:

1. Development of a user questionnaire.
2. Documentation of the hypotheses of the H-IBAS-H developer.
3. Conduct of the questionnaire with real users.

4.1. H-IBAS-H settings

For the user study purposes, H-IBAS-H pre-set mode was operated which was set to work with **4** pass-images, at least **2** training rounds, **4** login rounds and a challenge-set of size **21**.Users were allowed to retry to log in up to **3** times.

4.2. Development of a user questionnaire

A seven-page user questionnaire was developed. It aimed to:

1. Build a trust relationship between the interviewer and the interviewee(s).It served to filter the participants into different groups.
2. Discover the reasons behind the users' choices of their pass-images.
3. Assess the time consumed while registering and logging with H-IBAS-H.
4. Assess the ease of use of H-IBAS-H.
5. Obtain the users' opinions as in where H-IBAS-H stands in comparison with other authentication systems in terms of speed, ease of use and joy of use and many more.
6. Find out the reasons behind the inability by some users either to register or to authenticate with H-IBAS-H.
7. Assess other different areas that are not covered above.

4.3. Documentation of the hypotheses

In this phase, the H-IBAS-H developer documented his own thoughts and assumptions of what the answerers to the survey questions would be. These hypotheses are based on the readings and the background research that the H-IBAS-H developer has formerly conducted. The readings involved close examination of the survey data collected and found by the Awase-E and Déjà Vu user studies. These hypotheses will be compared with the real results that the H-IBAS-H user study would yield.

4.4. Conduct of the H-IBAS-H experiments

The third phase of the user study involved conducting three experiments; the pilot survey, the one-time experiment and the four-week experiment.

4.4.1. The pilot survey

The pilot survey is defined as "a preliminary survey undertaken to test whether a survey questionnaire has been properly designed" [16]. The pilot survey, carried out in the H-IBAS-H project, could be thought of as an initial study that aimed to solve any ambiguities in the questionnaire. In addition, it served to get a feel from the 'real' users about their experience with H-IBAS-H software. The survey questions were edited accordingly and H-IBAS-H was technically adjusted so that it performs its functionality in a better user-friendly environment.

4.4. 2.The one-time experiment

In this part, the survey targeted the ECE department, staff and students. Since surveying the entire ECE department was neither practical nor possible within the time allowed, there was a need to survey a reasonable sample of the ECE. For this purpose, the *random stratified sampling* was used.

4.4. 2.1. Random stratified sampling

Random Stratified Sampling is where as the population is divided into subpopulations (strata) and random samples are taken of each stratum [12]. Overall, it can be stated that the two main reasons for the use of the stratified sampling were firstly to ensure that the distinctive groups within the ECE population are adequately represented in the sample, and secondly to improve efficiency by gaining a greater control on the composition of the sample [13-14]. In addition, the use of the stratified sampling makes it possible to work out the variances between the different groups, i.e. strata. Thus, it would be possible to deduce whether the differences in age or on the educational level have a major influence on image-based authentication systems.

4. 4.2.2. Conduct of the one-time experiment

The ECE population was divided into 5 distinctive groups which are; the *first year* group, the *second year* group, the *third year* group, the *Masters + PhD* group, and the *staff* group, which included the lecturers, system administrators, and the technicians. A sample size of equal percentage, 10% of each group, randomly selected, has been surveyed. As for the participants, all of them have used and currently use student or staff portals. Also, they are all familiar with the ATM machines and, undeniably, they are all familiar with the traditional user name and password systems. The experiment was mostly conducted by means of face-to-face interviews. During the experiment, the participants were invited to firstly register and log in with H-IBAS-H and then to answer the survey questions.

4.4. 2.3. Data cleaning

At this part, a cleaning approach was conducted to eliminate all the unreasonable and biased answers.

4. 4.3. The four-week experiment

The main objectives for this experiment are to:

1. Inspect whether the number of experiences with H-IBAS-H has an effect on the participants' answers.
2. Examine the effects of updating the student's pass-images after becoming familiar with the old ones in terms of whether the new pass-images would be confused with the old ones.
3. Study the effects of having more than one image-set.
4. Evaluate the participants' ability to recognise their images over a period of four weeks.

4.4. 3.1. Conduct of the four-week experiment

4. 4.3.1.1. Week 1

20 randomly selected participants, all from the ECE, were asked to register and to authenticate with H-IBAS-H. Then, they were all asked to fill in a survey.

4.4. 3.1.2. Week 2

The 20 participants were asked to authenticate to their corresponding accounts using H-IBAS-H and they were required to fill in the corresponding survey.

4. 4.3.1.3. Week 3

Two experiments were conducted as follows:

1. Participants were firstly asked to authenticate and then they were asked to fill in an identical survey to that of week 2.
2. Participants were invited to create a new account with H-IBAS-H. Then, they were asked to authenticate with their new pass-images and were asked to fill in an identical survey to that they filled in week 1.

4. 4.3.1.4. Week 4

Three experiments were conducted here as follows:

1. First of all, the participants were asked to authenticate to their newer account using H-IBAS-H. Regardless to whether they passed or failed, the participants were, then, asked to complete the corresponding survey.
2. Secondly, the participants were asked to authenticate to their 'older' accounts that they created in week 1. They were, also, asked to fill in the corresponding survey.
3. Thirdly, the participants were asked to use the '*flexible*' mode where they were allowed to freely choose the number of the pass-images and the number of the training and login rounds.

5. Data analysis

5.1. Success in the usability of H-IBAS-H

The survey results show that the rate of success has been high, both with the registration and the authentication with H-IBAS-H. This high rate of success has been shocking since a success above 90% was never expected. This is due to the complicated authentication algorithm used, i.e. 4 pass-images are randomly distributed on random locations on the 4 challenge-sets on the 4 login rounds. Yet, astonishingly 94.3% of the total participants were able to successfully authenticate. The following factors are believed to have some direct or indirect relationships with the mentioned success:

1. Flexibility in key generation.
2. Exclusion of similar key inputs.
3. Disallowance of a key input to appear more than once.

5. 2. Flexibility in key generation

5.2.1. Observation

The flexibility in key generation represented in the "reload/refresh" feature contributed towards the high success in registering and authenticating with H-IBAS-H.

5.2.2. Discussion

In H-IBAS-H, flexibility in key generation is granted by means of refreshing the registration page. When the registration page is refreshed, different key inputs, i.e. images, are shown, and thus become available for selection. The users can, therefore, select the keys, i.e. image-sets, that they are the most comfortable with and which they think they can recognise easier and better. This flexibility has proven to be a key factor to the high success in H-IBAS-H on the usability side.

Currently, H-IBAS-H has a bank of 783 images, from which keys can be created. This is, by far, more than the bank of the traditional password-based and PIN-based systems which only rely on some of the ASCII characters. In total, there are 256 ASCII characters [15]. However, not all the password systems support the full ASCII characters. In fact, many of them only support 36 characters; the 26 English alphabets and the 10 numerical digits. This is particularly true at an ATM machine where only the 10 numerical digits, 0 to 9, are permitted to be used as inputs to form a 4-digit PIN. Thus, it can be concluded that H-IBAS-H provides higher flexibility in terms of key generation than that provided by the password and the PIN systems. While the flexibility in key generation can be a key factor in the success of authentication systems, and can open the doors to their world-wide popularity, as in the password systems, such flexibility could, however, result in some negative consequences. For example, it could become a time-consuming task, especially in image-based systems where users can spend quite a time browsing for images. Similarly, this is also found in text-based systems where users can spend a lot of time trying to think of a new, unique, and memorable password that they have not used before. Nevertheless, H-IBAS-H users have expressed that they found it fun browsing for new and different images. In fact, some of them stated that it was more of a hobby to them rather than an effort. Where users enjoy refreshing the registration page to view more images, the fact that they spend time doing that becomes insignificant. Flexibility in key generation could, also, lead to the creation of describable keys, an issue that image-based systems, in particular H-IBAS-H, struggle to avoid. Such an issue can, however, be remedied if all of the describable and weak key inputs, i.e. images, are manually removed such that all the remaining images are thought of as being potential candidates for image-sets.

5.2.3. Finding

For image-based systems, “flexibility in key generation” should be provided if the system is desired to gain high success in usability! This is an example of a piece of information that could not have been possibly learnt without the implementation of H-IBAS-H and then without the development and the conduct of the corresponding survey.

5.2.4. Image-based versus text-based authentication systems (in terms of flexibility)

Flexibility in key generation is as good in image systems as in password-based and PIN-based systems. In fact, it may well be actually better in image-based systems since the number of key inputs available to choose from could be, by far, more than that available in the text-based systems.

5.2.5. Evaluation

H-IBAS-H offers better flexibility in key generation than the traditional password and PIN systems. Hence, image-based systems may have brighter future than the password systems.

5.3. Exclusion of similar key inputs

5.3.1. Observation

The vast majority of the similar key inputs in H-IBAS-H have been manually removed. This has greatly contributed towards the mentioned high success with H-IBAS-H.

5.3.2. Discussion

The images used in H-IBAS-H have been downloaded from the random art website, “www.random-art.com”. In total, a bank of 1000 images has been initially downloaded, some of which were similar or even too similar. At the initial testing of H-IBAS-H, and in particular while the ‘pilot’ study was being conducted, it was deduced that the similar images needed to be removed. Thus, most if not all of the similar images were manually eliminated and the image-bank in H-IBAS-H was reduced down to 783. Similar images, mainly the ‘too’ similar ones, created huge confusion to users and presented a threat to both the usability and the security of H-IBAS-H. It threatened the usability in terms that it confused the users and it endangered the security of H-IBAS-H since it can be more than reasonable to assume that users are likely **not** to pick images for their image-set if they think that they would not be able to distinguish between them as they are too similar. Thus, from an attacker point of view, the too similar images on a particular challenge-set can be ruled out on the assumption that they could have not been chosen as pass-images. The manual removal of the similar key inputs has been, thus, a wise remedy to such threats, leading to the success of H-IBAS-H on both the usability the security sides.

In addition to the deletion of similar key inputs requiring a lot of physical effort, exclusion of similar key inputs might not be possible in some scenarios with image-based systems such as where images are automatically created during the run time! This is one reason why such approach was not adopted with H-IBAS-H.

It is worthy of note that H-IBAS-H is not the only authentication system that uses keys, some of its inputs were similar. Yet, the recall-based systems still include some similar key inputs. For instance, the traditional password system allows the use of capital ‘I’ as in the word ‘Inn’ and also allows the use of lower case ‘L’ as in the word “lamp”. In addition to the number one ‘1’, the pipe “|” is also allowed as a valid key input in some password systems. Clearly, the password inputs, “I 1 1 |” are too similar and may well be confusing! Although they have been around for decades, they still exist as valid ‘inputs’ in use by the password systems. However, since the text-based passwords depend on recall rather than recognition and then input of keys rather than identification of keys, such an issue may not be of concern with the recall-based systems.

5.3.3. Finding

For image-based authentication systems, “similar images” should be eliminated if the system is desired to score a high percentage of success in usability. A supportive factor to this finding is that the vast majority of the students who failed either to log in or to complete their training rounds mentioned that the similarity between the key inputs, i.e. images, was a key factor to their failure.

5.3.4. Image-based versus text-based authentication systems (in terms of similar key inputs)

If H-IBAS-H is compared against a password system that only employs the alphabets and digits, H-IBAS-H is found to offer as, if not better, dissimilar key inputs as the password system. This is despite the fact that H-IBAS-H currently uses 783 key inputs while the mentioned password system only uses 36 key inputs or 62 key inputs if upper and lower cases were considered.

5.3.5. Evaluation

While the similar key inputs can characterize a major concern for recognition-based systems, recall-based systems, on the other hand, do not hugely suffer from such problems. Consequently, it can be rightly stated that the ‘too’ similar key inputs are an inherent issue in recognition-based systems! The exclusion of such key inputs is, therefore, a significant factor for the success of recognition-based systems, such as the image-based systems.

5.4. Disallowance of a key input to appear more than once

5.4.1. Observation

In text-based systems, it is permitted to use one key input more than once in a password or a PIN. By contrast, this is strictly prohibited in H-IBAS-H. That is to say, the image-sets that the users have to select must include different images. A user is not allowed to use the same image more than once in any single image-set.

5.4.2. Discussion

Password-based and PIN-based systems are classically considered to offer better usability than the H-IBAS-H since, for one reason, a key input, in the password and PIN systems, is allowed to be used more than once when generating a key.

The knowledge that the key inputs cannot be repeated might have actually better helped the users to successfully register and, then, authenticate with an authentication system, such as H-IBAS-H. On the other hand, such knowledge could be a free give away to attackers. However, a success of 98.4% in the registration stage and, then, a success of 94.4% in the login stage with H-IBAS-H endorse that it is not necessary to allow a key input to appear more than once for image-based systems to enjoy a high percentage of success.

5.4.3. Findings

- It might be not necessary to allow repetition of key inputs when forming a key in image systems to achieve high success.
- The ban of repetition in key inputs might be in favour of success with image systems on both, the security and the usability sides.

5.5. Choice of key inputs in image-based systems

This section attempts to demonstrate the characteristics of the images favoured by users. It essentially answers the following questions; what are the popular images from a user point of view when registering with H-IBAS-H? Or, on what basis, have the users selected their images when registering?

5.5.1. Findings

By and large, a successful image-based authentication system should use images that are *made up of 1 or 2 colours, consisted of 1 or 2 shapes, different, unique, appealing and meaningful.* However, it may be not necessary for an image-based system to be successful to use images that are made up of 1 or 2 colours or images that are made up of 1 or 2 shapes. As long as there is sufficient distinction between the images, such that it can be said that the vast majority of the images offered are distinctive and unique, an image-based system can still enjoy a high degree of success.

An image-based system that uses 'too' similar or "too" abstract images is likely to fail from a usability point of view.

Moreover, there is adequate evidence that shows that users prefer photographic pictures, such as pictures of real objects, animals, famous people…etc. This supports the findings of Awase-E. In H-IBAS-H, such photographic pictures were ruled out on the basis that such images could provide clues as to which pass-images a user is more likely to select.

5.5.2. Image-based versus text-based authentication systems (in terms of favourable key inputs)

Meaningful and **appealing** key inputs are also keys to usability success on both kinds of the knowledge based systems; the recall-based one and the recognition-based one. In recall-based systems, users more than often choose passwords which are either of personal meanings to them, such as their love partners, or passwords that they understand what they mean. For example, the chances of choosing "love" as a password is, by far, more enormous than the choice of "segjfiqbweh" which does not mean anything. The same applies to image-based systems, the chances of choosing an image of Princess Diana as a pass-image is, considerably, greater than the choice of some random abstract meaningless image. Since only abstract images are allowed in random art, users still look for the most appealing ones, at least the most appealing to themselves!

5.6. Evaluation of the time consumption in H-IBAS-H

This section assesses the time taken when using H-IBAS-H as an authentication system. It investigates the issue by looking at the time taken while creating keys and the verification of every key input in the challenge-set.

5.6.1. Key Creation

Key creation in image-based systems takes no longer than the key creation in password systems. Actually, as the survey data show, it takes relatively less time than that taken for the choice of a new and a unique password.

5.6.1.1. Possible Reasons

Some users, in fact, commented that they always find it hard to come up with a new and unique password since they already have a number of different passwords for a number of different purposes that they are struggling to remember. Thus, according to them, it takes them quite a longer time to think of a new memorable password that they have not used before. Where there are plenty of keys already chosen by an individual, the individual's ability to come up with a new key becomes tougher and hence can take up long time. This is more of an issue to text-based systems rather than the image-based ones since the latter are by far less common than the former ones.

5.6.1.2. Findings

As far as the key selection, i.e. the image-set creation, is concerned, image-based systems are by no means more time-consuming than the password systems.

5.6.2. Verification of every key input in challenge-set

It may be not necessary for a user of an image-based authentication system to verify every key input of the offered key inputs in a particular challenge-set. Instead, a quick skim through might suffice to identify the real authentication key. Thus, the time spent to do such an operation is considerably less than the time that would have been spent on the verification of every image of the offered 21 * 4 images. Consequently, while password systems are, undoubtedly, faster since no such identification is required, the image-based systems can be reasonably fast, though not as fast as the password systems. Hence, the image-based systems still offer a reasonable degree of usability, in terms of speed.

5.7. H-IBAS-H versus PIN-based and password-based authentication systems (in terms of ease of use)

Overall, it can be stated that the majority of the surveyed ECE find image-based systems easy to use. This is despite the fact that the ECE, in the one-time experiment only, still believes that the password and the PIN systems are still easier to use than the image ones. The reasons for such a belief can be related to many factors such as:

1. All users are used to password and PIN systems and have had experiences with them for years while they only had a single experience with H-IBAS-H.
2. PIN and password systems are relatively faster according to users since they only involve 1 login round compared to 4 login rounds in H-IBAS-H.
3. With password and PIN systems, the users are only required to type in their user-name and their corresponding password all on one page, while in H-IBAS-H, the users are expected to identify their 4 images in 4 pages, each of which offers 21 images with no knowledge as of the number of their pass-images shown at each round and neither do they have any knowledge in regards to whether a particular login round contains any pass-images or not in the first place.

Despite all of this, the users still find H-IBAS-H easy to use and not only that but it can be CLEARLY stated that the users find the image-based authentication systems to be **the most fun to use** compared to the password-based systems and the PIN-based systems used at the ATM machine.

What is more appealing is that the one-time experiment results show that the ECE participants place a great amount of trust on H-IBAS-H. Most of the users have related this trust due to the technique used in the system and, astonishingly, to its complications. What can be learnt from this is that users are likely to place their trust on the more complicated systems!

5.8. Evaluation of the failure scenarios

This discusses the reasons that have led to the failure of some users to authenticate using H-IBAS-H. The survey data show that the following reasons were key figures to the failure.

5.8.1. Similarity between images

This has been discussed earlier.

5.8.2. Existence of too abstract images

Although abstract art is ideal from the point of view that it barely gives any clues about the users, the too abstract art can be an issue that might stand against the success of the image-based systems. Thus, only the 'too' abstract keys should be eliminated for the image-based systems to be highly successful! The high rate of success achieved by H-IBAS-H can be used as evidence that the 'abstract' random art could be finely used as keys in the recognition systems.

5.8.3. Level of uncertainty is high

To secure high success in image-based systems, the level of certainty provided should be carefully planned such that the information necessary to the completion of the registration and the authentication of the system is provided but in a way that does not compromise security.

6. The Four-Week Experiment

6.1. Authenticating with H-IBAS-H/the old account

Table 1 shows the percentage as well as the number of the participants who successfully managed to log in with the H-IBAS-H in week 1, week 2, week 3, and week 4.

Week	Successful logins (%)	Successful Participants	Total Participants
1	100%	20	20
2	80%	16	20

3	100%	16	16
4	93.8%	15	16

Table 1: Overall users' statistics in the four-week experiment

6.2. Authenticating with H-IBAS-H/the new account

Table 2 shows the percentage as well as the number of the participants who successfully managed to log in to their second account with H-IBAS-H in week 3 and week 4.

Week	Successful logins (%)	Successful Participants	Total Participants
3	100%	16	16
4	75%	12	16

Table 2: Overall users' statistics in the four-week experiment after creating a new account

6.3. Discussion

The fact that 75% of the participants were able to authenticate successfully to their new account in week 4 is surprising! What is even more astonishing is that , 93.8% of the participants were able to actually authenticate successfully to their old account in week 4, as shown in Table 2. The reason why this is shocking is because, initially, it was assumed that the success rate with H-IBAS-H would decline dramatically based on the assumption that most of the participants would get confused between their newer and the older pass-images. This assumption originated from the initial thought that the new images would be confused the old ones since the participants had gained more familiarity with the old pass-images as they had used to log in with them for 3 weeks. Yet, the vast majority of the participants managed to successfully distinguish between their images and used the right ones to log in to the right account.

The minimum interval of authentication was 7 days and this is probably less frequent than the use of an ATM in participants' daily lives. It is, also, by far less frequent than the use of the traditional passwords' systems to authenticate to the participants' portals. What can be learnt from this is that authentication stability can be provided even where the image-based authentication system is not frequently used! This finding supports what the Awase-E developers also found [8, 11]. Since image-based keys may be still recognised and distinguished over longer periods of times, image-based authentication systems might represent valid and effective solutions for some infrequently used websites that require authentication. Equally well, they can be applied to any organisation that needs to authenticate its irregularly-visiting clients.

6.4. Findings

- Authentication stability can be provided even where the image-based authentication system is not frequently used!
- Image-based authentication systems may be effective on both the longer and the shorter terms.
- Users may effectively use different image-keys for different purposes.
- Random art keys may be efficient for use by the image-based authentication systems on both the longer and the shorter terms.

6.5. Image-based systems versus text-based systems (in terms of authentication stability)

Previous research data, as in the Déjà Vu and Awase-E data, showed that the text-based authentication systems performed poorly in situations where the password or the PIN was not often used. Thus, based on the outcomes of the four-week experiment conducted by H-IBAS-H, it can be concluded that image-based systems might provide better authentication stability than the text-based systems in situations where the authentication system is infrequently used.

6.6. Time consumption and ease of use

In short, the four-week experiment has shown that the more experiences that the users have with an image-based system, the faster and the easier they think it becomes for them. In fact, the participants in the four-week experiment have gone as far as rating H-IBAS-H to be faster and easier than the text-based authentications systems used for the University portal and the ATM machines. This clearly brings fine news for the usability of the image-based authentication systems and, hence, it pushes such systems forward.

6.7. Flexible mode

The participants found the flexible mode in H-IBAS-H easy and fun to use, and less time-consuming than other text-based authentication systems. Thus, this meets one of the objectives of H-IBAS-H which is to design an authentication system that is fun and easy to use!

7. RECALL OR RECOGNITION?

7.1. Observation

On selection of their pass-images, most of the participants tend to relate their images to some real-world objects. For example, one 'male' student stated that he selected his 4 pass-images based on the following; 1- One appears as a highway when you look at it from a faraway distance.2- One looks like a piece of marble. 3- One looks like a curtain.4- One looks like a human female breast. At the time the student was selecting his pass-images, he had no view whatsoever to a highway, or to a female breast. Thus, he had to recall how they look like from the top of his head. The student was asked to log in to their account on week 1, week 2, week 3 and week 4. Before he logged into his account, the student was asked to talk about his pass-images. He actually described them all as above. He stated that he had all his pass-images in mind. As he was performing his first login round, the student skimmed through the challenge-set to look for an image or images that look(s) like a highway, or a piece of marble, or a curtain or a female breast. As soon as the student found one of them, he 'recognised' that it was his pass-image, thus he selected it. He used a similar technique in the subsequent login rounds. This was just a single observation of one student. Many students, in fact the majority of the students, used similar techniques. Certainly, there is no need for a user to precisely and exactly remember how their image looks like before they log in. For example, before they perform their recognition, a user could say 'I know that my image looks like an eye but I am not sure about its background colour'. When the user is offered the 'challenge-set', and once their eyes glance over the challenge- set, they would immediately recognise their pass-image. H-IBAS-H facilitated this since most, if not all, of the similar images have been manually removed!

7.2. Findings

The observation above suggests that the image-based systems that use random art as their authentication keys depend on both, recognition and recall;

• They depend on recognition in terms that they show the 'decoy' and the 'pass-images' on a challenge-set, and the user is required to identify the correct pass-images as soon as they recognise them from the decoy images.

• And they depend on recall in terms that the users recall their pass-images before and while they perform their authentication. Here, the users actually 'remember' how their pass-images look like, though not precisely, and then when the system offers them the challenge-set, they 'recognise' them. Therefore, in image-based systems, in particular, the ones that apply random art, the separation between 'recall' and 'recognition' is not a wise one and neither is it an easy one, as most of the users of these systems depend on both, the recall and the recognition when authenticating with such systems.

7.3. Image-based versus text-based systems (in terms of precise and partial recall)

While text systems entirely depend on the recall, the image-based systems depend on the recognition and the recall. Since the latter ones depend on two senses, this may be the reason behind the high success of image-systems compared to the recall systems.

Another distinction between the text-based systems and the image-based systems is that the text systems depend wholly on the 'precise' recall of the key, i.e. almost or partial recall is not sufficient. A 'partial' recall of the key might, however, suffice to successfully authenticate in image-based systems since while they mainly depend on 'recognition', they also depend on recall. Elimination of the similar images makes the image-based systems that depend on recall and recognition powerful systems, i.e. more usable and hence more popular.

8. Frequency of Key Updates

The frequency of key updates can influence the security of any authentication system. Where users are more enthusiastic to update their keys, as in Awase-E, the security level is likely to escalate. On the contrary, where users are less keen to update their keys, as in H-IBAS-H, the security level could decline. As the survey data imply, the reason why users are less enthusiastic to switch their keys in H-IBAS-H is because they find the random art keys hard to remember since they are abstract and random. If users are allowed to use their own keys in image-based authentication systems, the frequency of key updates in such systems is likely to be higher than that of other authentication systems. Therefore, the usability and the security might be better in such image systems. However, the employment of users' own keys could, on the other hand, trigger another security problem where the users' keys can be attacked by educated guesses based on the knowledge of users' personal tastes.

9. Conclusion

H-IBAS-H demonstrated how image-based systems could be effectively used in the process of authentication of a particular purpose. In addition to the technical achievement accomplished by the successful implementation of the system within the scheduled time, the analysis operation conducted on the data collected from a hundred and ninety surveys from real users has afforded valuable contribution to the research society, specifically to the authentication field. In addition, it has also provided a precious insight that offers the potential for considerable future work.

A functional system has been developed which allows users to authenticate using image keys in two modes, a flexible mode and a pre-set mode. Where users can select the number of pass-images and the number of login rounds that they desire in the flexible mode, the system administrator can force the users to select a certain number of pass-images and go through a certain number of training and login rounds in the pre-set mode.

The high rate of success, achieved by users attempting to authenticate, strongly supports the arguments of those seeking to push image recognition forward as a viable alternative to the widely-used text-based systems. H-IBAS-H suggests that the flexibility in key generation as well as the elimination of similarity between key inputs are two key players that need to be supplied in order to secure a high success in an image-based authentication system.

H-IBAS-H has proven that the image-based authentication systems, even the ones that use random art keys, can provide stability in authentication even where the frequency of use of the authentication system is as low as once a week.

Perhaps the most important finding of all in this project is that H-IBAS-H discovers that users depend on both recognition and recall when using image-based authentication systems. H-IBAS-H explains that where text-based authentication systems rely entirely on the 'precise' recall of the password or of the PIN to achieve a successful authentication, image-based authentication systems, in particular the ones that use random art keys, rely on both recognition and recall, but here a 'partial' recall might suffice to accomplish success when authenticating. One significance of this finding is the fact that at the start of this project, and based on the background research conducted, the H-IBAS-H developer thought that the image-based authentication systems rely solely on recognition.

Acknowledgment

The authors wish to thank the Diwan of Royal Court of the Sultanate of Oman (ديوان البلاط السلطاني العماني) for their continues care and for their unlimited support to this Paper and its authors.

References

[1] Authorization, Authentication, and Access control. Retrieved February, 2008, from: http://httpd.apache.org/docs/1.3/howto/auth.html#intro

[2] Authentication . research is sponsored by the Defense Advanced Research Projects Agency and managed by the U.S. Army Research Laboratory under contract DAAL01-95-C-0112. Retrieved February, 2008, from: http://www.objs.com/survey/authent.htm

[3] A definition from whatis.com. Retrieved February, 2008, from, http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci211621,00.html

[4] Srinath Akula, Veerabhadram Devisetty "Image Based Registration and Authentication System", IBRAS, Department of Computer Science St cloud State University, St. Cloud, MN 56301. Retrieved in March 2008.

[5] Chi Nguyen, University of Portsmouth, ECE, Tutorial notes for M591, "Concepts of identity and privacy" Retrieved January, 2008, from: http://cnfolio.com/AuthenticationTechTutorial02

[6] Rachna Dhamija, Adrian Perrig, "D´ej`a Vu: A User Study Using Images for Authentication", SIMS / CS, University of California Berkeley. Retrieved February, 2008, from: http://people.ischool.berkeley.edu/~rachna/papers/usenix.pdf

[7] Mark Blay, "Authentication System using Image-Based Keys" Final-year Project Report supervised by the lecturer Chi Nguyen. ECE, University of Portsmouth, Academic Year of 2006/07.Retrieved in November 2007.

[8] Tetsuji TAKADA 1and Hideki KOIKE2, 1SONY Computer Science Laboratories,2Graduate School of Information Systems, University of Electro-Communications "Awase-E: Image-based Authentication for Mobile Phones using User's Favorite Images". Retrieved March, 2008, from http://www.netaro.info/~zetaka/publications/papers/awasee-MobileHCI03.pdf

[9] Richard E. Newman, Piyush Harsh, and Prashant Jayaraman, CISE Dept., University of Florida, Gainesville FL 32611-6120, "SECURITY ANALYSIS OF AND PROPOSAL FOR IMAGE-BASED AUTHENTICATION". Retrieved March, 2008, from: http://www.cise.ufl.edu/~nemo/papers/Carnahan2005.pdf

[10] Art Conklin, Glenn Dietrich, Diane Walz, "Password-Based Authentication: A System Perspective", Proceedings of the 37th Hawaii International Conference on System Sciences – 2004. Retrieved in February 2008.

[11] Hideki Koike†, Tetsuji Takada‡, Takehito Onuki†, ‡Information Technology Research Institute, National Institute of Advanced Industrial Science and Technology, "AwaseE:PhotobasedUserAuthenticationSystem"RetrievedFebruary,2008,from:http://www.netaro.info/~zetaka/publications/papers/awasee-UBICOMP2005.pdf

[12] WordNet Search - 3.0, a lexical database for the English language. WordNet 3.0 © Princeton University 2006. Retrieved April, 2008, from: wordnet.princeton.edu/perl/webwn

[13] Iarossi, Giuseppe. Power of Survey Design : A User's Guide for Managing Surveys, Interpreting Results, and Influencing Respondents. Herndon, VA, USA: World Bank, The, 2006. p 99. Retrieved April, 2008, from: http://site.ebrary.com/lib/portsmouth/Doc?id=10106731&ppg=117

[14] Sampling (Statistics) – Wikipedia, the free encyclopaedia. Retrieved April, 2008, from: http://en.wikipedia.org/wiki/Sampling_(statistics)#Stratified_sampling

[15] ASCII 256 DOS Characters. Retrieved May, 2008, from: http://www.flexcomm.com/library/ASCII256.htm

[16] FAO Corporate Document Repository, Glossary, retrieved April, 2008, from: http://www.fao.org/DOCREP/006/Y4851E/y4851e0f.htm