Mathematical and Computer Modelling 58 (2013) 108–116

Contents lists available at SciVerse ScienceDirect

Mathematical and Computer Modelling

journal homepage: www.elsevier.com/locate/mcm

A novel image-based implicit password authentication system (IPAS) for mobile and non-mobile devices

Sadiq Almuairfi, Prakash Veeraraghavan, Naveen Chilamkurti *

Department of Computer Science and Computer Engineering, La Trobe University, 3086, Melbourne, Australia

ARTICLE INFO

Article history:
Received 29 June 2011
Received in revised form 21 February 2012
Accepted 7 July 2012

Keywords:
Authentication
Graphical password
Security
Mobile banking

ABSTRACT

Authentication is the first line of defense against compromising confidentiality and integrity. Though traditional login/password-based schemes are easy to implement, they have been subjected to several attacks. As an alternative, token and biometric-based authentication systems were introduced. However, they have not improved substantially to justify the investment. Thus, a variation to the login/password scheme, viz. graphical scheme was introduced. But it also suffered due to shoulder-surfing and screen-dump attacks. In this paper, we introduce a framework of our proposed (IPAS) Implicit Password Authentication System, which is immune to the common attacks suffered by other authentication schemes.

1. Introduction

Authentication is a process of determining whether a particular individual or a device should be allowed to access a system or an application or merely an object running in a device. This is an important process which assures the basic security goals, viz. *confidentiality and integrity.* Also, adequate authentication is the first line of defense for protecting any resource. It is important that the same authentication technique may not be used in every scenario. For example, a less sophisticated approach may be used for accessing a "*chat server*" compared to accessing a *corporate database.* Most of the existing authentication schemes require processing both at the client and the server end. Thus, the acceptability of any authentication scheme greatly depends on its robustness against attacks as well as its resource requirement both at the client and at the server end. The resource requirement has become a major factor due to the proliferation of mobile and hand-held devices. Nowadays with the use of mobile phones, users can access any information, including banking and corporate databases. In this paper, we specifically target the mobile banking domain and propose a new and intelligent authentication scheme. However, our proposal can also be used in other domains where confidentiality and integrity are the major security requirements.

The rest of the paper is organized as follows: Section 2 deals with various authentication schemes, and their advantages and disadvantages. In Section 3, we present our proposal and discuss its strengths and weaknesses compared with the existing schemes. Section 4 deals with conclusion and future directions.

2. Various authentication schemes

There are several authentication schemes available in the literature. They can be broadly classified as follows:

- What you know
- What you have and
- What you are.

* Corresponding author.
E-mail addresses: sadiqjafar@students.latrobe.edu.au (S. Almuairfi), p.veera@latrobe.edu.au (P. Veeraraghavan), n.chilamkurti@latrobe.edu.au (N. Chilamkurti).

0895-7177/$ – see front matter
doi:10.1016/j.mcm.2012.07.005

The traditional *username/password* or *PIN*-based authentication scheme is an example of the "what you know type". Smartcards or electronic tokens are examples of "what you have type of authentication" and finally biometric-based authentication schemes are examples of the "what you are" type of authentication. Some authentication systems may use a combination of the above schemes. In this paper, we focus only on "what you know" types of authentication.

Although traditional alphanumeric passwords are used widely, they have problems such as being hard to remember, vulnerable to guessing, dictionary attack, key-logger, 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 sticky residue left by finger on the devices), which reduces the security and usability levels. Thus, recent developments have attempted to overcome biometric shortcomings by introducing *token-based* authentication schemes.

Token-based systems rely on the use of a physical device such as smartcards or electronic key for authentication purpose. This may also be used in conjunction with the traditional password-based system. Token-based systems are vulnerable to man-in-the middle attacks where an intruder intercepts the user's session and records the credentials by acting as a proxy between the user and the authentication device without the knowledge of the user [3]. Thus as an alternative, *graphical-based passwords* are introduced to resolve security and usability limitations mentioned in the above schemes.

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 [4]. Psychologists have confirmed that in both recognition and recall scenarios, images are more memorable than text [2]. Therefore, graphical-based authentication schemes have higher usability than other authentication techniques. On the other hand, it is also difficult to break graphical passwords using normal attacks such as dictionary attack, brute force and spyware, which have been affecting text-based and token-based authentication [5]. Thus, the security level of graphical-based authentication schemes is higher than other authentication techniques.

In general, the graphical password techniques can be classified into two categories: recognition-based and recall-based graphical techniques [4].

2.1. Recognition-based systems

In recognition-based systems, a group of images are displayed to the user and an accepted authentication requires a correct image being clicked or touched in a particular order. Some examples of recognition-based system are Awase-E system [6], AuthentiGraph [3,5], and Passfaces system [4].

An image password called Awase-E [6] is a new system which enables users to use their favorite image instead of a text password for authentication purpose. Even though Awase-E system has a higher usability, it is difficult to implement due to the storage space needed for images and also the system cannot tolerate replay attack. Adding to this, a user may always tend to choose a well-known (or associated with the user through some relation, like son, wife or a place visited etc.) image which may be prone to guessing attacks.

Weinshall and Kirkpatrick [7] studied a recognition-based scheme and concluded that users can still remember their graphical password with 90% accuracy even after one or two months. Their study supports the theory that human remember images better than text. In addition for example, the commercial system Passfaces [4] uses images of human faces. Davis, et al. [7] worked on such A scheme and concluded that user's password selection is affected by race and gender. This makes the Passfaces's password somewhat predictable.

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 [7]. 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 proposed system, which overcomes the problems of recall-based schemes too.

2.2. Recall-based systems

In recall-based systems, the user is asked to reproduce something that he/she created or selected earlier during the registration phase. Recall-based schemes can be broadly classified into two groups, viz: *pure recall-based technique* and*cued recall-based technique*.

2.2.1. Pure recall-based technique

In this group, users need to reproduce their passwords without any help or reminder by the system. Draw-A-Secret technique [8], Grid selection [9], and Passdoodle [10] are common examples of pure recall-based techniques.

In 1999, Jermyn et al. [8] proposed DAS (Draw-A-Secret) scheme, in which the password is a shape drawn on a two-dimensional grid of size G * G as in Fig. 1. Each cell in this grid is represented by distinct rectangular coordinates (x, y).

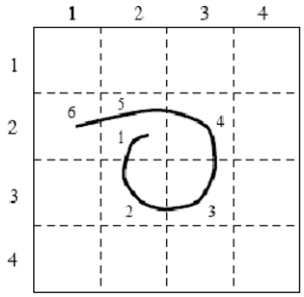

Fig. 1. Draw a secret on a $4 * 4$ grid.

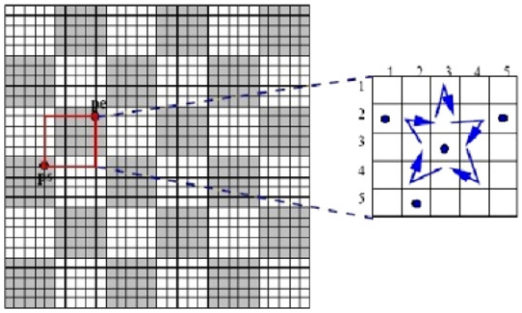

Fig. 2. Grid selection method.

Fig. 3. An example of a Passdoodle.

The values of touch grids are stored in temporal order of the drawing. If exact coordinates are crossed with the same registered sequence, then the user is authenticated. As with other pure recall-based techniques, DAS has many drawbacks. In 2002, Goldberg [11] conducted a survey which concluded that most users forget their stroke order and they can remember text passwords easier than DAS. Also, the password chosen by users are vulnerable to graphical dictionary attacks and replay attack.

In 2004, the Grid selection technique was proposed by Thorpe and Van Oorschot [9] to enhance the password space of DAS. Their study showed the impact of stroke-count on DAS password space which decreases significantly with less strokes for a fixed password length. To improve the DAS security level, they suggested the "Grid Selection" technique, where the selection grid is large at the beginning, A fine grained grid from which the person selects a drawing grid, a rectangular area to zoom in on, in which they may enter their password as shown in Fig. 2. This technique would increase the password space of DAS, which improves the security level at the same time. Actually, this technique only improves the password space of DAS but still carries over DAS weaknesses and drawbacks as mentioned above.

Passdoodle [11], is a graphical password of handwritten drawing or text, normally sketched with a stylus over a touch sensitive screen, as shown in Fig. 3. In [11], Goldberg et al. have shown that users were able to recognize a complete doodle password as accurately as text-based passwords. Unfortunately, the Passdoodle scheme has many drawbacks. As mentioned in [9], users were fascinated by other users' drawn doodles, and usually entered other users' password merely to a different doodles from their own. In [1], the authors concluded that the Passdoodle scheme is vulnerable to several attacks, such as guessing, spyware, key-logger, and shoulder-surfing.

2.2.2. Cued recall-based technique

In this technique, the system gives some hints which help users to reproduce their passwords with high accuracy. These hints will be presented as hot spots (regions) within an image. The user has to choose some of these regions to register as 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 Blonder algorithm [12] and PassPoint scheme [13].

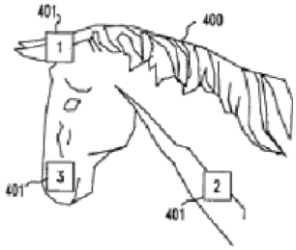

Fig. 4. Example of Blonder scheme.

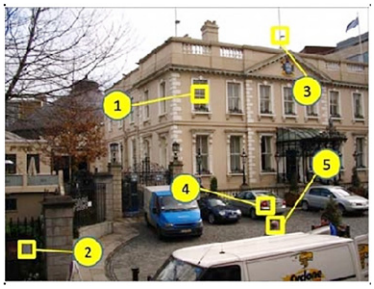

Fig. 5. Example of a PassPoint system.

In 1996, Blonder [12] designed a method where a pre-determined image is shown to the user on a visual display and the user should "click" on some predefined positions on the image in a particular order to be authenticated as in Fig. 4. This method was later modified and presented as PassPoint [13].

In 2005, the PassPoint [13] scheme was created to be similar to the Blonder's scheme while overcoming some of its main limitations. In PassPoint, the image can be an arbitrary photograph or paintings with many clickable regions, as shown in Fig. 5. This will increase the password space of the PassPoint scheme, which in turn will increase the security level. Another source of difference is that there is no predefined click area with clear boundaries like the Blonder algorithm. The user password could contain any chosen sequence of points in the image, which increases the usability level of this scheme.

The PassPoint system has a large password space, which improves the security level compared with other similar systems. For example, five or six click points on an image can produce more passwords than 8-character text-based passwords with standard 26-character alphabet [13]. For more security, the PassPoint system stores the image password in a hashed (encrypted) form in the password file. Moreover, hashing does not allow approximation, e.g. two passwords that are almost the same but not fully identical will be hashed differently. In order to be authenticated, the user has to click close to the selected points, within some measured tolerance distance from the pass point.

Wiedenbeck et al. [14] proposed the best tolerance around the click point in such an image. To log in, the user should click with the tolerance of such a click point. In fact, a larger password space leads to a smaller tolerance size, e.g. 2 to 5 mm around the chosen click point or pixel. For example, an image of size 330×260 mm^2 with tolerance areas of size 6×6 mm^2 gives more than 590 tolerance areas [14]. It is clear that password space depends on the tolerance size or system choice. This enhancement makes the PassPoint system more flexible, especially for people using mobile devices.

2.3. Problems with the existing schemes

Traditional alphanumeric passwords are always vulnerable to guessing and dictionary attack. There may even be a rogue program that may record the key strokes and publish it on a remote website. In order to overcome the key logger-based attacks, newer systems may show a graphical keyboard and the user has to press the correct password using "mouse clicks". This may also be defeated if the attacker uses a screen capture mechanism, rather than using a key logger. Since new video codecs are providing higher compression ratio, an attacker may use a screen capture program and record a short video clip and send it to a remote server for publishing. So, as an alternative, a token-based authentication method may be used either as a stand-alone authentication or used in addition to the traditional alphanumeric password. But this technology is not pervasive. The user may have to carry a trusted token card reader. With unknown token readers, a user may not be aware whether they are using a trusted legitimate reader or using an untrusted one that may clone the token (similar to the recent ATM card scam).

Although image-based authentication systems reviewed in our paper address most of the threats, still they suffer from the following attacks: replay, shoulder-surfing, and recording the screen.

One may argue that replay attack can be prevented using encryption and tamper-proof time stamps, and physical shoulder-surfing may be known to the user as this process is invasive. However, due to the availability of high-bandwidth

to mobile devices and light-weight, high-efficient video codecs, a rogue program may still capture and publish remotely. Since all the image-based password schemes known to us use static passwords, the recorded movie may be replayed and with some human-interaction, the user's password may be decoded.

In this paper, we provide a theoretical and implementation framework of our proposed Intelligent Password Authentication Scheme (IPAS) to address the issues of security problem existing in the present image-based authentication schemes. We also compare our proposal with other successful authentication schemes to show the strength of our proposal. It can be seen from our proposal that the proposed algorithm can be easily implemented without any extra hardware and software requirements. However, our proposed method may require more bandwidth compared to the existing authentication schemes. This is not a major problem, as more bandwidth is readily available to mobile devices. The section on future directions narrates how we plan to proceed in making our proposal operational.

3. Implicit password authentication system

In this section, we propose our Implicit Password Authentication System (IPAS). IPAS is similar to the PassPoint scheme with some finer differences. In every "what you know type" authentication scheme we are aware of, the server requests the user to reproduce the fact given to the server at the time of registration. This is also true in graphical passwords such as PassPoint. In IPAS, we consider the password as a piece of information known to the server at the time of registration and at the time of authentication, the user give this information in an *implicit* form that can be understood only by the server. We also provide the implementation framework which is divided into phases as described in Section 3.1.

Our proposed (IPAS) may also be implemented in any client–server environment, where we need to authenticate a human as a client (IPAS will not work in machine-to-machine authentication). We also assume that the server has enough hardware resources, such as RAM and CPU. This is not unrealistic as high-end servers are becoming cheaper day-by-day.

We now provide a brief overview of the proposed scheme:

During the registration process, a user will provide personal information to the server. The system (or the administrator) will extract *keywords* based on the provided information. The server may have several images and each image may have more than one clickable area (like the PassPoint). Each clickable area may represent an object and have several text attributes associated with it. For example, a book object in an image may have text attributes such as *book, reading, colour* of the book etc.

During the authentication phase, the server may pick a random keyword related to the user and pick a random image that has the text attribute associated with an object and send to the user. The user has to click the right object that represents the expected keyword. Unlike PassPoint, our system will choose different images every time.

To make our system more flexible, if a user is unable to work through the image map, he/she may switch to a text-based system. Here, the expected keywords are the response to challenges sent by the server. However, this may suffer from shoulder-surfing. It is up to the implementer to allow this feature or not.

We now provide a detailed implementation framework.

3.1. Implementation framework

The framework process will involve four models that comprise of design, system development, user acceptance testing and the production roll out. The authentication system usually has both a client and server component. Each component provides implementation of a standard interface function and an initialization function that will register the module with the system. In fact, the client–server model is a more scalable approach to client authentication than other models. Thus, design model of IPAS is a client–server model where both ends must be trusted. Any client is authenticated when connected to the server, and trusted afterwards. The authenticated user actions are checked against a specific access control policy that controls which actions are allowed or denied for that user.

The design model

A client device could be any portable device such as laptop or mobile phone. Mobile phones are becoming increasingly important for our daily life. One main reason is that more and more functions have been integrated within mobile phones, such as Internet browsing, mobile banking, and shopping. Some of the latest smart phones match the performance of high-end desktop PCs a decade ago. People are now paying much more attention to their mobile phones than they did before, which makes mobile phones relatively hard to lose compared with devices that users do not tend to care very much, such as USB flash drives. However, having such an advantage on security is not enough to prove that mobile phones are more suitable for online banking authentication than USB drives. Therefore, an in-depth inspection on mobile phone malware and application are desirable. IPAS has considered this issue by allowing users to access their accounts on the move with a high level of security and usability. Our system does not require any high-end specialized software. The presence of a standard web browser with Internet connection is enough to launch our application. Thus our system may very well scale from a smart phone to desktop PCs.

On the other side, the server is the other entity of our design model in IPAS. However, we assume that the communication between client and server is secure and trusted through protocols such as SSL and IPSec against malicious intermediate nodes caching and making off-line guess. This only adds an extra-layer of protection. However, our authentication process

may still work without this assumption. The server(s) which is located at an organization side such as bank should be equipped with appropriate safety measures such as firewalls, intrusion detection systems and rapid recovery mechanisms to guarantee information security. The authentication server, which is one of the most important servers in our design model, should contain an *Intelligent Graphical (IG)* module to covert user information/answer into an image. This image, which implicitly represents the user password, will be pushed to the client device during authentication process. The user will be authenticated only if he/she clicks on the right objects in the image that match the stored information. Moreover, a trusted link between the authentication server and main image database server should take place for the access control purposes of such authentication level.

System development model:

Image database:

The image database at the server side is the heart of our authentication scheme. Depending upon the number of users, the image database may contain tens of thousands to millions of images. The system administrator may add more images on a regular basis. Each image may have more than one "clickable" object. One or more text keywords are associated with each clickable object. The relation between the image objects and associated texts play a significant role in our authentication scheme, which is described later in this subsection.

User registration phase:

In this phase, the user's initial information will be collected to enable him/her to use the system. During the time of registration (either online or off-line), a set of different areas will be provided to the user. For example, the areas may include *childhood memories, current hobbies, dream holidays* etc. The user may have to choose m out of n areas (where m and n are the system parameter decided by the domain people).

For each chosen area, the user may have to provide a *phrase* with sufficient information (again, this is application and domain dependant). If there is insufficient information, the system will prompt the user again to input more information. The phrases provided by the user create a personalized information space for the user (similar to the static password).

We now demonstrate this feature through an example. Here, the user describes her childhood experience.

"*When I think about it I had a real good child hood. Believed in the things some kids suppose to believe in like Santa Clause and the tooth fairy which made it exciting. Always had a good Christmas with toys laid out like Santa had been there and when I lost a tooth when I put it under my pillow would get money for it. I enjoyed playing child hood games, playing with my cousin and the other kids. I was crazy about Barbie dolls and had a lot of them and Barbie houses. I had a bike and a scooter. I had the love and care of my family and knew it. I loved jumping on our trampoline and playing outside. Well, life was great back then when i was a kid! I could look any way I wanted to and had no real worries. I didn't have it hard i had it good and easy. I hate ghosts and scary stories. I was always afraid of dark places and being alone*".

Based on the given phrase, the system will extract *keywords and information* from every possible sentences (for a much simpler implementation, the system manager may extract the keywords from the given phrase). The following are the possible keywords and information:

- Santa
- Tooth fairy
- Jumping on *trampoline*
- hate *ghosts* and *scary* stories
- Afraid of *dark places* and *being alone.*
- Crazy about *Barbie dolls.* Had *Barbie houses.*
- Love to *play* with cousin and friends.

Based on this information, the system may either create or link with the existing image database. The keywords and the information will be embedded in an image and implicitly presented to the user during the authentication process. The user has to click the right object to represent his/her answer. In fact, this information is easy to remember than complex passwords.

Segmentation phase:

In this phase, the system will work on creating a visualized image of a user's logged answers (keywords) which lead to an interface behavior. The tool used in visualization is geared towards improving the system design so that the technique realized within the system development is perfectly segmented. The registered users can be categorized, in relation to their interaction behavior, into two domains: Region/State domain and word space/distance domain.

Various kinds of user in a system can at times have a different perspective of their needs. For instance, the perception while one is in America may not be the same as someone who is in Australia [15]. Therefore, the system will consider the area/region which the user belongs to when creating the user password and link his/her 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 *Sydney Opera House*, whereas users from Europe may easily recognize "*London Coliseum Theatre*" rather than Sydney Opera house (some may not even recognize it). Thus, the system under this domain will be country/region dependent, which should be considered during the production roll-out module.

Secondly, the domain will rely on taxonomy of relationship between images and words that can be used for analyzing the way that images and text interact. Merch et al. [16] mentioned that the taxonomy identifies 49 functions that the image plays in relationship to the relevant text. Therefore, word space/distance domain can apply some of these functions according to the required security level.

As in [16], the image relationships functions are categorized into three sets: (A) functions expressing far/long relation to the text; (B) functions expressing a close relation to the text (C) functions going beyond the text. Applying these sets would identify the level of relevance for each image in this domain. For example, let the chosen keyword be an Apple. Then the image which contains an "Apple Pie" will represent a closer relation to the word "Apple", while the image which contains "Albert Einstein" will represent a far distance relation to the word "Apple". The semantic variants of this concept can be developed quickly and with little effort by the system developer. It is true, therefore, to state that implementing a new segment of technology will take specialized skills and time, as well as many resources that many organizations will need to take into consideration.

Database and image characteristics

A user profile which contains personal information, account data, access control levels, and authentication questions and answers will be linked to the intelligent image server. Each authentication image may contain one or more "clickable objects" that represent the user keyword(s) or information. For example, a "trampoline" represents one of the keywords on which the user loved to jump on. For some other user, it represents a game he/she *hates* most; it may represent a *black colour;* it may represent *gymnastics etc*. Thus an image may have the following characteristics:

- An image may contain one or more objects
- Each clickable area may have different keywords associated with it.
- Each object represents one answer at a time implicitly
- An object is clickable once
- There may some decoy objects within the image to increase the security level.
- Each keyword will be presented by different objects every time.

The system picks an image in such a way that the "expected" keyword is exclusive to the presented image. For example, if the expected answer is "trampoline" and the image contains both a trampoline and a "Barbie" doll, then there is a conflict. To avoid this conflict, the system may choose an image that has only one of the expected keywords or will make the area that represents "Barbie" as "Non-clickable".

In addition, user can request another image in case he/she could not go through the present image or switch to text/token-based at anytime. Thus, IPAS provides a flexible authentication environment which increases the user friendly usage with a high level of security.

The authentication process:

First, a user may request access to the system by presenting his *user name* and the level of access required. This may be sent as a plain text. Depending on the level of access required, the system might request k out of m areas chosen by the user during the time of registration process. For each chosen area, the server may pick a random keyword extracted from the user phrase. For each keyword, the server may again pick a random image from the image database that contains an object which has the chosen text attribute.

Similar to Kerberos, a session key $S(Q_i)$ is derived from the correct clickable area through a function $f(I)$. The server will choose a random number p and then encrypt p with the session key $S(Q_i)$ and transmit $\langle \text{Image}, S(Q_i)[\text{p}], f(I)\rangle$ to the mobile device. The client application then displays the image. Using the stylus or a mouse, the user needs to choose the correct "clickable area". Then, based on the function $f(I)$, the image I and the area the user clicked, the client will then generate a key K. The function $f(I)$ is chosen in such a way that $S(Q_i) = K$ if and only if the user and the server has exactly the same area of interest in the image. The user then decrypts $S(Q_i)[\text{p}]$ to get the random number. He then transmits $p + 1$ to the server for authentication and to the next level. In this way, the user is authenticated implicitly and no confidential information is exchanged over the network. When the server is executing the last question in the authentication process, instead of encrypting a pseudo random number, it will pick a session key and encrypt with the derived key. When the client decrypts it, he gets an implicit message from the server to use this session key for transmission. This procedure not only authenticates a user implicitly, this will also exchange a session key implicitly.

It is up to the application developer and the organization to decide on what to do when a user gives an incorrect answer to one or more of the questions.

IPAS components:

Most of current schemes have to authenticate a user with a static process such as a password or token, while IPAS flexibility gives the user space and choices to be authenticated depending on the access level needed for such an operation. Thus, the user can switch from image-based to text-based at any time using same information as below:

Intelligent image-based authentication option

Image-based is the main component of IPAS, where user's answers are represented implicitly in an image during the authentication process. The system will choose the implicit level of the image depending on the requested access level, as described above in segmentation phase. Therefore, the user needs to click on the correct objects within the image, which

represent his/her answers to be authenticated. Then, the access control module will allow the user to perform the required operations and actions.

Due to the dynamic and high flexibility of IPAS, the user can switch to the text-based way at any time in case he/she cannot go through an image based way.

Intelligent text-based authentication option

In the text-based method, the user will be allowed to type his/her answers by using the keyboard. These answers (keywords) will represent the implicit objects in the given image. For example, user can type "apple" or "pillow" if the image contains an implicit object of apple or pillow. The user will be authenticated only if he/she types the correct answers of the given implicit image's objects. Then, the access control module will control the needed actions.

Similar to text-based method, the user can switch to the token-based "something you have" type of password, especially in a numeric password. Therefore, if the user cannot go through an image-based method for some reason, he/she can switch to the token-based way at any time. For example, a one time password (OTP) token, which is provided by some banks, could be used for the numerical password in the case where the user cannot figure out the numbers in an implicit image-based method.

For authentication purposes, it is desirable to rely on information the user already knows, rather than requiring him/her to memorize further information. In general, the system or registrar that collects user information should be aware of user privacy principles. Thus, the privacy, security, and usability of IPAS are major concerns.

Criteria for IPAS evaluation:

As an aid of both design and evaluation of IPAS, privacy, security, and usability criteria are considered.

Privacy: in environments that use personal information, it should be common practice to follow recognized privacy principles. For example, collected personal user information should be used only for authentication process. In addition, the answer of such a question should allow the user to access a particular level of his or her account.

Security: Generally, the security of IPAS is concerned with protecting the user's account information and financial records. On other hand, comparing IPAS with other authentication schemes, in the case of password space, would show the strength of IPAS as a security criteria. Also, the difficulty of a formal attack to break IPAS would improve the security level among other schemes.

Usability: IPAS usability is concerned with providing a user-friendly experience in the stages of answering personally related questions which are picked from the user's previous memorable stories. In fact, a password as information could provide an easy way for the user to remember his/her password during the authentication process. Moreover, IPAS is not used as a replacement of regular authentication in some cases, but rather, as an add-on factor. Thus, user is allowed to switch back at anytime to a normal authentication process such as a regular user name and password.

Strength of IPAS:

As one can easily see, IPAS is immune to shoulder-surfing and screen-dump attacks. Also, the authentication information is presented to the user in an implicit form that can be understood and decoded only by the legitimate end-user. Traditional password-based authentication schemes and PassPoint are special cases of IPAS. The strength of IPAS depends greatly on how effectively the authentication information is embedded implicitly in an image, and it should be easy to decrypt for a legitimate user and highly fuzzy for a non-legitimate user.

One of the weaknesses of implementing this scheme is that the system may simply ask the user an alphanumeric question given during registration process and ask the user to input the answer through a graphical keyboard.

4. Conclusion and future direction

In this paper, we have proposed a new Implicit Password Authentication System where the authentication information is implicitly presented to the user. If the user "clicks" the same grid-of-interest compared with the server, the user is implicitly authenticated. No password information is exchanged between the client and the server in IPAS. Since the authentication information is conveyed implicitly, IPAS can tolerate shoulder-surfing and screen-dump attack, which none of the existing schemes can tolerate. The strength of IPAS lies in creating a good authentication space with a sufficiently large collection of images to avoid short repeating cycles. Compared to other methods reviewed in our paper, IPAS may require human interaction and careful selection of images and "clickable" regions. IPAS may also need user training. Once this is done, IPAS can be more robust.

This paper represent the second phase of the IPAS project. In our subsequent paper, we will present the next phase, which is the user acceptance testing phase, where we will do a lab experiment with participants and volunteers. Statistical data such as time, security level, and user ability to remember his/her password over time intervals will be some of the outputs of the experiment. Therefore, our future paper will provide a real compromise between IPAS and other authentication schemes. The last phase of the IPAS project will be the production roll out phase, which will be real-life implementation within an organization, such as a financial institute.

References

[1] A.P. Sabzevar, A. Stavrou, Universal Multi-factor authentication using graphical passwords, in: IEEE International Conference on Signal Image Technology and Internet Based Systems, 2008, SITIS '08, Nov. 30 2008–Dec. 3 2008, pp. 625–632.

[2] Haichang Gao, Xiyang Liu, Sidong Wang, Honggang Liu, Ruyi Dai, Design and analysis of a graphical password scheme, in: 2009 Fourth International Conference on Innovative Computing, Information and Control, ICICIC, 7–9 Dec. 2009, pp. 675–678.
[3] J.D. Pierce, Jason G. Wells, Matthew J. Warren, David R. Mackay, A conceptual model for graphical authentication, in: 1st Australian Information security Management Conference, 24 Sept. Perth, Western Australia, November 2003, paper 16.
[4] S. Xiaoyuan, Z. Ying, et al. Graphical passwords: a survey, in: 21st Annual Computer Security Applications Conference, 2005, pp. 463–472.
[5] Jason Wells, Damien Hutchinson, Justin Pierce, Enhanced security for preventing man-in-the-middle attacks in authentication, data entry and transaction verification, in: Australian Information Security Management Conference, 2008. Paper 58.
[6] T. Takada, H. Koike, Awase-E: image-based authentication for mobile phones using user's favorite images, in: Human–Computer Interaction with Mobile Devices and Services, vol. 2795, Springer, Berlin / Heidelberg, 2003, pp. 347–351.
[7] A.E. Dirik, N. Memon, et al. Modeling user choice in the PassPoints graphical password scheme, in: ACM Proceedings of the 3rd symposium on Usable privacy and security, Pittsburgh, Pennsylvania, 2007, pp. 20–28.
[8] K. Wei-Chi, T. Maw-Jinn, A remote user authentication scheme using strong graphical passwords, in: 30th Anniversary IEEE conference on Local Computer Networks, 2005, pp. 351–357.
[9] A.H. Lashkari, F. Towhidi, et al. A complete comparison on pure and cued recall-based graphical user authentication algorithms, in: Second International Conference on Computer and Electrical Engineering, 2009, ICCEE '09, pp. 527–532.
[10] K. Renaud, On user involvement in production of images used in visual authentication, Journal of Visual Languages and Computing 20 (I) (2009) 1–15.
[11] M. Masrom, F. Towhidi, et al. Pure and cued recall-based graphical user authentication, in: International Conference on Application of Information and Communication Technologies, 2009, AICT 2009, pp. 1–6.
[12] J.C. Birget, H. Dawei, et al., Graphical passwords based on robust discretization, IEEE Transactions on information Forensics and Security 1 (3) (2006) 395–399.
[13] S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, N. Memon, PassPoints: design and longitudinal evaluation of a graphical password system, International Journal of Human-Computer Studies 63 (2005) 102–127. Special issue on HCI research in privacy and security.
[14] S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, N. Memon, Authentication using graphical passwords: effects of tolerance and image choice, in: Symposium on Usable Privacy and Security (SOUPS), 6–8 July 2005, at Carnegie-Mellon Univ., Pittsburgh.
[15] http://www.inventoryops.com/software_selection.htm.
[16] E.E. Merch, M.D. White, A taxonomy of relationships between images and text, Journal of Documentation 59 (6) (2003) 647–672.