Image based Authentication System

Pintu R Shah
Department of Information Technology, Mukesh Patel School of Technology Management & Engineering
Behind Homeopathy College, Bhakti Vedant Swami Marg, JVPD, Vile Parle (W)
Mumbai 400056, India

ABSTRACT

Username and password are the most commonly used mechanism for authentication because of simplicity and convenience. However it suffers from few drawbacks like selection of weak passwords by the users, users disclosing their passwords etc. This weakens the security posture of the organizations. Hence we propose a new image based authentication system. Research suggests that use of images may be more effective in terms of security and ease of use for some application. This is because we, humans are good at recognizing images than remembering password. In this paper we describe new image based authentication system which can be used independently or along with current character based authentication system to improve security and usability. We implemented the said system along with current authentication system (username and password). We carried out the user survey. Around seventy users including students and faculty tested the system and gave their feedback. After analysis, One of the key outcome is that 97% were able to register with the system and 94% we able to successfully authenticate with the system. Results of the user feedback are presented and discussed in this paper.

General Terms

Computer Security, Information Security.

Keyword

Authentication, Image based authentication, Graphical passwords, Multi level authentication, Usable Security, Human Computer Interaction.

1. INTRODUCTION

Authentication is the process of verifying the identity of the subject. Subject can be human user or some process. Hence authentication is the act of confirming the claims made by the subject. Authentication system can be describe by following five components [1]

1. Authentication data (A), which is provided by the user for verification like username and password.
2. Complementary data(C), which is stored on the system and used to validate authentication data provided by the user. For example password stored in the shadow file in Unix OS.
3. Complementation function (f) provides mapping of A with C. For eg. If password are stored as a message digest (MD) of password than f is the hash functions that creates MD.
4. Authentication function (L) proves the identity for eg. It can be equality function for comparison of A and C.
5. Selection function (S) allows users to create or change data in A or C. For eg. Change password function or set password function.

Traditionally Identity is established by any one or combination of two or more of the following methods:

- Knowledge factor. What user knows for eg. password
- Ownership factor. What user has for eg. smart card
- Inherence factor. What user is for eg. fingerprints, Iris scan etc

Recently in some authentication systems, apart from the above mentioned factors, locations [2], [3] as well as social factors [4] are also used for establishing identity. If only one factor is used for establishing the identity of the user we call that as one factor authentication. If two factors are used for establishing identity than we call that as two factor authentication. A classical example of two factor authentication is the use of credit or debit card and a PIN at the ATM machine. Here we use knowledge factor (PIN) and ownership factor (credit or debit card). In this paper, we describe two level authentication system using knowledge factors. First level is character based i.e username and password and second level is image based.

2. CURRENT SYSTEM

Username password is one of the most widely used authentication system for long. In this system, end user provides username and password at the login screen and system verifies the same. Outcome of the system can be binary either true or false, authenticated or not authenticated, success or failure. Alternative to username and password based authentication system is biometric system and smart card based system. Biometric system provides better security but requires an additional hardware which increases the cost. This also raises the question about every day usability and affordability. Also some biometric systems like iris scan are intrusive in nature to capture authentication data.

Other alternative is a smart card based system. However smart card can be easily lost or stolen. Therefore many smart cards based systems use knowledge based authentication systems to prevent impersonation through loss of card or theft of card.

In spite of common use and popularity of username and password based system, it has multiple shortcomings. Since the authentication data can be formed from a set of characters like combination of upper case, lowercase, numerals, special characters etc, it is subjected to brute force attack or dictionary attack. Selection of password plays a very

important role for providing strength to the security of the system. If the password selected is dictionary word like apple or some common passwords like pass123 etc, password can be easily guessed by the attacker [5] and system can be easily compromised. To overcome this problem, many organizations have password policy which enforces the rules for the formation of strong password and regular change of password. In many situations this has failed because users simply make a variation of old password or write down password or swap them with their friends or family. All this solutions do not remedy the main cause of password insecurity, which is the human limitation in terms of memory for secure passwords. [10]. Many times people communicate or share their password with other people for multiple reasons. This weakens the security of the organizations [6]. To overcome this we propose new system which uses images along with password to provide authentication.

3. PROPOSED SYSTEM

In the proposed system we use images along with the password to overcome the problem which arises because of sharing and selection of weak passwords. Hence the system aims to achieve following:

- Authentication should not be based on precise recall of password.
- Make it difficult to share or write passwords.
- Provide good user experience.

Also it's a proven fact that human user recognizes images faster as compared to recall of words [7]. Standing [8] shows that people can recognize images in spite of distracters and can retain over a period of time.

3.1 Stages of System

The proposed system has two stages: Registration stage and authentication stage.

3.1.1 Registration Stage

In registration stage, first users need to fill personal details like name, DoB, email address etc. During this stage user selects a password with the following constraints

- Minimum of eight characters as per the Anderson formula[1]
- Atleast one uppercase character and one numeral
- Atleast one special character from the character set {!, @, #, $, %,^,&}

Apart from selecting the password, user needs to select minimum one image as a pass image. User can select images from the various categories display in the Pass image selection grid as shown in figure 1.

C1	C2	C3
C4	C5	C6
C7	C8	C9

Figure 1. Pass Image Selection Grid

C1 to C9 represents various categories of the images. Image categories selected were related to animals, natural scenery, random art, flowers, objects etc. Every time user refreshes the page, various category images are populated in the grid randomly. We assume user selects three images. To select first image, say user selects C1 from the fig 1. Immediately a new randomly generated grid of 3x3 is presented to the user which contains 9 similar but distinct images of category C1. User selects one of the images as the pass image. Every time a grid is displayed position of the image changes randomly. These make it difficult for the user to share or describe the image to someone else. After the selection of first image, user selects second image from Pass image selection grid (fig 1) say C2. Second grid containing various images for category 2 is presented for the selection of second image. Similarly third image is selected. Once images are selected, user submits the same to the system to be stored as complementation data. Now once the user is registered he moves on to training phase where user needs to correctly identify the pass images from a group of decoy images. This completes the first stage.

3.1.2 The authentication stage

Now whenever user tries to log in, user needs to provide the username password and pass images. Pass images need not be in the same sequence as selected during registration phase. Pass images are randomly distributed on the login rounds. Every round may have all, some or none of the pass images. At least one round need not have pass images to counter intersection attack [9].

3.2 Advantages of the system

- Adds one more layer of security to the existing system and hence makes the system more secure.
- Log in by sharing of password is prevented as user needs to provide the password as well as pass images to log in. Sharing of pass images is difficult.
- Prevents brute force attack. After three unsuccessful attempts user account gets locked. This can be unlocked by the administrators.
- Prevents automated attack by the bots.
- Eliminate the possibility of deducing the user's image set by means of an intersection attack [9].

3.3 Limitation of the system

- System cannot prevent offline dictionary attack.
- Slower than traditional username password system as loading of image grid take some time.

3.4 Results

After implementation, users were invited to register with the system and then give feedback about their experience and the system. We had prepared questionnaire to get structured feedback from the users of the system. Objectives of this survey are given below:

- To assess the general awareness of the user regarding image based authentication system.
- To assess the time consumed while registering and logging with system.
- To assess the ease of use of system.
- To obtains user's opinions regarding our system in comparison with other authentication systems in terms of the speed, the ease of use etc.
- To find out the reasons behind the inability by some users either to register or to authenticate.
- To assess some other different areas that is not covered by the objectives above. An example of this is to assess the Random Art features of the images.

We got 70 responses of which 53 were male and 17 were female. Analysis of the feedback is given below:

- Only 37% were aware of the image based authentication before using this system.
- 97% were able to register with the system and 94% were able to login successfully. 47% were able to register in the first attempt, 50% were able to register after two attempts and 3% took three or more than three attempts to register successfully.

- 38% agreed that recognizing the image was faster as compare to recall of the password. 26% were not able to judge the difference.
- 70 % were of the opinion that system is easy to understand.
- Around 74% were easily able to identify three pass images.
- Around 90% trusted security of the system.

The survey result shows high success rate as 97% of the users were able to register and 94% were able to successfully authenticate with the system. This success may be because of following factors which may be contributing directly or indirectly.

- Removal of similar pass images
- Pass images does not appear more than once
- Flexibility in selection of pass images

3.4.1 Removal of similar pass images

Many of the too similar images were removed from the database. This has greatly contributed towards the high success of the system. The images used were downloaded from various sources from Internet. In total we had 1200 images for all categories. Of this we removed too similar images, which led to a total of 979. These images were removed because during development and testing we found that we ourselves were not able to distinguish between too similar images. Development team felt that this might lead to confusion which will affect usability and security of the system. Later actual users who were not able to either register or login indicated the similarity between the images as the key factor for their failure. This similarity may not be an issue for recall based system like username and password. For example password may contain capital I, small l, one 1 or pipe | as a character in password which are all confusing but still acceptable. This confusion may not be a problem with recall based system but it affects the usability of the recognition based system. Hence exclusion of such too similar images is a significant factor for success of image based systems.

3.4.2 Pass image does not appear more than once

In character based system we can have same character repeated in the formation of password. This will weaken the password. However in our system we have restricted user to select different pass images from various categories. High success rate indicates that it is not necessary to allow repetition of images. Also it will be beneficial for the usability and security of the system. Usability will be affected if the user selects similar images from same category.

3.4.3 Flexibility in selection of pass images

Traditional username password system support ASCII characters. However not all systems supports all 256 ACSII character set. Majority of the current system allows users to form password from typically 60 characters (upper case, lower case, numerals and some special characters). However in our system, user can select pass images from a set of 979 images. This gives user flexibility to select pass images which they can easily recognise later. While this is one of the key factors for the success of the system, it has negative consequence as well. It might be a time consuming task to browse through images. However users have indicated that it was a good experience to browse through images rather than to think of a new good password which is strong and easy to recall.

3.4.4 Choice of the pass images

We tried to find what kinds of images were favoured by the users. We found that users prefer to use images of objects, animals etc more as compared to random art images. This is in tune with the findings of Awase-E [11], [12]. The chance of choosing an image which has some meaning and appeal is higher than random arts.

3.4.5 Evaluation of time consumption

We monitored the time required to register with the system and verification of images. We found that the time required to select pass images is less as compared to select new password. This might be because system assist user to select pass images. It is difficult to always come up with new secure password which is easy to memorize and recall. Verification time for the password was faster as compared to pass images. This was because that password verification requires only one round whereas our system requires multiple images to be verified. However user's survey indicates that the time for our system was reasonable.

3.4.6 User Awareness

Many of the users of our system were not aware of image based authentication. Small numbers of the users were aware about image based authentication system. However, they had not used any such system. Many of the users believed that password and PIN systems were easy to use. The reason can be their long experience with the PIN and password system, comparatively faster authentication as compared to our system since user need to type only username and password or PIN. However majority of the users trusted the system to be secure and found ease to use.

4. CONCLUSION

High success rate indicates that authentication based on images can be used successfully for a particular purpose. A functional system was developed and user survey was carried out for seventy real users. Users were successfully able to recognize pass images from a group of images. It was not just based on the recognition but also on recall. This is because many users associated some images with some recall hints specifically for random images. For eg some random images appears to be a highway. However users favoured images with animals, objects rather than random art or abstract images. We implemented system along with username and password, but it can be implemented independently also.

5. ACKNOWLEDGMENTS

I would like to acknowledge the encouragement and guidance provided by Dr. Vijay Raisinghani and Dr. Ketan Shah. Thank you for your continuous motivation. I would like to thank my students Krishna Joshi, Shalin Sanghvi and Harsh Kagrana for implementing the said system and all study participants.

6. REFERENCES

[1] M. Bishop, S.S. Venkatramanayya, "Introduction to Computer Security", Pearson Education, 2009

[2] Shraddha D. Ghogare, Swati P. Jadhav, Ankita R. Chadha, Hima C. Patil, "Location Based Authentication: A New Approach towards Providing Security", International Journal of Scientific and Research Publications, Volume 2, Issue 4, April 2012. ISSN 2250-3153

[3] Sharma, Seema, "Location Based Authentication" (2005). University of New Orleans Theses and Dissertations. Paper 141. [Online]. Available : http://scholarworks.uno.edu/cgi/viewcontent.cgi?article=1145&context=td

[4] J. Brainard, A. Juels, R. Rivest, M. Szydlo, M. Yung, "Fourth Factor Authentication: Somebody you know", ACM'06. [Online]. Available: http://www.rsasecurity.ca/rsalabs/staff/bios/ajuels/publications/fourth-factor/ccs084-juels.pdf

[5] (2013) Imperva Site [Online]. Available: http://www.imperva.com/docs/wp_consumer_password_worst_practices.pdf

[6] M. Whitman, H. Mattford, " Principles of Information Security",2nd Ed. Cengage Learning,2009

[7] I. Rock and P. Engelstein, "A study of Memory for Visual Form",[Online]. Available: http://www.jstor.org/stable/1419366

[8] L. Standing," Learning 10,000 Pictures",[online]. Available: http://cvcl.mit.edu/SUNSeminar/standing73.pdf

[9] G. Danezis and A. Serjantov, " Statistical Disclosure or Intersection attacks on anonymity systems",[Online]. Available: http://research.microsoft.com/en-us/um/people/gdane/papers/poolsda3.pdf

[10] Rachana Dhamija and Adrian Perrig, "Déjà vu: A user using images for authentication", [online]. Available : https://sparrow.ece.cmu.edu/group/pub/old-pubs/usenix.pdf

[11] Hideki Koike, Tetsuji Takada, Takehito Onuki, "Awase-E: Photo-based User Authentication System", [online]. Available : http://www.netaro.info/~zetaka/publications/papers/awasee-UBICOMP2005.pdf

[12] Hideki Koike and Tetsuji Takada, "Awase-E: Image-based Authentication for Mobile Phones using User's Favorite Images", [online]. Available : http://www.netaro.info/~zetaka/publications/papers/awasee-MobileHCI03.pdf