Image Based Authentication Techniques to Prevent Intrusion

Kavya.S
Dept. of ISE
City Engineering College
Bangalore-560061
kavya.dashmi@gmail.com

Manasa.D
Dept. of ISE
City Engineering College
Bangalore-560061
manasadeshik@gmail.com

Abstract

PDAs are becoming one of the most popular gadgets all over the world. A PDA functions as a personal information manager. It has many functions. People store personal information like PIN numbers, account numbers etc. in the PDA. No one should access this information except the owner. Owner should be authenticated to use the gadget. Textual passwords are vulnerable to dictionary attacks, social engineering and shoulder surfing. Many graphical schemes are proposed to address these problems, but most of them are vulnerable to shoulder-surfing. Two authentication techniques- Pair based, and Text based Image Authentication are proposed in this paper which are resistant to shoulder surfing.

Keywords: Image based authentication, Intrusion prevention, Graphical passwords, Shoulder-surfing .

1.Introduction

With the development of many sophisticated gadgets like PDAs, people are accustomed with these technologies in their everyday life. With the quick development in technology, PDAs are surely becoming more and more popular. It is becoming common now-a-days to have a PDA which functions as a personal information manager. Today's handheld computers and PDAs have many functions that allow people to store and access their personal and confidential information at ease. So, there is a necessity to provide authentication into these devices. Due to the vulnerabilities of textual passwords, there has been a growing interest in using graphical passwords as an alternative technique. With the help of these graphical password schemes, it is possible to provide authenticity to PDAs.

Conventional textual passwords use alphanumeric characters to authenticate a user. Generally, users pick easy or short passwords [1] and this makes the authentication system easy to break [*2, 3*]. But strong passwords are hard to remember so, it is necessary to provide an authentication system which is easy for the user to remember and hard for the attacker to break. Many graphical password schemes are proposed based on the fact that it is easy to remember pictures or images than text for humans [4, 5]. Based on the survey [6], it is considered that there are two types of authentication categories: recognition-based and recall-based approaches. In recognition-based techniques, users are presented with a set of images and users prove their authenticity by identifying pre-defined images. In recall-based techniques, users are asked to reproduce something that they created or selected earlier during the registration stage. Most of these graphical password schemes suffer from shoulder-surfing which is becoming quite a big problem.

Pair based image authentication uses both recognition and recall based approaches in which user has to recollect the key positions and recognize his image pairs. Text based image authentication also uses recognition and recall based approaches where user has to recognize his images and recall their respective characters assigned at the time of registration. techniques are user friendly, generate session passwords and are resistant to shoulder-surfing.

This paper is organized as follows: related work is discussed in section 2, image based authentication techniques are discussed in section 3, analysis and user study are presented in section 4, conclusion is proposed in section 5.

2.Related Work

As we store sensitive information in PDAs and due to increase in corporate theft, it is important to provide proper security mechanisms to these handheld devices. With graphical password

authentication as alternative to both textual passwords and biometrics [*7*], many graphical authentication schemes have been proposed.

Dhamija and Perrig [8] proposed a graphical authentication scheme where the user has to identify the pre-defined images to prove user's authenticity. But it took a lot of time to log-in compared to textual passwords since the user has to select number of pictures. Passface [9] is a technique where the user sees a grid of nine faces and selects one face previously chosen by the user. Since there are four user selected images it is done for four times. The drawback of the both of these techniques is vulnerability to shoulder-surfing. Davis et al[10] proposed an alternative scheme story that used images instead of faces. It was difficult to remember images than faces but user choices were less predictable.

Jermyn et al.[11] proposed a new recall based technique called "Draw- a-Secret" (DAS) where the user has to re-draw the pre-defined picture on a 2D grid. If the drawing touches the same grids in the same sequence, then the user is authenticated. DAS have lower password strength due to user chosen passwords and it is vulnerable to shoulder surfing. The technique proposed by Syukri, et al. [*12*] uses user signature as the password, but the probability of breaking by forging the signature by the attacker is there in this corporate world. Blonder [13] designed a graphical password scheme where the user must click on the approximate areas of pre-defined locations. Wiedenbeck [14] extended Blonder's idea in which the user has to click within the tolerance of their chosen pixels and also in correct sequence. But results showed that these schemes have difficulty in learning the password and took more time to input their password. Sonia Chiasson, et al. [*15*] where each user click results in next image leading to certain path. This process can be hectic and also not implement able to small devices like PDAs.

To overcome shoulder-surfing problem many mechanisms have been developed. S. Komanduri and D. Hutchings [16] proposed a shoulder-surfing resistant system where selection of items by on-screen mouse cursor was not enabled for this task, although the mouse pointer was still visible. Users then press the key which appeared in the same location as their password users to select a sequence of images to make a story. The concern with this is the tolerance level for the drawing trace length wherein user has to be careful and also with the use of stylus where the user always has to have it. This is mainly developed for PDAs and this is one of the effective schemes that could be implemented.

All the above discussed existing methods have disadvantages- 1. Login process slow. 2. Too many objects involved. 3. stylus required. 4. Display may be crowded with too many images. 5. tolerance levels to be considered. 6. may not be suitable for PDA's because of small size display. The two proposed techniques have the features- 1. Resistent to dictionary attack and social engineering since session passwords are generated. 2. Strongly resistant to shoulder surfing. 3. Login procedure is simple and easy to use, comparatively faster item. Upon pressing any key corresponding to picture in their password, the characters reshuffled while the picture grid remained unchanged. This is continued until the complete password has been entered. So this has significant usability drawbacks as the users are required to keep track of unfamiliar locations and also this could not be employed on PDA since the display is crowded making it is time consuming for users to log-in for everyday authentication.

Sobrado and Briget [17] proposed a technique which is resistant to shoulder-surfing. In this technique the user has to recognize their three objects and click the convex hull formed by these three objects to prove his\her authenticity. In their second scheme, the users have to prove their authenticity by moving the frame containing user object until it lines up with the two other user's objects. But the drawback of this technique is that it makes the log-in process slow because user need to recognize his/her images (or objects) from a crowded display of objects which contains 1000 objects as suggested by the authors. In such case, this could not be applicable to relatively small displays like PDAs.

Man, et al [18] proposed a shoulder surfing resistant scheme where users has to authenticate themselves by identifying their objects and typing in a string which is the unique-code, pre-defined by the user while registration, corresponding to the variant of the user objects present on the display as well as their relative location. They extended their technique by allowing the users to assign their own codes to their objects. Even though these techniques are hard to crack, it makes users to memorize many strings and making them similar to textual passwords. Also this technique requires many objects to be displayed on the screen making the screen crowded so that it is difficult to crack and thus makes this difficult to implement on PDAs .

Haichang, et al proposed a new shoulder-surfing resistant scheme where the user is required to draw a curve across their password images orderly rather than clicking on them directly. This technique makes use of DAS and Story to draw a free-form picture and to allow

than other techniques. 4. Only 16 images will be displayed on the screen which is more suitable for PDA's. 5. remembering image pairs or image and text pairs are easy if the user follows some concept/story for his selection. 6. Extensive training is not required as they are simple.

3. Image Based Authentication Techniques

Two image based authentication techniques: Pair Based and Text Based Image Authentication schemes are proposed in this paper. The authentication technique consists of three phases: registration, login and verification. In the registration phase, user has to create his password. During login phase, user enters his password. In the final phase, the password entered is verified and the user is authenticated.

3.1 Pair Based Image Authentication: (PIA)

During registration, user selects eight pairs of images from a set of images in the system. That is the user need to select sixteen images and pair them at his choice making eight pairs. Figure 1 shows the pairs of images selected by the user. The user has to select three key positions in the 4x4 grid since the images are displayed in 4x4 grid. At the time of login, the interface displays 16 images (selected by the user as 8 pairs) in a 4x4 grid. The images are randomly placed in the grid. Now, as password user has to click on three images. Considering the key positions selected by him during registration, for the images in the key positions he has to recollect the pair of images and he has to click on those images even if they are in key positions.

Figure 2 shows the interface during login, 4x4 grid with images. The images marked At the time of login, the interface displays sixteen images in the form of a 4x4 grid. The grid consists of some of the images selected by the user and the other images selected from the database. Now the user has to type the password based on his images in the interface grid.

Figure 4 shows the login interface for a user which contains four user images marked with letter 'p'. Now the user has to type the character assigned to each image at the time of registration in the order in which they appear on the interface. Since there are only four user images he needs to type four characters as the password. But the password length should be six, so user should add two junk characters to the password. For the figure 4, the password is "mbrtxy" where "mbrt" is actual password which is based on the images in the interface and the last two letters "xy" are junk. It can be entered as "mbrtmb". During verification, system counts the no. of images selected by the user that appeared on the interface and compares only that no. of characters. The remaining characters will not be considered by the system.

with letter 'k' are the images which are in the key positions specified by the user (say, the key positions are 2, 9, 16). Now the user has to click on their respective pairs which are marked with letter 'p'. The respective pairs are in the positions 4, 13, 8. To verify the password, system takes the pairs of those images in the key positions and compares the images with the images selected by the user and authenticates the user. A new interface is generated for every login because the images are randomly placed on the grid every time.

3.2 Text Based Image Authentication: (TIA)

Sometimes or even most of the times people recollect the names of someone or something on seeing his image. Based on this ability, a technique is developed where the user types the password on seeing the images. This technique uses text as the password to provide authenticity. The password depends on the images in the interface. During registration, user selects six images and assigns a character to each image as shown in figure 3.

Figure 1. Selected pair

With the constraint on password length, the intruder is not having actual information about the length of the password.

4.Analysis

Every authentication scheme should be evaluated against possible attacks. Since the proposed techniques generate session passwords, they are resistant to dictionary attack and social engineering.

Shoulder Surfing:

Figure 2. Login Interface

Shoulder surfing refers to using direct observation techniques, such as looking over someone's shoulder, to get information. In PIA, the attacker cannot identify the three key positions even though the pass images are visible and these pass images change for every session. It is not possible to know the password for TIA since the observer cannot predict the actual length of the password. Because of the generation of session passwords for every login, these techniques are not vulnerable to shoulder surfing.

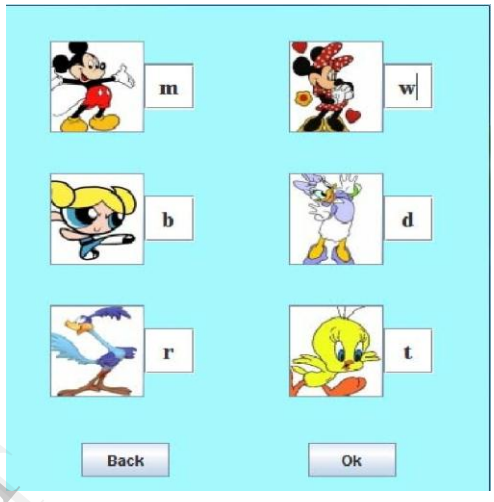

Figure3.Characters Assigned To Images

Guessing: In PIA technique, the strength of the password depends upon the user selected images and the way user paired them. If the user selects well known pairs like Tom and Jerry, it is easy to break the technique. In TIA, the strength of textual password depends on the user selection of characters for images.

Brute force attack: It is more difficult to carry out a brute force attack against graphical passwords than text-based passwords. Traditional brute force cannot break any of these techniques.

With extensive search PIA could be breakable in ($16C_3$x15x13 x 11) attempts whereas for TIA it takes ($20C_6x36^6$) attempts to break .

The number of images in the database reflects the strength of the password in these techniques, particularly in TIA because if the database contains too many or too less images these techniques become weak, so database must contain moderate number of images. For this a moderate number of images i.e 20 is selected for these techniques.

User Study

We conducted the user study of the proposed techniques with 20 participants.. They are first, second and third year B.Tech students.

Figure 4: Login interface

We conducted a learning session for them explaining how to create a password and how to enter password during login. Initially there was password registration phase in

which users created their passwords. Usability study was conducted with the students in two sessions with 10 students for each technique. During password creation each user selects pairs of images or images and text. The technique PIA took more time than TIA for password creation.

Table 1 shows the registration time for each technique. Table 2 shows the log -in time for each technique for the first session of user study. It is found that, though pair based technique took more time to register, it took very less time to log-in than text-based techniques since it requires only three clicks to register. Table 3 shows the log-in time for the second session which was taken after one week of first session. The no of successful logins is also recorded for both sessions and given in table 4 and table 5.

Table 1
Registration time for passwords

Technique	Avg	Min	Max
Pair-based Image Authentication	187.16	69.07	262.61
Text-based Image Authentication	53.85	49.49	70.97

Table 2
Login time for correct passwords at session 1

Technique	Avg	Min	Max
Pair-based Image Authentication	17.95	12.51	29.26
Text-based Image Authentication	42.69	23.41	76.41

Table 3
Login time for correct passwords at session 2

Technique	Avg	Min	Max
Pair-based Image Authentication	11.10	7.07	17.01
Text-based Image Authentication	29.91	16.69	47.76

We observed that PIA took less time compared to the first week of analysis. TIA also showed a great improvement in the average time to log-in once users are familiar and could remember the password images and their codes.

Table 4
Successful logins at session 1

Technique	Correct	Incorrect
Pair-based Image Authentication	5	5
Text-based Image Authentication	6	4

Table 5
Successful loginsat session 2

Technique	Correct	Incorrect
Pair-based Image Authentication	7	3
Text-based Image Authentication	8	2

5.Conclusion

A PDA which is designed to function as a personal information manager has a variety of functions. It is necessary to provide authentication to handheld devices. In order to overcome the drawbacks of textual passwords, we proposed two techniques making use of graphical passwords. The Pair based and Text based image authentication techniques are resistant to shoulder-surfing and generates session passwords making intruder's job difficult. The security analysis is provided and the usability of these techniques is given. It is observed that PIA success rate is being increased with the familiarity of the images selected .An extensive study has to be done on regarding user selection of images.

References

[1] A. Adams and M. A. Sasse, "Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures," *Communications of the ACM*, vol. 42, pp. 41-46, 1999.

[2] A. S. Patrick, A. C. Long and S. Flinn, "HCI and Security Systems". Presented at CHI, Extended Abstracts (Workshops). Ft. Lauderdale, Florida, USA, 2003.

[3] Gilbert Notoatmodjo, "Exploring the 'Weakest Link': A Study of Personal Password Security". Thesis of Master Degree, the University of Auckland, New Zealand, 2007

[4] R. N. Shepard, "Recognition memory for words, sentences, and pictures," *Journal of Verbal Learning and Verbal Behavior*, vol. 6, pp. 156-163, 1967.

[5] D. Weinshall and S. Kirkpatrick, "Passwords You'll Never Forget, but Can't Recall," in *Proceedings of Conference on Human Factors in Computing Systems (CHI)*. Vienna, Austria: ACM, 2004, pp. 1399-1402.

[6] X. Suo, Y. Zhu and G. Owen, "Graphical Passwords: A Survey". In Proc. ACSAC'05.

[7] Justin D. Pierce1, Matthew J. Warren1, David R. Mackay1, and Jason G. Wells2, "Graphical Authentication: Justifications and Objectives".

[8] R. Dhamija, and A. Perrig. "Déjà Vu: A User

Study Using Images for Authentication". In 9th USENIX Security Symposium, 2000.

[9] RealUser. "www.realuser.com" last accessed in June 2005

[10] Davis, D., F. Monrose, and M.K. Reiter. "On User Choice in Graphical Password Schemes" 13th USENIX Security Symposium, 2004.

[11] I. Jermyn, A. Mayer, F. Monrose, M. Reiter and A. Rubin. "The design and analysis of graphical passwords". In Proceedings of the 8th USENIX Security Symposium, August 1999

[12] A. F. Syukri, E. Okamoto, and M. Mambo, "A User Identification System Using Signature Written with Mouse," in *Third Australasian Conference on Information Security and Privacy (ACISP)*: Springer-Verlag Lecture Notes in Computer Science (1438), 1998, pp. 403-441.

[13] G. E. Blonder, "Graphical passwords," in *Lucent Technologies, Inc., Murray Hill, NJ*, U. S. Patent, Ed. United States, 1996.

[14] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system," *International Journal of Human Computer Studies*

[15] Sonia Chiasson, P.C. van Oorschot, and Robert Biddle, "Graphical Password Authentication Using Cued Click Points".