Enhancing security of Pass Points system using variable tolerance

M.Samuel John
Department of Computer Applications, V.R.Siddhartha Engineering College, Vijayawada, INDIA
Email: write2samuel@gmail.com
V.Siva Parvathi, M.Raja Sekhar
Department of Computer Science and Engineering,
P.V.P.Siddhartha Institute of Technology, Vijayawada, INDIA
Email: sivaparvathi.mtech@gmail.com, macharlasekhar@yahoo.co.in
P.Raveendra Babu
Department of Computer Science and Engineering,
V.R.Siddhartha Engineering College, Vijayawada, INDIA
Email: raveendrababup@gmail.com

ABSTRACT

Passpoints system is one of the techniques used in Authentication using Graphical Images. In this method users click on images rather than typing a long and complex alphanumeric password with the computer keyboard. Psychological studies have shown that people can remember pictures better than text. During the time of registration a user may choose several areas (click points) on an image. In order to log in the user has to click close to the chosen click points, e.g. within .25 to .50cm from the click point, because users cannot click exactly on the same pixel on which they have clicked at the time of registration. This margin of error around the click point is called Tolerance. Existing Passpoints scheme uses the same tolerance (20X20 pixels) over a number of clicks by the user. But by varying the tolerance (i.e. decrementing the tolerance level) as users click on more points, the information left to an attacker is reduced. Hence, the security of the system is increased. In this paper we described how the level of security is increased.

Keywords- **Authentication, Graphical Passwords, PassPoints Scheme, Tolerance.**

Date of Submission: December 22, 2009 Accepted: February 23, 2010

1. Introduction

NOW a days, all business, government, and academic organizations are investing a lot of money for the security of information. A key area in securing the valuable information is authentication. What is Authentication? Authentication refers to the process of verifying the Identity of a communication partner. It determines whether a user is allowed to access a particular system or resource. Today it is a critical area of security research. Authentication techniques can be classified into three categories (shown in Fig.1). They are

1. Token based authentication
2. Biometric based authentication
3. Knowledge based authentication

The best example for token based authentication is a bank card (credit /debit). Some token-based authentication systems also use knowledge based authentication technique to enhance the security of information. For example, ATM cards generally require a PIN number which is to be remembered by the user.

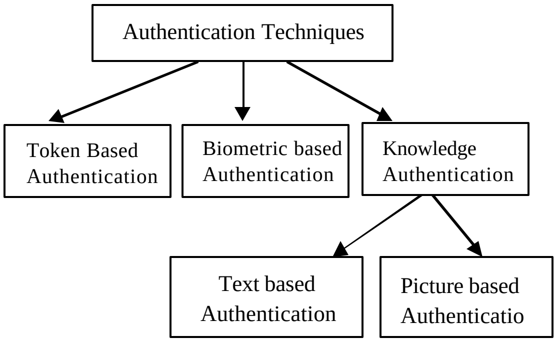

Authentication Techniques
Token Based Authentication
Biometric based Authentication
Knowledge Authentication
Text based Authentication
Picture based Authenticatio

Fig 1: Classification of authentication techniques

Fingerprints , Iris scan, voice recognition, hand geometry are comes under Biometric Authentication. But the drawback of this approach is that the systems and equipment used for verifying the authenticity are not only expensive but also the process is slow. However, this technique has a high level of security.

Finally, Knowledge based techniques are the most commonly used techniques. Knowledge based techniques are classified into two categories. They are text based passwords and picture based passwords [1]. The picture based authentication techniques are further divided into two categories. They are recognition-based graphical techniques and recall based graphical techniques.

In recognition based technique, a user is given a pool of images and the user has to recognize and identify the images, which he or she selected during the time of registration.In recall based techniques, the user has to reproduce something he or she created at the time of registration.

2. Why graphical Passwords?

Graphical passwords are an alternative to existing alphanumeric passwords. In graphical passwords users click on images. Prior to the graphical passwords, the most common authentication method used is a 'Password', which is an alphanumeric word known to the computer and the user. The results of a recent survey shows that 93% of large businesses in United Kingdom still use passwords to authenticate users [2] .But users have many problems with the alphanumeric passwords like difficulty in remembering complex, pseudo-random passwords over time.

Generally, a 'good' password has some characteristics like including numbers, alphabets (both capital and small) and special symbols, words not present in dictionary and not only that it must be long enough to stand against different attacks. As a general rule of thumb, a strong password should have no less than eight characters. Such pseudo-random passwords lack meaningful content and can be learned only by rote memorization, which is a weak way of remembering [3]. Studies have shown that users tend to pick short passwords or passwords that are easy to remember [4], like alphabetic-only passwords consisting of personal names of family or friends, names of pets etc. Such passwords are easy to discover using dictionary attacks or attacks based on the knowledge of the user. According to Computerworld news article, a team of security engineers ran a password cracker in a network and within 30 seconds, they cracked 80% of the passwords [5].

People often forget their passwords. If a password is not used frequently it will be even more susceptible to forgetting. If the password is hard to guess, it is hard to remember. Psychological theories have identified decay over time and interference with other information in long term memory as underlying reasons for forgetting [6]. Another complicated issue is that users have many passwords for computers, networks and e-mails. Remembering a complex and long password is difficult. But Studies shows that human brain can better recall images than text [7].

Further studies on images shows that images are recognized with very high accuracy (up to 98%) after a two hour delay, which is much higher than accuracy for words and sentences [8]. In addition, it has been found that errors in recognition of images is only 17% after viewing ten thousand pictures [9]. Studies of recall also confirm that pictures are recalled better than words, and this has led to the "picture superiority effect" [10].

3. Background on graphical Password Systems

Apart from Passpoints technique [11], other techniques are also available [12, 13, 14]. One such technique is Passfaces [15], in which user chooses four faces from a pool of faces. When logging in , the user sees a 3X3 grid of nine faces, consisting of one face previously chosen by the user and eight decoy faces, the user has to recognize and click anywhere on the chose n face. This procedure is repeated with different target and decoy faces, for a total of four rounds.

It is observed that passfaces may be more memorable than alphanumeric passwords [16]. Another similar system is proposed [17] which suggest that choosing images from a pool of images is a slow process, but the images are easier to remember over time .

Passlogix [18] has developed a similar system. In their method, users must click on areas in the correct sequence in order to be authenticated. Invisible boundaries are defined for each clicked area in order to detect whether a particular area is clicked by the mouse. A similar technique was developed by sfr [19]. The software giant Microsoft has also developed a comparable graphical password technique where users are required to click on pre-selected areas of an image in a chosen sequence [20].

4.What is PassPoints system?

The passpoints system by Wiedenbeck, et al. [21, 22], is based on the idea of Blonder [13] in which the password is represented by multiple clicks on a single image. But passpoints system overcame the limitations of his (Blonder) scheme, i.e. there are no predefined boundaries around areas of the image where the user can click.

One of the advantages with passpoints scheme is that a user can click on anyplace on the image. An interface used in Passpoints scheme is shown in Fig. 2.

It allows the use of arbitrary images. After clicking on several places (pixels) the sequence is stored. A tolerance region around the chosen click points is calculated. When logging in, the user has to click on points within the tolerance. Generally, users cannot click on the same points that are selected during registration. So, a tolerance is given. This tolerance allows a user to click on nearby locations. For example, if the tolerance is 20X20, users can click on any location within the 20 pixels around a click point.

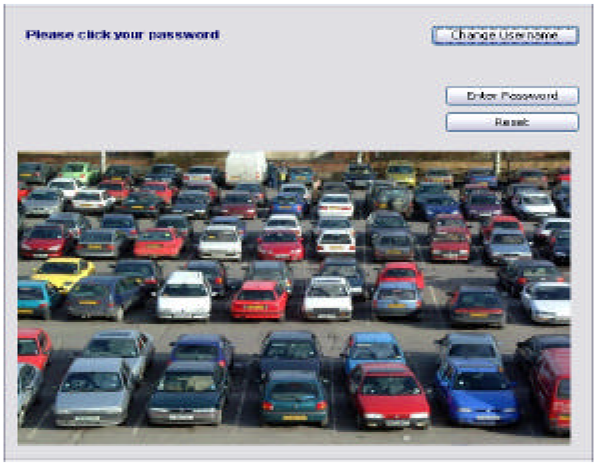


Fig 2: The PassPoints [22] interface

Wiedenbeck, et al [22] conducted a user study, in which one group of participants was asked to use alphanumeric password, while the other group was asked to use the graphical password. The result showed that graphical password took fewer attempts for the user than alphanumerical passwords. However, graphical password users had more difficulties learning the password, and took more time to input their passwords than the alphanumerical users.

There is another method in which a single click on multiple images is allowed. It is called as Cued Click Points. These schemes are called as cued recall based schemes since the background image can be regarded as a cue to recall the location of clicks chosen as a password.

Cued recall based schemes are different from recognition based schemes in one important aspect. Their password space (e.g. 2^{43} [13, 14]) is larger than the space in recognition based schemes (e.g. 10000 [17]). So recognition based schemes are generally not suitable for Internet applications where brute force attacks are possible.

5. Advantages of passpoints system

An image which is populated with many objects has hundreds of memorable points, which means that the passpoints scheme provides a large password space when compared with an alphanumeric password. For example an image with the size of 350X280 mm^2 with tolerance region of size $5X5mm^2$ and assume that nearly quarter of the image consists of memorable places, we can get 980 memorable tolerance regions.

If a user selects five click points, then this leads to 980^5 memorable passwords, which has a very large password space. Another observation is that, for alphanumeric passwords of length 5 over a 64 character alphabet, the number of possible passwords is 64^5.

Passpoints scheme also provides protection against key logger spy ware. A key logger captures all keystrokes that the user types on the computer keyboard, including passwords, personal information entered into an online registration form (e.g., a mailing address or telephone number), and financial information submitted as part of an online transaction, and the contents of emails or instant messages. Since, we use computer mouse than the keyboard to enter our graphical password, this protects us from key loggers.

6. Effects of varying tolerance

In our study we used client systems with 19inch monitors. This system is implemented as a web application. We used advanced java to develop this application. Images are stored at server side.

If a new user wants to register, he has to enter a user name. He/she will be given a set of eight images, shown in Fig 3. We used a forest image with different kinds of animals , a map with marked locations, a cage, an image with different colored birds, a group of national flags and fruits of different colors etc. The screen shot is:

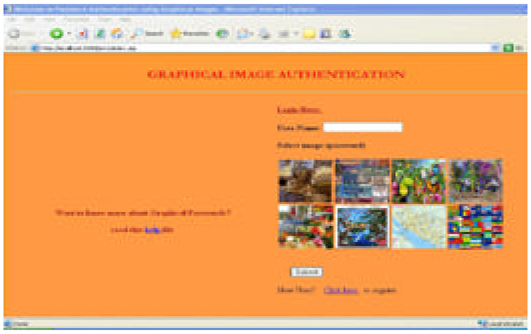


Fig 3: A screen shot of Login page

From these eight images, user has to select one image and then click on one or more areas as a graphical password. Users should remember the order of clicks and they have to produce the same order when they log in. Size of an image used in our application is 431X540. We modified original images in such a way that some English alphabets are added on the background of the image where background is plain and clear.

Now users can click not only on the areas of objects but also on areas where alphabets are present and they can even select small areas for example, upper half circle of the letter 'o'. Studies shows that images that are pleasant and have positive affect may support memorability [23].

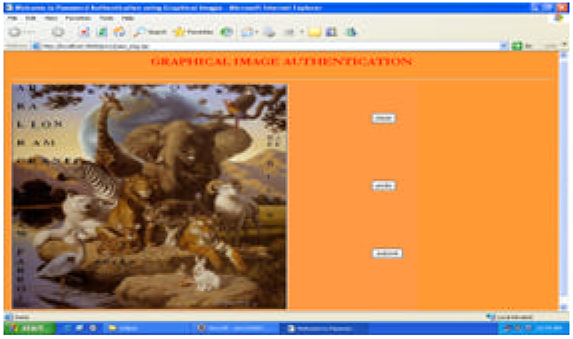


Fig 4: A screen shot of selected image for clicking

The original passpoints system used a constant tolerance over several click points. But we observed that by varying the tolerance i.e. by decreasing the tolerance level as the user click on more points, it has become more secure.

We implemented the system with the first four clicks taking the tolerance is 20X20, but from then onwards for every two clicks the tolerance is decremented.

The following table (Table.1) describes the tolerance (the margin of error around a click point) levels for consecutive clicks and corresponding sizes of squares (areas of an image) on the screen. If the user clicks within the square it is taken as accepted.

Table 1: Tolerance levels and selected areas in an image

Clicks	Total no. of clicks	Tolerance	Size in cm^2	Example
First 4 clicks	4	20X20	$.53cm^2$	□
Next 2 clicks	6	18X18	$.47cm^2$	□
Next 2 clicks	8	16X16	$.42cm^2$	□
Next 2 clicks	10	14X14	$.37cm^2$	□
Next 2 clicks	12	12X12	$.31cm^2$	□
Remaini-ng clicks	….	10X10	$.26cm^2$	□

In our experiment, we observed that most of the users are interested to have six to eight clicks in their graphical passwords. So, we gave high tolerance to the first four clicks and from then onwards the tolerance levels are decremented.

If a third person observes our clicks and try to reproduce the same after some time he/she may not succeed because for first four clicks the tolerance is same and for next two clicks onwards a clear observation is needed.

For example, if user selects only four click points the results are same for the existing system and our system. But if the user selects more than four clicks then security is enhanced i.e. if the user selects six points, and then in the existing passpoints system the same tolerance for all six points is used.

When we compare this with our system, if an attacker observes these clicks and tries to reproduce the same, the fifth click makes the difference.In the fifth click nearly 76click points (400-324) are reduced. So, attacker will not succeed if he clicks on these reduced 76 points .similarly for the next click (sixth click) another 76 pixels are reduced bringing a total of 152 pixels. In this manner for eight click points, same tolerance is used in the existing passpoints scheme but with the reduced tolerance levels the information left to an attacker is reduced by nearly 440(152+144+144)pixels are reduced. In this fashion if user selects more clicks in his/her graphical password, information left to an attacker is reduced by more number of pixels (Fig.6).

Since, images used in our experiment are having more clickable points, users had no trouble in clicking as long as the tolerance is greater than 10X10.

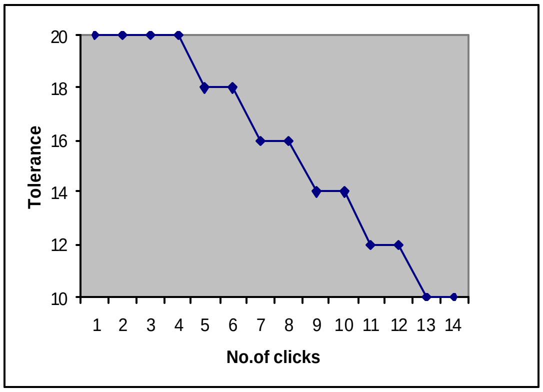


Fig 5: varying tolerance through number of clicks

This system could have been implemented in other way i.e. continuously decreasing the tolerance levels over the number of clicks starting from 20 to 10 with 10 clicks. But we observed that psychologically users are keeping in mind that they should choose only small and specific objects, so, it leads to a slow clicking process by forcing the user to select small objects. Based on Fitts' Law [24], if the input involves mouse movement and a small tolerance, we expect slower input times in graphical password systems. We found good results with long-term, regular use of the graphical password s.

7. Conclusion and future work

A major advantage of PassPoints scheme is its large password space over alphanumeric passwords. But the security of PassPoints system is also an important issue. We observed that by varying the tolerance levels, we leave less information to the attacker. Although graphical passwords are vulnerable to shoulder surfing attacks, our method provid es security over this attack. If an attacker observes our clicks from a distance, since we choose specific small objects or areas on the image with reduced tolerance, it is difficult to capture and reproduce the same. The 2D images used in this scheme can be extended to use 3D images and graphics.

References

[1] Xiaoyuan Suo, *"A Design and analysis of graphical password"*, Thesis submitted to Georgia state university, 2006.

[2] Information security Breaches Survey 2006, Price PaterhouseCoopers, April2006.

[3] Rundus D.J. Analysis of rehearsal process in free recall.. *Journal of Experimental Psychology* 89(1971) , 63-77.

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

[5] Gilhooly, K. "Biometrics: Getting Back to Business" in computer world, May 09,2005

[6] Wixted, T.J. The psychology and neuroscience of forgetting. Annual Review of Psychology 55 (2004) , 235-26

[7] Madigan, S. Picture Memory, In John C.Yuille,editor, *Imagery memory and cognition*, Pages 65-89. Lawrence Erlbaum Associates,N.J., U.S.A.1983.

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

[9] Standing, L.P.Learning 10,000 pictures .*Quarterly Journal of Experimental Psychology* 25,207-222.

[10] Nelson, D.L., Reed, U.S., and Walling, J.R.Picture superiority effect. *Journal of Experimental Psychology: Human Learning and Memory* 3(1977) ,485-497

[11] Wiedenbeck, S.,Waters, J.,Birget, J.C., Brodskiy, A. and Menon, N. "Authentication using graphical passwords: Basic results". In *Human-Computer Interaction International (HCII 2005)*,Las Vegas, NV, 2005.

[12] A kula,S and Devisetty,V "Image Based Registration and Authentication System," in Proceedings of Midwest Instruction and Computing Symposium,2004.

[13] Blonder, G. *Graphical Passwords*, In Lucent Technologies,Inc., Murray Hill,NJ, U.S Patent,Ed.United States,1996.

[14] Chiasson, S.,van oorschot, .P.C., Biddle, R *Graphical Password Authentication using Cued Click-Points*. ESORICS, September 24-27 2007, Dresden, Germany, Springer-verlag, LNCS4734 (2007).

[15] Real User Corporation. The Science behind Passfaces. www.realuser.c om/published/ScienceBehindPassfaces.pdf accessed in Dec 2009

[16] Brostoff,S and Sasse, M.A..Are Passfaces more usable than passwords: A field trial investication.In "people and Computers XIV-Usability or Else"*: Proceedings of HCI 2000(Bath, U.K., Sept.8-12, 2000)*..Springer Verlag, 405-424.

[17] Dhamija, R.,.Perrig,A., 2000. De'ja' vu*:* a User Study Using Images for Authentication. *Proceedings of USENIX Security Symposium*,August2000

[18] Passlogix.http://www.passlogix.com,accessed on October, 2009.

[19] sfr, www.viskey.com/tech.html, last accessed in Oct 2009.

[20] Paulson, L.D., "*Taking a Graphical Approach to the Password* ," Computer, vol.35, pp.19, 2002.

[21] Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A and Menon,N. "*Authentication using graphical passwords: Effects of tolerance and image choice*". In Symposium on Usable Privacy and Security (SOUPS) .Carnegie-Mellon University, Pittsburgh 2005.

[22] Wiedenbeck, S., Waters , J., Birget, J.C., Brodskiy, A and Menon, N. PassPoints: Design and longitudinal evaluation of a graphical password system. *International J. of Human-Computer Studies* (Special Issue on HCI Research in Privacy and Security), 63:102-127, 2005.

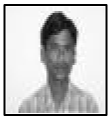
[23] Bradley, M.M., Grenwald, M.K. ,Petry, M.C.and Lang, P.J.Remembering pictures: Pleasure and arousal in memory. *Journal of Experimental Psychology* 81,2(1992), 379-390

[24] Hollingsworth, A. and Henderson, J.S.Accurate visual memory for previously attended objects in natural scenes. *Journal of Experimental Psychology* –Human Perception and Performance 28 (2002), 113-136

Authors Biography

M.Samuel John received the M.C.A degree from Bapatla Engineering College, Bapatla, Nagarjuna University in 2003. He is currently working as Lecturer in the Deparment of Computer Applications, V.R.Siddhartha Engineering College, Vijayawada, INDIA. He has four and half years teaching experience and pursuing M.Tech(Computer Science) in P.V.P.Siddhartha Institute of Technology. His research areas are Computer Networks, Cryptography and Network Security and Data mining and DataWarehouseing.

V.Siva Parvathi received the M.Tech (Computer Science) degree from Andhra University. She is currently working as Asst.Professor in the Department of Computer Science, P.V.P.Siddhartha Institute of Technology, Vijayawada, INDIA. She has 2 years and 1 month of teaching experience .Her research areas are Cryptography and Network Security and Computer Networks.



P.Raveendra Babu received the B.Tech (Computer Science) degree from V.R.Siddhartha Engineering College, Vijayawada, Nagarjuna University in 2006.He is currently working as Lecturer in the Department of Computer Science, V.R.Siddhartha Engineering College, Vijayawada. He is pursuing M.Tech (Computer Science) in P.V.P.Siddhartha Institute of Technology, His research interests are Cryptography and Data warehousing and mining.

M.Raja Sekhar received the B.Tech (Information Technology) degree from Lenora College of Engineering, Rampachodavaram, JNTU in 2006. He is pursuing M.Tech (Computer Science) in P.V.P.Siddhartha Institute of Technology, His research interests are Cryptography, Computer Networks and DataBaseManagementSystems.