IJDCST @October Issue- V-1, I-6, SW-88
ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

An Efficient Security Aspect of Three Level Systems for Data Authentication

Sahila Khan[1], Sumathi Rondla[2]

[1]M.Tech Student, Dept of CSE, Aurora's Technological and Research Institute, Parvathapur, Uppal, Hyderabad, A.P, India

[2]Associate Professor, Dept of CSE, Aurora's Technological and Research Institute, Parvathapur, Uppal, Hyderabad, A.P, India

ABSTRACT

There is a lot of increase in the technology and in which there is an improvement in the existence of the development of the web followed by the internet plays a major role in its key aspects by which it is related to the phenomena of the issue of the security is a primary concern respectively.

There is a huge challenge for the present method in which it is supposed to work on the present phenomena in which related to the security respectively. Here the passwords oriented with respect to the text based format is not sufficient for the enough protection of the data in a well stipulated fashion rather the problems is increase apart from the resolution based strategy and the approach is anachronistic in nature.

There is a lot of research takes place in the system in which related to the effective study of the above scenario where there is a complete resolution of the above problem is a major concern.

Here in order to overcome the above problem a new technique is implemented in which the approach is completely based on the security aspect of the three tier phenomena by which the one tier includes the security oriented text relative fashion whereas the tier two involves the security of the data authentication of the images as a password and followed by the present method in which it is completely based on the strategy of the three tier phenomena in which there is a password generation of the onetime strategy of the level one fashion where there is a complete reduction of the time followed by the accurate analysis with respect to the security oriented approach in a well oriented fashion respectively.

Here in the present strategy there is a receive of the security oriented data authentication in the form of the password is a primary concern in which it involves the email oriented fashion by which it receives the password by the help of the electronics mails where there is a less possibility of the hacking respectively.

Here an effort of the assiduous phenomena in which it is designed to overcome the problem of the attack related to the shoulder strategy in a well efficient manner followed by the attack of the tempest and the brute force is a primary concern respectively. Here this particular strategy is implemented by the help of the images oriented with the system of the IBA is a primary scenario respectively.

Experiments have been conducted on the present method and a lot of analysis takes place on the large number of the data sets with respect to the unknown environment and there is an improvement in the performance followed by the outcome of the entire system compared to the several previous methods in a well efficient fashion respectively.

Keywords: **Data authentication, Image processing, Authentication of images, Logging oriented key stroke, AJAX, attack of the tempest and the attack of the brute force respectively.**

1. INTRODUCTION

It is now beyond any doubt that USER AUTHENTICATION is the most critical element in the field of Information Security. To date, Text Based Password Authentication (TBPA) has shown some difficulties that users have tended to write passwords down manually or save them on hard disc.

This tendency is caused by passwords being strong and thus difficult to memorize in most cases. This has inadvertently given rise to security issues pertaining to attack. Graphical User Authentication (GUA) has two symbiotic pillars as its foundation: USABILITY & SECURITY. The macro-concept of GUA is based on the human psychological factor that is images are more readily committed to memory than would TBPA's.

Undoubtedly, there is currently the phenomenon of threats at the threshold of the internet, internal networks and secure environments. Although security researchers have made great strides in fighting these threats by protecting systems, individual users and digital assets, unfortunately the threats continue to cause problems. The principle area of attack is AUTHENTICATION, which is of course the process of determining the accessibility of a user to a particular resource or system.

Today, passive or active users are the key consideration of security mechanisms. The passive user is only interested in understanding the system. The active user, on the other hand, will consider and reflect on ease of use, efficiency,

Memorability, effectiveness and satisfaction of the system. Generally, authentication methods are classified into three categories:

a. Inherit Based Authentication

The Inherent Based Authentication category which is also known as Biometric Authentication, as the name suggests, is the automated method/s of identity verification or identification based on measurable physiological or behavioral characteristics such as fingerprints, palm prints, hand geometry, face recognition, voice recognition and such other similar methods.

Biometric characteristics are neither duplicable nor transferable. They are constant and immutable. Thus it is near impossible to alter such characteristics or fake them. Furthermore such characteristics cannot be transferred to other users norbestolen as happens with tokens, keys and cards.Unlike the security of a user's password, biometric characteristics, for

Instance the user's fingerprint or iris pattern, are no secret. Hence there is no danger of a break in security.

b. Token Based Authentication

The Token Based Method category is again as the name suggestsauthentication based on a TOKEN such as: a key, a magnetic card, a smart card, a badge and a passport. Just as when a person loses a key, he would not be able to open the lock, a user who loses his token would not be able to login, as such the token based authentication category is quite vulnerable to fraud, theft or loss of the token itself.

c. Knowledge Based Authentication

The concept of Knowledge Based Authentication is simply the use of conventional passwords, pins or images to gain access into most computer systems and networks. Textual (alphabetical) and graphical user authentications are twomethods which are currently used. True textual authentication which uses a username and password has inherent weaknesses and drawbacks which will be discussed in the following section.

2. BACKGROUND

One of the major problems of the textual password is the difficulty of remembering passwords. A survey has shown that most of the users tend to select short passwords or passwords that are easy to remember which unfortunately, can be easily guessed or broken by attackers. Other users select long passwords which are difficult to commit to memory, as well as hard to guess or break.

The other drawback with textual passwords is that most users cannot remember a number of passwordsfor different authentications; they tend to use the same passwords for different accounts. Survey done by Xiaoyum at 2005 has revealed that running a password cracker in a sample network uncovered about 80% of passwords in 30 seconds (Xiaoyuan et al. 2005).

Psychological confirmed that, people can recognize and remember combinations of geometrical shapes, patterns, textures, and colors better than meaningless alphanumeric characters, making the graphical user authentication to be greatly desired as a possible alternative to textual passwords. This type of authentication is formed by combining images, icons or pictures.

3. Background on graphical Password Systems

Graphical passwords were firstdescribedbyBlonder.Since then,manyother graphical passwordschemes have been proposed.Graphicalpassword systemscanbe

classifiedas:

1. recognition-based
2. recall-based

3.1 RECOGNITION BASED TECHNIQUES

3.1.1D´ej`a Vu: A User Study Using Images for Authentication

This approach to improve the security of systems relies on *recognition based*.

It consists of 3 phases:

1. Portfolio creation phase
2. Training phase
3. Authentication phase

Portfolio Creation Phase

To set up a D´ej`a Vu image portfolio, the user selects a specific number of images from a larger set of images presented by a server. Figure shows the image selection phase in our prototype.

The type of images used has a strong influence on the security of the system. For example, if the system is based on photographs, it would be easy for users to pick predictable portfolios, to describe their portfolio images and to write down this information and share it with others.

For this reason, we use Andrej Bauer's *Random Art* togenerate random abstract images

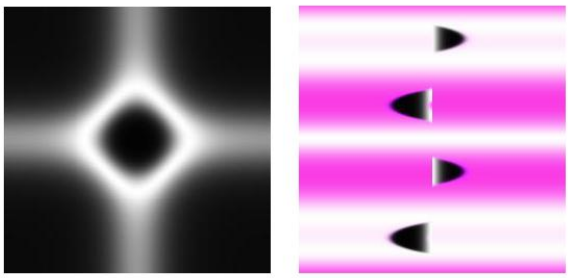

Figure1: Random Art Images

Training Phase

After the portfolio selection phase, we use a short training phase to improve the memo ability of the portfolio images. During training, the user points out the pictures in her portfolio from a challenge set containing decoy images. The selection and the training phase need to occur in a secure environment, such that no other person can see the image portfolio.

Authentication Phase

A trusted server stores all portfolio images for each user. Since each image is derived directly from the seed, the server only needs to store the seed and not the entire image. In our prototype implementation, the seed is 8 bytes long, hence the storage overhead for each portfolio is small. For each authentication challenge, the server creates a challenge set, which consists of portfolio and decoy images. If the user correctly identifies all portfolio images, she is authenticated.

3.1.2 COMPARISON WITH JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY IMAGE BASED AUTHENTICATION (JUIT-IBA) SYSTEM

In JUIT-IBA system the user can go back to any of the previous image sets to select or de-select his password images.

But in our 3-Level Security system, the user can move on to the next image grid, only after selecting the appropriate image from that current image grid.

The image sets used in JUIT-IBA system, are easy to be remembered by an eavesdropper, due to considerable difference in the colours of the images. Also they have incorporated three levels in JUIT-IBA, which are designed as beginner, moderate, and advanced, from where the user can select upto 5,9,13 images respectively. This definitely will be a tedious job for the user to select such large number of images.

Figure2: JUIT-Login Screen

3.2 RECALL BASED TECHNIQUES

In recall based techniques we use pass points techniques in our project.

3.2.1 Pass point:

Based on Blonder's original idea, Pass Points is a click-based graphical password system where a password consists of an ordered sequence of five click-points on a pixel-based image as shown in figure. The image is displayed on the screen by the system. The image is not secret and has no role other than helping the user remember the click points.

Any pixel in the image is a candidate for a click point.To log in, the user has to click again closely to the chosen points, in the chosen sequence. Since it is almost impossible for human users to click repeatedly on exactly the samepoint, the system allows for an error tolerance r in the clicklocations (e.g., a disk with radius r = 10 or 15 pixels). The image acts as a cue to help users remember their password click-points.

An important feature of the PassPoints system is thatthe underlying images for a password are not restricted tosimple comics-like drawings. Complex real-world images canbe used; users can even install their own images. Naturalimages help users remember complex passwords better.

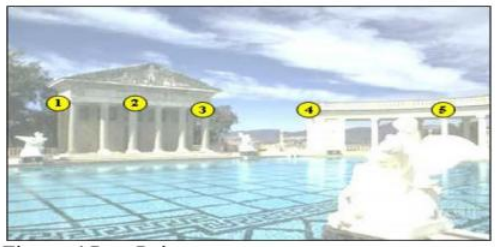

Figure3: Click Points Example

4. PROPOSED SYSTEM:

4.1Text Authentication (LEVEL-1)

Passwords have been used with computers since the earliest days of computing. MIT's CTSS, one of the first time sharing systems, was introduced in 1961. It had a LOGIN command that requested a user password. "After typing PASSWORD, the system turns off the printing mechanism, if possible, so that the user may type in his password with privacy. Tolog in,at the client side is ensured by the use oftext password, and that text password has to be entered byensuring employment of special characters. Therefore, security at LEVEL1 is ensured by use of text password which is a usual approach with normal login scheme.

Figure4 : Login Screen

4.2Image Grid BasedAuthentication(LEVEL-2)

The 3-Level Security System will then generate image grid with which contains the Image which is chosen by user earlier. The User must select the correct Image among the grid of 8 images in level 1and level 2 contains 6 images per grid.

The user had choice of choosing an image among the totally three grid formed by the server. If the user is choosing the all the correct images in the all the grids then only he can capable of passing this level. The user will be

authenticated as an authentic user, and will be awarded access to the stored information, only after crossing the three security levels.

Difficulty Level-1 In Level-2:

Figure5: Grid 1 of Difficulty Level-1

Involving different shades of blue.Mix of Blue, Indigo and White shades, in the different images above, are certainly not easy to be remembered.

Figure6: Grid 2 of Difficulty Level-1

The eye can distinguish up to a few hundred hues as per the fact, and when those pure spectral colours are mixed together or diluted with white light, the number of distinguishable chromaticities are sufficiently high

Figure6: Grid 3 of Difficulty Level-1

Indigo is meant to lie in the wavelengths range of blue and violet, and the hue changes in this range is relatively insensitive to the human eye. Therefore, most individuals find it hard to distinguish between different shades of blue, indigo, and violet.

Difficulty Level-2In Level-2:

The Image Based Authentication Level2 is difficult in comparison to Level1, as it employs images of ancient Egyptian picture symbols called “Hieroglyph”

Difficulty has been raised at this stage, just by the involvement of such unique and definitely interesting images. So, as to eliminate Brute force attack, Shoulder Attack and Tempest attack. These images require special attention and time, to be able to be recognized and to be remembered.

Figure7: Grid1,2,3 of Difficulty Level-2

4.3Click Point Authentication (LEVEL-3)

Image based authenticationwasdevelopedasanalternative clickbasedgraphicalpasswordschemewhere usersselectthree clickpointsonimageforone image.Theinterfacedisplaysonlyoneimage at atime; the imageis uploaded assoonasauserselectsaclickpoint and pixel points are saved for next login authentication. The system determinesthenextpixel point basedontheuser’s click-pointonthecurrent image and deterministicfunctionofthepoint whichiscurrentlyselected.

It nowpresentsa one- to-manycued recall scenario where imagetriggers the user's memoryof the one click-pointonthatimage.Secondly,if auser entersanincorrectclick-pointduringlogin,the next click pointdisplayedwillnot be considered. Conversely, thisimplicit feedbackisnothelpfultoanattackerwhodoes

notknowtheexpectedclick points onimage.

Figure 8: Click Points

5. CONCLUSION& FUTURE WORK

A common security goal in password-based authentication systems is to maximize the effective password space. This Impacts usability when user choice is involved. We have shown that it is possible to allow user choice while still increasing the effective password space. Furthermore, Grid Generation done by random number generator algorithm (used during grid alignment) cannot be exploited during an attack.

The approaches discussed in this paper present a middle ground between insecure but memorable user-chosen passwords and secure system generated random passwords that are difficult to remember.

Providing instructions on creating secure passwords, using password managers, or providing tools such as strength meters for passwords have had only limited success. The problem with such tools is that they require additional effort on the part of users creating passwords and often provide little useful feedback to guide users' actions.

InImage Based authentication, creating a less guessable password (by selecting a click-points within that image) is the easiest course of action. Users still make a choice but are constrained in their selection. Another often cited goal of usable security is helping users from accurate mental models of security.

The three level security approach applied on the abovesystem, makes it highly secure along with being more user-friendly. This system cannot be a suitable solution for general security purposes, where time complexity will be an issue. But will definitely be a boon in areas where high security is the main issue, and time complexity is secondary, as an example we can take the case of a firm where this system will be accessible only to some higher designation holding people, who need to store and maintain their crucial and confidential data secure.

REFERENCES

[1] Security Analysis and Implementation of JUIT-IBA System using Kerberos Protocol, Proceedings of the 7th IEEE International Conference on Computer and Information Science, Oregon, USA, pp. 575-580, 2008.

[2] Chippy.T, and R.Nagendran,"Defences Against Large Scale Online Password Guessing Attacks By Using Persuasive Click Points Volume 03– No.3, Issue: 01 March2012.

[3] Ahmet Emir Dirik, NasirMemon, Jean Camille Birget, "Modelling User Choice In The Click Points Graphical Password Scheme."

[4]R.DhamijaandA.Perrig,"Deja Vu:AUser StudyUsingImagesforAuthentication," in *Proceedingsoj9thUSENIXSecuritySymposium,*2000.

[5]SoniaChiasson, P.C.vanOorschot,and RobertBiddle,"Graphical Password Authentication UsingCuedClickPoints" ESORICS,LNCS4734, pp.359-374,Springer- VerlagBerlinHeidelberg2007.

[6] Richard E. Newman, Piyush Harsh and PrashantJayaraman, "Security Analysis of and Proposal for Image Based Authentication," 2005.

[7]ManuKumar,TalGarfinkel,DanBonehand TerryWinograd,"ReducingShoulder-surfingby UsingGazebasedPassword Entry",Symposium OnUsablePrivacyandSecurity(SOUPS),July 18-20,2007,Pittsburgh,PA,USA.

[8]ZhiLi,QibinSun,Yong Lian,andD.D. Giusto, 'Anassociation-based graphical passworddesiguresistant toshouldersurfing attack',InternationalConference onMultimedia andExpo (ICME),IEEE.2005

[9]S.AkulaandV.Devisetty,"Image Based RegistrationandAuthenticationSystem," in *Proceedings ojlv1idwes Instruction and Computing Symposium,*2004.

[10]L.SobradoandJ.-C.Birge!,"Graphical passwords,"*TheRutgersScholar,AnElectronic Bulletin forUndergraduateResearch,* vol. 4, 2002.

[11] Sonia Chiasson, Alain Forget , Robert Biddle,P.C. vanOorschot,"Userinterface desiguaffects security:patternsinclick-based graphicalpasswords",Springer-Verlag2009.

[12]**I**.Jermyn,A.Mayer,F. Monrose,M. K. Reiter,andA.D.Rubin,"The Desiguand Analysis ofGraphicalPasswords," in *Proceedingsofthe 8th USENIXSecurity Symposium,*1999.

[13] S. Chiasson, R. Biddle, and P. van Oorschot, "A Second Look atthe Usability of Click-Based Graphical Passwords," Proc. ACM Symp. Usable Privacy and Security (SOUPS), July 2007.

[14] S. Chiasson, A. Forget, R. Biddle, and P. van Oorschot, "Influencing Users towards Better Passwords: Persuasive Cued Click- Points," Proc. British HCI Group Ann. Conf. People and Computers: Culture, Creativity, Interaction, Sept. 2008.

[15] S. Chiasson, A. Forget, E. Stobert, P. van Oorschot, and R. Biddle, "Multiple Password Interference in Text and Click-Based Graphical Passwords," Proc. ACM Conf. Computer and Comm. Security (CCS), Nov. 2009.

[16] E. Stobert, A. Forget, S. Chiasson, P. van Oorschot, and R. Biddle, "Exploring Usability Effects of Increasing Security in Click-Based Graphical Passwords," Proc. Ann. Computer Security Applications Conf. (ACSAC), 2010.

[17] S. Chiasson, A. Forget, R. Biddle, and P.C. van Oorschot, "User Interface Design Affects Security: Patterns in Click-Based Graphical Passwords," Int'l J. Information Security, vol. 8, no. 6, pp. 387-398, 2009.