ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 9, Issue 6, June 2022

EMAIL DIGITAL SIGNATURE

Boomika J
Computer Science & Engineering
Salem College of Engineering and Technology,
Salem, India.
boomikakalpana@gmail.com

Essakiyammal M
Computer Science & Engineering
Salem College of Engineering and Technology,
Salem, India.
rohinikanmani293@gmail.com

Gokila M
Computer Science & Engineering
Salem College of Engineering and Technology,
Salem, India.
jamunagokila2000@gmail.com

Gayathri V
Computer Science & Engineering
Salem College of Engineering and Technology, Salem,
India.
gayathrivpy2019@gmail.com

***Abstract*— The project entitled "Email Digital Signature" is web application. This application is developed using **ASP.Net** as front end and **SQL** Server as back end. This system, which will computerize the activities of the Secured Intranet Email Facility Using Digital Signature. The main feature of the computerized system is to keep track of all the information in more authenticated way where the information is not hided whereas this package provides the security measures which will inform the receiving user where the information from the other user is altered or not. The computerized process of Secured Intranet Email Facility Using Digital Signature has one Session.

Existing authentication system has certain drawbacks for that reason graphical passwords are most preferable authentication system where users click on images to authenticate themselves. An important usability goal of an authentication system is to support users for selecting the better password. User creates memorable password which is easy to guess by an attacker and strong system assigned passwords are difficult to memorize. So, researchers of modern days gone through different alternative methods and conclude that graphical passwords are most preferable authentication system. The proposed system combines the existing cued click point technique with the persuasive feature to influence user choice, encouraging user to select more random click point which is difficult to guess.

IEEE Keywords— Authentication, graphical passwords, images, usable security.

I. INTRODUCTION

Email digital signature is handle using graphical password. Graphical passwords provide a promising alternative to traditional alphanumeric passwords. They are attractive since people usually remember pictures better than words. In this extended abstract, we propose a simple graphical password authentication system. We describe its operation with some examples, and highlight important aspects of the system. Graphical passwords are an alternative authentication method to alphanumeric passwords in which users click on images to authenticate themselves rather than type alphanumeric strings. This research aims to study the usability features of the recognition base graphical password methods available and extract the usability features of the existing methods. In this paper we study the recognition base graphical password type with the available methods from the usability point of view according to previous studies and surveys. Then we match the usability features (General usability features, existing usability features for existing graphical password methods, and ISO usability features) to the existing graphical password methods and make a comparison study between these methods and the usability features. We have found that there is no method has the most important usability features. Thus, by completing this study a set of usability features is suggested to be in one graphical password system. This set includes the easy for use, memorize, creation, learning and satisfaction. Moreover, this work proposes to build a new system of graphical password system that provides promising usability features.

II. NOMENCLATURE OF AUTHENTICATION

The following figure 1 shows the representation of current authentication methods. The problem with text based password is that user creates memorable password which can be break easily and also the text password has limited length password which means that password space is small. Biometric based authentication techniques are somewhat expensive, slow and unreliable and thus not preferred by many [3]. Token based authentication system has high security and usability and accessibility then the others. Also the system uses the knowledge based techniques to enhance the security of token based system. But the problem with token based system is that if token get lost, the security get also lost.

Therefore the Knowledge based authentication high security. Graphical Password is one of the knowledge based technique and it is categorized into Recognition based and Recall based [11]. In Recognition based techniques user has to recognize or reproduce the things during the login where as in case of recall based technique user has to recall the things during the login in such a way that whatever they selected during the password creation they have to recall it in the same manner. The three most commonly recognized factors are: 'Something you know', such as a password or PIN 'Something you have', such as a credit card or hardware token 'Something you are', and such as a fingerprint, a retinal pattern, or other biometric.

In computer security, authentication is the process of attempting to verify the digital identity of the sender of a communication such as a request to log in.

The sender being authenticated may be a person using a computer, a computer itself or a computer program. A blind credential, in contrast, does not establish identity at all, but only a narrow right or status of the user or program.

In a web trust , "authentication" is a way to ensure users are who they say they are—that the user who attempts to perform functions in a system is in fact the user who is authorized to do so, Wikipedia (2007).

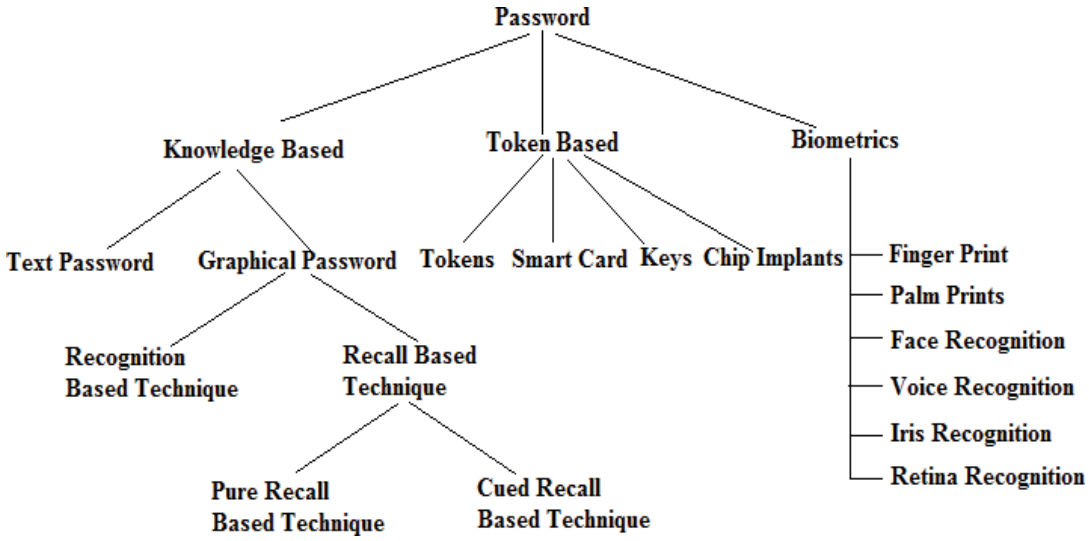

Fig. 1.Categorization of Password Authentication Techniques

III. LITERATURE REVIEW

G. E. Blonder proposed graphical password scheme in which user click on several different predefined location on a predetermined image. During login, the user has to click on the approximate area of those locations. Basically the image helps the user to summon up their passwords and therefore this scheme is considered more suitable than unassisted recall. The problem with this system is that boundaries are predefined which results various attacks are easily possible.

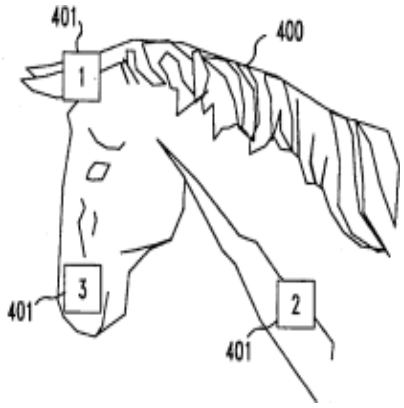

Fig. 2. Blonder's Scheme

In this method Blonder designed a graphical password scheme in which a password is created by having the user click on several locations on an image. During authentication, the user must click on the approximate areas of those locations. The image can assist users to recall their passwords and therefore this method is considered more convenient than unassisted recall (as in text-based password). G.E. Blonder (1996).

Fig. 3. Pass-Point

This system proposed by Wiedenbeck, *et al* Las Vegas (2005) and. Wiedenbeck, *et al* Pittsburgh (2005), extended Blonder's idea by eliminating the predefined boundaries and allowing arbitrary images to be used. As a result, a user can click on any place on an image (as opposed to some pre-defined areas) to create a password. A tolerance around each chosen pixel is calculated. In order to be authenticated, the user must click within the tolerance of their chosen pixels and also in the correct sequence This technique is based on the discretization method proposed by Birget, *et al* (2003). Because any picture can be used and because a picture may contain hundreds to thousands of memorable points, the possible password space is quite large. Wiedenbeck, et al. conducted a user study Google (2007), in which one group of participants were asked to use alphanumerical 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.

Later Wiedenbeck, *et al,* also conducted a user study to evaluate the effect of tolerance of clicking during the re-authenticating stage, and the effect of image choice in the system. The result showed

after using smaller tolerance for the user clicked points, but the choices of images do not make a significant difference. The result showed that the system works for a large variety of images.

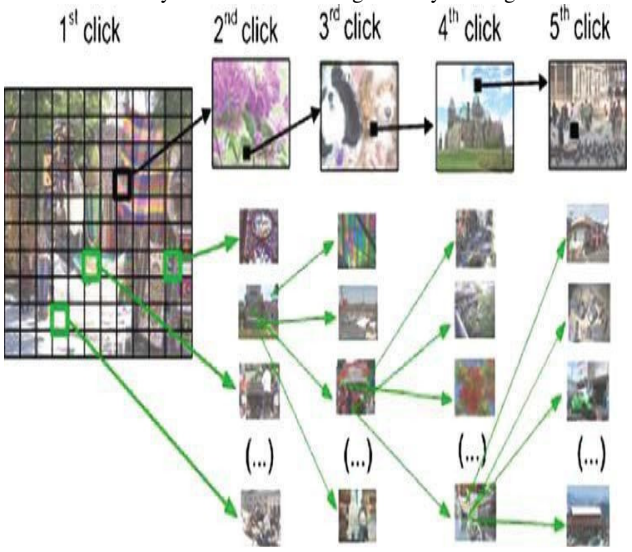

Fig. 4. Cued Click point

A. Forget et al. [10] proposed persuasive text password (PTP) scheme which employs a persuasive technology principles to persuade users in creating more secure passwords. During password creation, the user select his own password, the PTP improve its security by placing the arbitrary chosen characters at random positions into the password. Users can shuffle the random characters until they find the combination to be memorable. Basically PTP is a user-chosen text secret code system which helps user to build their password more secure.

IV. PROPOSED SYSTEM

The proposed system is based on click based graphical password system that not only guides and helps the user for password selection but also encourages the user to select more random distributed password. The proposed system is based on Persuasive Technology which motivates and influence people to behave in a desired manner. The proposed system combines the Persuasive features with the cued click point to make authentication system more secure. Basically, during password creation, the part of an image which is less guessable is highlighted and user has to select the click-point within the highlighted portion and if the user is unable to select the click-point then he can move towards the next highlighted portion by pressing the shuffle button.

The highlighted part of an image basically guides users to select more random passwords that are less likely to include hotspots. Therefore, this works encouraging users to select more random, and difficult passwords to guess. During Login, images are displayed normally and user has to select the click point as chosen at the time of password creation but this time highlighted portion is not present as it only provides the system suggestion. An important usability goal of proposed system is to support users in selecting password of higher security with larger password space. The proposed system removes the pattern formation attack and Hotspot attack (it is an area of an image where most of the user is selecting it as the click-point). Also, it removes the shoulder surfing attack.

EXPERIMENTAL RESULTS

Two modules are implemented which is described as follows,

A. *Module I*

Module I is used to set the seed value or unique value for the user. This seed value plays a vital role to select the First image. Also this seed value is used for further image selection. The seed value is generating on the basis of user name. Then the user name and seed value will decide the First image. Here for example Fig. 5. shows the first module result such that user name is "**boomikavijay@gmail.com**" for this user name the seed value generated is "**65025**" and correspondingly first image is retrieve on the basis of user name and seed value.

B. *Module II*

In module II Centred Descreatization technique is implemented. Discreatization is used to just allow the correct click-points to be accepted in the region without storing exact click-point co-ordinates. Centred Descreatization [12] offers centre tolerance such that during password creation an invisible grid is overlaid in such a way that the grid comes in centre with respect to selected click-point and the grid size used is 2r×2r. It divides an image into square\ tolerance regions, to verify whether a login click-point comes within the same tolerance region as the original click-point. During password creation the grid's location is set for every click-point and there is a identical tolerance area centered around the original click-point, by calculating the appropriate (x,y) and grid offset (Gx,Gy) (in pixels) from a (0,0) origin at the top-left corner of the image. Later during user login, the system uses the originally recorded grid offsets to place the grid and determine the acceptance of the each login click-point. [2] discussed about a method, Wireless sensor networks utilize large numbers of wireless sensor nodes to collect information from their sensing terrain. Wireless sensor nodes are battery-powered devices. Energy saving is always crucial to the lifetime of a wireless sensor network. Recently, many algorithms are proposed to tackle the energy saving problem in wireless sensor networks. [4] discussed about a method, This scheme investigates a traffic-light-based intelligent routing strategy for the satellite network, which can adjust the pre-calculated route according to the real-time congestion status of the satellite constellation.

Fig. 5. Module I: Seed value generation and First Image Generation.

During Password Creation:

1. Grid offset (Gx,Gy) used for grid positioning and can be calculated as,

   Gx = (x - r) mod 2r

   Gy = (y - r) mod 2r where r is tolerance value

2. A Tolerence area identifier (Tx,Ty) is given by,

   Tx = (x - r)/2r

   Ty = (y-r)/2r

During Login:

First it retrieves the corresponding (Gx,Gy) for corresponding click point and calculate

Tx = (x - Gx)/2r

Ty = (y-Gy)/2r and checks the current click-point falls in the grid or not.

Following Fig. 6. shows the implementation of second module in which for every click-point the corresponding grid offset(Gx_i,Gy_i) and tolerance factor(Tx_i,Ty_i) is calculated and corresponding grid offset is stored in the database. Fig: 6 shows the result for first click-point. For password generation SHA-1 algorithm is used. SHA1 is one way hash function. Password is generated using

$$PW=Hash([C_1,. \ldots\ldots\ldots ,C_i],W,X]$$

where C_i=current click-point having [I_i,Gx_i,Gy_i,Tx_i,Ty_i]

W= seed value.

X=User Name

Similarly Fig. 7. Shows the password generated for the user and which is stored in database.

Fig. 6. Module II: First Click-point(x1,y1) , Grid offset(Gx1,Gy1) and Tolerance factor(Tx1,Ty1) calculated.

V. SECURITY ANALYSIS OF GRAPHICAL PASSWORD

A. *Dictionary attack*

In Graphical Password scheme dictionary attack is not possible because here user gives an input using mouse where as in case of text password user provides input through the keyboard which results dictionary attack is easily possible.

B. *Guessing*

The most basic guessing attack is Brute-force attack. Some Graphical Password system is vulnerable to guessing attack.

C. *Shoulder Surfing*

Like text password Graphical password is also vulnerable to Shoulder-Surfing attack.

D. *Spy ware*

Key logging or key listening spy ware cannot be used to break graphical passwords system. Mouse motion alone is not enough to break graphical passwords.

E. *Social engineering*

It is very difficult for a user to discuss regarding the graphical password as compare to text password. So Graphical Password Systems are free from Social Engineering attack.

VI. CONCLUSION

In this project we did an Adding Persuasive feature in Graphical Password to increase the capacity of KBAM. It's to develop this project; we used ASP as a front end and MS SQL as backend.A major advantage of proposed scheme is that it provides larger password space then the alphanumeric passwords. For Graphical passwords there is a rising interest is that they are better than the Text based passwords, while the important argument for graphical passwords are that people are better at memorizing graphical passwords than text-based passwords. Also, it removes the pattern formation and hotspot attack since it provides the system suggestion. Also, the proposed system removes the shoulder surfing attack.

REFERENCES

[1] Learning Visual Basic .NET - Jesse Liberty - Oct 25, 2002

[2] Christo Ananth, T.Rashmi Anns, R.K.Shunmuga Priya, K.Mala, "Delay-Aware Data Collection Network Structure For WSN", International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST), Volume 1,Special Issue 2 - November 2015, pp.17-21

[3] Professional VB 2005 with .NET 3.0 (Programmer to Programmer) -Bill Evjen, Billy Hollis, Bill Sheldon, and Kent Sharkey - Jun 5, 2007

[4] Christo Ananth , P.Ebenezer Benjamin, S.Abishek, "Traffic Light Based Intelligent Routing Strategy for Satellite Network", International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST), Volume 1,Special Issue 2 - November 2015, pp.24-27

Web References

1. www.w3schools.com
2. www.programmersheaven.com
3. www.codeproject.com