ISSN: 2277-9655
Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Increasing the Security Of Graphical Passwordauthentication Using Persuasive Cued Click Points Increasing the Security Of Graphical Passwordauthentication Using Persuasive Cued Click Points

Keerthana S[*1], Lavanya T S[2], Krishnamoorthy[3]
[*1,2,3] Adhiyamaan College Of Engineering,Department of Information Technology,
DR.MGR nagar, Hosur, Tamilnadu,635109, India
Keerthiyadav92@gmail.com

Abstract

Passwords are the standard usage for user authentication. Traditional passwords are easy to implement but faces several attacks. Alternatively graphical passwords are used for users authentication which provides more security than text passwords. Strong passwords are difficult to remember and memorable pass words are easy to guess. The cued click points technique is combined along with the persuasive feature. Cued click points allows users to select the password using 5 different images. The proposed system consists of division and shuffling of images. Graphical passwords reduce the memory burden of users by replacing the task of recalling the password to that of recognizing the password.

Keywords: Authentication, CCP, graphical password, persuasive technology.

Introduction

A password is a form of secret authentication data that is used to control access to a resource. The passwords are used to control access to protected computer operating systems, mobile phones, ATM machines.

A typical computer user may require passwords for many purposes: logging in to computer accounts, retrieving email from servers, accessing files, databases, networks, web sites, and even reading the morning newspaper online.Various graphical password schemes have been proposed as alternatives to text-based passwords. Research and experience have shown that text-based pass- words are fraught with both usability and security problems that make them less than desirable solutions. Psychology studies have revealed that the human brain is better at recognizing and recalling images than textIn the proposed system the cued click points is combined along with the persuasive technology and also a feature is added which divides the image into 16 parts and then during the login session the divided image will be shuffled in a random manner each time the user logs in. This feature increases the security when compared to the existing system.

Nomenclature of Authentication

Text based passwords was one of the existing systems which had so many problems and there was no much security in the system. The text based passwords are easy to guess and difficult passwords are tough to remember. Due to these problems graphical password came in to existence which overcame the problems of text based passwords.

Graphical passwords are of three types ,firstBlonder's scheme in which the problem was pattern formation attack and predefined location. Second was pass point system it overcame the problem of predefined location but still faced pattern formation attack. At last cued click points came in to existence in which one click was made on 5 different images. It included a new feature called hotspot .this system used robust discretization technique which removed the problems of previous system but it faces false accept and false reject problems. The proposed system removes all these problems.

Literature Survey

A. Blonder's scheme:

Blonder's scheme is considered as the first cued recall based scheme .In this scheme, the user has to click on the predefined regions of the predetermined image to create a password. To authenticate successfully, user has to click on the previously selected region in the same sequence. One

ISSN: 2277-9655
Impact Factor: 1.852

drawback is that the user still needs to remember the sequence of clicks which requires memory recall.

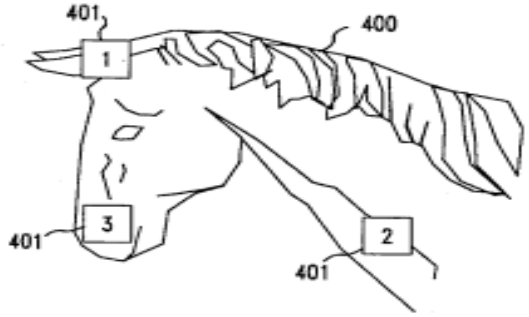

Fig 1: Blonders scheme

B. Passpoint scheme:

PassPointscheme which is an improvement over Blonder's scheme. In PassPoint system, any image can be used to create password with clear boundaries instead of predefined click region. The author also used tolerance distance for click points in order to avoid the difficulty for users to click exactly at the same pixel.

One problem with Pass Points system is that the image selection could be a tricky task. This is so because the image has to be rich enough to allow selection of many click points with negligible "hot spots". Images with fewer click points lead to security issues.

Fig 2:Passpoint Scheme

C. Cued click point:

Cued click point uses one click points on five different images instead of five clicks points on one image. The next image to be displayed is based on previous click point and the user specific random value by using a deterministic function.

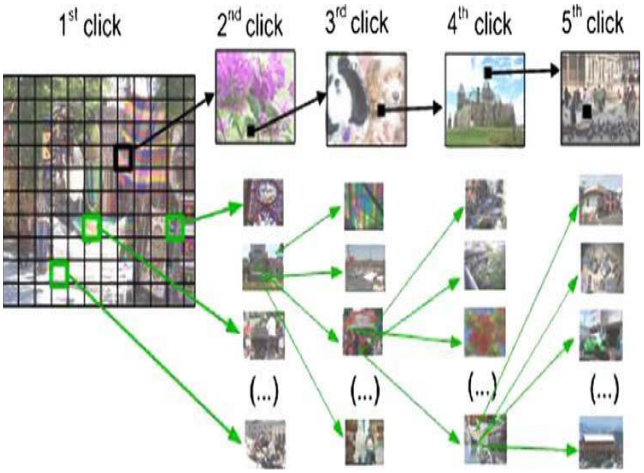

Fig 3:Cued Click Points

Proposed System

The proposed system is based on click based graphical password system which guides the user to select more random distributed password. The cued click points technique is combined with the persuasive feature and also additionally image division and shuffling is being done in order to increase the security.

During the password creation the image is split into 16 parts and displayed to the user so that the user can select the part which he wishes to choose as his password. The same procedure is followed for all the 5 images these points are less likely to be guessed by others.

This technique allows users to select more random passwords. During login process the divided images are shuffled randomly an displayed to the user and the user has the click on the same spot which he selected during the registration process. The proposed system removes pattern formation attacks.

Experimental Resuts

There are 2 modules in the proposed system.

A.Module 1:

This is the first module known as registration module in which the user details such as name email phone no. etc is taken as the input. The 5 different divided images are displayed to the user for the selection of the password. Fig 5 displays the result of module 1 while registering. The seed value of the user is determined.

The user has to click and 5 different images and those points are stored in the database by using a hashing algorithm called MD5. The centered discretization technique is been used in this process in which the grid offset is being calculated by using the x and y coordinates.

ISSN: 2277-9655
Impact Factor: 1.852

Fig 5:Image During Registration

The image size is taken as 200*200 pixels which is fixed. The image is divided into 16 parts i.e. Taking 50*50 each part then the grid offset and tolerance value are calculated based on those x and y coordinates.

The input for hash function is the points clicked each time, user name and the seed value generated for each user. The seed value is the value generated for each user which is different for each user. It is unique value through which a person can be identified and the images can be retrieved from the database.

B.Module 2

The second module is the login module where the same 5 images will to retrieve from the database and displayed to the user in the shuffled manner. The user has to select the image which he choose during the registration process.

During login process the user can click on any spot in the selected region, This is done because human eye cannot determine the exact pixel. The fig 7a and 7b shows the 2nd module result when user is logging in. The admin will maintain the user login and profile details.

The hash value is calculated using the MD5 algorithm. The **MD5** message-digest algorithm is a widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed in text format as a 32 digit hexadecimal number. MD5 consists of 64 of these operations, grouped in four rounds of 16 operations. F is a nonlinear function; one function is used in each round. M_i denotes a 32-bit block of the message input, and K_i denotes a 32-bit constant, different for each operation. $\lll_s$ denotes a left bit rotation by s places; s varies for each operation.

MD5 processes a variable-length message into a fixed-length output of 128 bits. The input message is broken up into chunks of 512-bit blocks (sixteen 32-bit words); the message is padded so that its length is divisible by 512.

The padding works as follows: first a single bit, 1, is appended to the end of the message. This is followed by as many zeros as are required to bring the length of the message up to 64 bits fewer than a multiple of 512. The remaining bits are filled up with 64 bits representing the length of the original message, modulo 2^{64}.fig 6 displays the MD5 process.

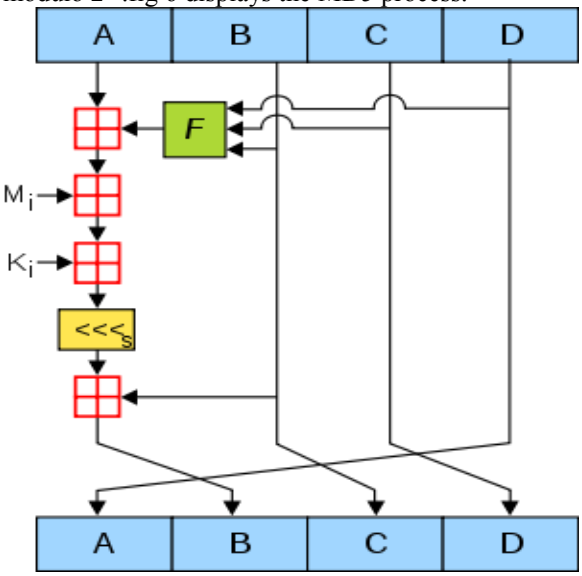

Fig 6: MD5 algorithm process

The main MD5 algorithm operates on a 128-bit state, divided into four 32-bit words, denoted A, B, C and D. These are initialized to certain fixed constants. The main algorithm then uses each 512-bit message block in turn to modify the state.

The processing of a message block consists of four similar stages, termed *rounds*; each round is composed of 16 similar operations based on a non-linear function F, modular addition, and left rotation. Figure 1 illustrates one operation within a round. There are four possible functions F; a different one is used in each round:

$$F(B,C,D) = (B \wedge C) \vee (\neg B \wedge D)$$
$$G(B,C,D) = (B \wedge D) \vee (C \wedge \neg D)$$
$$H(B,C,D) = B \oplus C \oplus D$$
$$I(B,C,D) = C \oplus (B \vee \neg D)$$

$\oplus, \wedge, \vee, \neg$ denote the XOR, AND, OR and NOT operations respectively.

Figure 8 displays the hash value stored in the database which is used for comparison while user logins.

ISSN: 2277-9655
Impact Factor: 1.852

Fig 7a: first image during login

Fig 7b: second image during login

location_grid_offset	hash_code
3,3=4,1=3,1=6,2=5,2	207873030745722568836503571356964474011
2,1=3,0=5,2=2,1=2,2	313730777129966504231280062820403916203[illegible]

Fig 8: database

Conclusion

Graphical passwords are introduced as alternatives to textual passwords. This paper proposed an authentication system which uses division and shuffling technique which will remove the pattern formation attack and shoulder surfing attack. This technique provides much security and as the future work the image can be split in more number and the grid offset value can be reduced to less number of pixels.

References

[1] *Uma D. Yadav, Prakash S. Mohod"Adding Persuasive features in Graphical Password To increase the capacity of KBAM" oct 2013*

[2] *L. O'Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication," Proc. IEEE, vol. 91, no. 12, pp. 2019 2020, Dec. 2003.*

[3] *A. Jain, A. Ross, and S. Pankanti, "Biometrics: A Tool for Information Security," IEEE Trans. Information Forensics and Security (TIFS), vol. 1, no. 2, pp. 125-143, June 2006.*

[4] *S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon,"Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice," Proc. First Symp. Usable Privacy and Security (SOUPS), July 2005.*

[5] *S. Chiasson, R. Biddle, and P. van Oorschot, "A second look at the usability of click-based graphical passwords," in ACMSymposium on Usable Privacy and Security (SOUPS), July 2007.*

[6] *Sonia Chiasson, Member, IEEE, Elizabeth Stobert, Alain Forget, Robert Biddle, Member, IEEE, and P. C. van Oorschot, Member, IEEE "Persuasive Cued Click-Points:Design, implementation, and evaluation of a knowledge-based authentication mechanism"*

[7] *S. Chiasson, P. van Oorschot, and R. Biddle, "Graphical PasswordAuthentication Using Cued Click Points," Proc. European Symp.Research in Computer Security (ESORICS), pp. 359-374, Sept. 2007.*

[8] *A. Forget, S. Chiasson, P. van Oorschot, and R. Biddle, "Improving Text Passwords through Persuasion," Proc. Fourth Symp. Usable Privacy and Security (SOUPS), July 2008.*

[9] *R. Biddle, S. Chiasson, and P. van Oorschot, "Graphical Passwords:Learning from the First Twelve Years," to be published in ACM Computing Surveys, vol. 44, no. 4, 2012.*