Integrated Intelligent Research (IIR)

International Journal of Computing Algorithm
Volume: 05 Issue: 01 June 2016, Page No. 34- 36
ISSN: 2278-2397

Image Based Password using RSA Algorithm

P L. Chithra[1], C. Vishnu Priya[2]
Department of Computer Science, University of Madras, Chennai
chitrasp2001@yahoo.com, Priyachengal2506@gmail.com

Abstract - A password is a sequence of characters used to determine whether the user is authenticated or not. Nowadays most of the password is text-based. Since text based password is hard to remember people try to use simple memorable password such as pet names, phone number, etc. which are easy to break by intruders. The main idea behind the paper is to replace the text-based passwords by image based password and encrypt using RSA algorithm. Our experimental result shows that image passwords are easy to remember, better than the text.

Keywords - Authentication, Image password, RSA.

I. INTRODUCTION

Authentication is the process of determining whether a user is authenticated to access a system. Text-based password is the most often used authentication system. A text password is nothing but a jumble of characters with strong encryption and decryption algorithm. But nowadays user can't remember strong password easily they create text passwords with pet names, phone number, etc. which is easy to remember and easy to guess. But password created must be easy to remember but hard to guess. Our human brain is better at remembering images than text. Image passwords are meant for reducing the memory saddle on users. Image passwords may offer better security than text-based passwords because most of the people, in an attempt to memorize text-based passwords, use simple words. Pass faces is a graphical password scheme where user needs to select the images from the large number and to login the user must identify one of the pre selected images amongst several images [1]. Draw - a - secret (DAS) is a graphical password scheme where user is requested to draw a picture using mouse or stylus. The coordinates of the grids occupied by the picture are stored. To login the user is requested to re-draw the same image. If the user draws the same image in the same grids, then the user is authenticated [2]. An alternative scheme is based on creating story using images . This would make users to select their images in the correct order. Users were encouraged for creating a story as a memory assist [3].

Pass-points is a technique where user needs to select five click points on the image for registration. For authentication user needs to select five click points in the same order [4]. In cued click points, user can select one click point for one image up to n levels as shown in figure 1. In login phase user should follow the order and select the click point [5]. In this paper, we propose an image based password authentication. A password consists of one click-point per image for a sequence of images. The image may be predefined or user defined. Image based password offers both improved usability and security. The rest of the paper is organized as follows. Section 2 describes the related work of this paper. Section 3 discusses the proposed methodology and section 4 provides the experimental result. Finally conclusion is presented in section 5 of the paper.

II. RELATED WORK

The concept of cryptography is to encrypt the plain text to cipher text and decrypt the cipher text to the plain text. It can be done in two ways (i) Secret key (symmetric): uses only a single key for encryption and decryption (ii) Public key (asymmetric): uses two keys namely public key and private key one for encryption and other for decryption. RSA was first described in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman. It is asymmetric cryptography, uses two different keys, one public and one private. The public key can be shared with everyone, whereas the private key must be kept secret. In RSA cryptography, both the public and the private keys can encrypt a message; the opposite key from the one used to encrypt a message is used to decrypt it [8]. The steps involved in this algorithm are discussed in figure 1.

Compute n = p * q = 53 * 61 = 3233
Compute φ(n) = (p - 1) * (q - 1) = 52 * 60 =3120
Choose e such that 1 < e < φ(n) and e and n are coprime.
Let e = 991
Compute a value for d such that (d * e) % φ(n) =1.
One solution is d = 1231
Public key is (e, n) => (991, 3233)
Private key is (d, n) => (1231, 3233)
The encryption of $m = 154$ is
$c = 154^{991} \% 3233 = 2896$
The decryption of $c = 2896$ is
$m = 2896^{1231} \% 3233 = 154$

Fig 1: Steps involved in RSA algorithm

According to this algorithm choose two distinct prime numbers p and q which should be considerably large enough. Then compute n which is the product of p and q and calculate the totient function φ(n).Next compute e such that e is less than totient function and gcd(e,n)=1 respectively and calculate d where (d * e) % φ(n) = 1. With the help of these values generate public key and private key and perform encryption and decryption process.

III. PROPOSED METHODOLOGY

The processes involved in this paper are shown in figure 2.

Fig 2: Process used in the image based password

The flowchart in figure 3 explains the sequence of steps involved in image based password. At first user requested to sign up by entering the name, date of birth, phone number, mail id and then user is provided with 3 images and the user must click one point per image. The images may be predefined or users wish. These click points are encrypted and decrypted

International Journal of Computing Algorithm
Volume: 05 Issue: 01 June 2016, Page No. 34- 36
ISSN: 2278-2397

using RSA cryptographic algorithm, which brings better security to the system. For login the user must select the same click points. If the user fails to select the correct password for more than 3 times, the user account would be locked and the account would be unlocked by entering the random alphanumeric text that has been sent to the authorized person mail. This approach would bring security and authorization to the system.

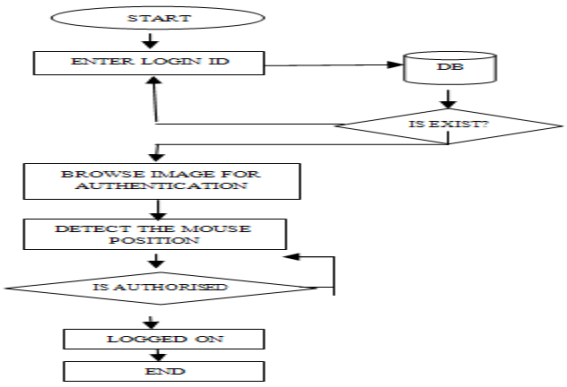

Fig 3: Flow chart for proposed methodology

IV. EXPERIMENTAL RESULT

The experimental result of the processes involved in this paper which has been implemented in c#.net and My Sql server are discussed below.

A. Registration process

In this process, the user is required to fill their detail such as name, phone number and email address as shown in figure 4. The user will be directed to a page where they can select their click points by clicking a particular position in the images as shown in figure 5. The user can also change the image by importing image from the system. By confirming, the details would be stored in the database.

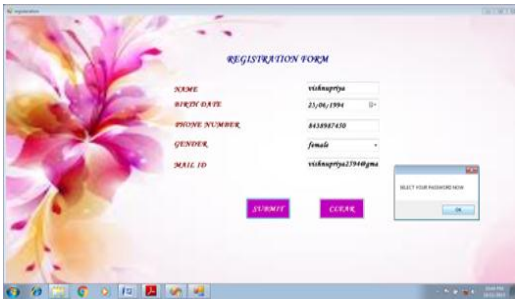

Fig 4: Registration form

Fig 5: Password selection form

B. Authentication process

In this process, the user is requested for the username and password. The user is given 3 chances to select the click points. If the user had crossed the chances, his/her account would be locked as shown in figure 6 and sent to a page where the user should enter the email id. If the username and password is correct then the user is directed to the second page, where the user can upload the files to the database and download it from the database. The user can change their personal information and password in this module.

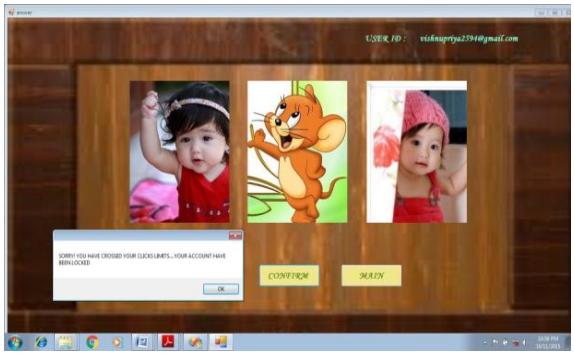

Fig 6: Account locked form

C. Retrieval process

The user would be directed to this process if the user had forgotten the password or the user account has been locked. Here the user must enter the mail id that has been submitted during registration process. If the mail id is found in the database then the random alphanumeric text is sent to their mail id as shown in figure 7. In the given textbox, if the user enters the correct alphanumeric text that has been sent to their mail id, then the user is authenticated and the user can select new click points or else the user can't.

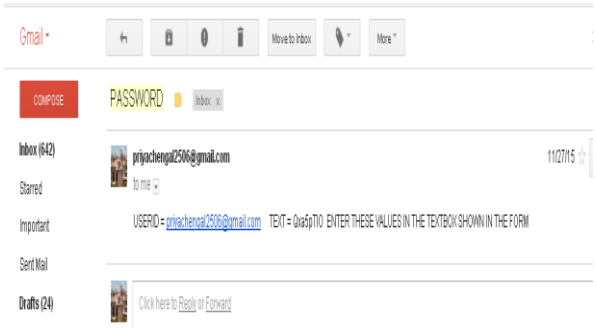

Fig 7: Alphanumeric text sent to authenticated mail

V. CONCLUSION

In this paper we have analyzed how to replace the text based password with image password using RSA algorithm in an effective manner. This system provides protection against key logger spy ware. Since, computer mouse is used rather than the keyboard to enter our image password this protects the password from key loggers.

Acknowledgment

Author would like to thank Dr.PL.Chithra, Associate Professor, Department of Computer Science, University of Madras for providing support.

International Journal of Computing Algorithm
Volume: 05 Issue: 01 June 2016, Page No. 34- 36
ISSN: 2278-2397

References

[1] M.P.Haridas, R.N.Devikar,(2015), **"**A Comparative Study of Graphical Passwords and Their Security Issues " in *International Journal of Advanced Research in Computer Science and Software Engineering* ,Vol. 5, pp. 575-581**.**

[2] S.Hande, N.Dighade , R.Bhusari, M.Shende, Prof. H.Agrawal,(2014),"Image Based Authentication for Folder Security using Persuasive Cued Click-Points and SHA," in IOSR Journal of Computer Engineering, Vol. 16, PP 124-128.

[3] V.Moraskar, S.Jaikalyani, M.Saiyyed, J.Gurnani, K.Pendke,(2014),"Cued Click Point Technique for Graphical Password Authentication," in International Journal of Computer Science and Mobile Computing, Vol.3, pp. 166-172.

[4] Iranna A M, P.Patil, (2013), "Graphical password authentication using persuasive cued click point," in International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering,Vol. 2, pp. 2963-2974.

[5] S.Pagidala, C.S.Bindu,(2013), "Improved Persuasive Cued Click Points forKnowledge-Based Authentication," in International Journal of Computer Science and Information Technologies, Vol. 4, pp. 1000-1003.

[6] J.A.Alex, S.Anees, N.Madheswari, (2013) , "User authentication based on persuasive cued clickpoints with sound signature," in Journal of Computer Science and Information Technology & Security,Vol. 3, pp. 353-358.

[7] S.Chaturvedi, R.Sharma, (2014),"Securing Image Password by using Persuasive Cued Click Points with AES Algorithm",in International Journal of Computer Science and Information Technologies, Vol. 5, pp. 5210-5215.

[8] W.Stallings,(2014) "Cryptography and Network Security Principles and Practices" 6th Edition, pp. 252-265.