ISSN No. 0976-5697

Volume 3, No. 4, July- August 2012

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

An Efficient Two Way Authentication Technique for the Protection of Personal Computer System

Mr. Ronak Jain*[1], Mr. Simarjeet Singh Bhatia[2] and Prof. Dinesh Chandra Jain[3]
Research Scholar*[1], Research Scholar[2], Reader[3]
C.S.E. Dept. SVITS Indore (M.P)
ronakjain1202@gmail.com*[1], bhatiasimarjeet@gmail.com[2] and dineshwebsys@gmail.com

Abstract- this research paper presents the authentication scheme that is particularly very lenient or very strict. Throughout the years authentication has been a very interesting approach. With all the means of technology developing, it can be very easy for 'others' to fabricate or to steal identity or hack someone's password. Therefore many algorithms are such based to pick a random number in the range of 10^6 and therefore the possibilities of the same number coming is rare.
Now a day's password scheme is based on verification, if entered information is matched with stored information than only user treated as valid user.

Keywords: two ways Authentication, Image Security Password, Verification.

I. INTRODUCTION

In the present scenario the pc security is a wide area of research and a lot of researchers and academicians have pursued their research in this direction but still there is major gap into the protection of system security[1]. So this research presenting a new era of technology for the system security like admin etc. basically we can use personal computer which can generally secured by a textual password and can be easily guessed by a person who is close to user and a lot of chances hack user's password when he enter during login[2]. If a user writes password on a paper and hides it, then there is a possibility of stealing the paper by an unauthenticated user know the password and access the files and directories easily.

This work carried out a proposed system that helps us to solve the problems which are coming into the existing systems by combining the various techniques used in the field of network security like one way authentication, two way authentication [3], digital signature, signature certificate etc.

II. EXISTING SYSTEM

The current authentication system have many drawback like textual passwords are commonly used by the users. Users tend to choose meaningful words from dictionaries, which make textual password easy to break and vulnerable to dictionary or brute force attack[4].

A. Problem in existing system:

Generally users make their personal identity as a password for example a name, telephone number, Mobile number, date of birth etc, which can be easily guessable by any person who knows all the details about that person[5][6].

B. Solution for existing system:

Due to lack of security in pc protection, many new techniques of authentication are developed such as fingerprint reader, eye scanner etc. But for a normal person, if security is important factor than cost is also an important factor. A normal user can't afford expensive recourses such as finger print scanner, webcam etc.[7]

III. PROPOSED SYSTEM

The proposed system is a 2 way authentication technique which provides user more security than single textual password. In this Technique user see 12 different images on his computer screen, each image is setup with their unique textual password. Now authentication is given on the basis of sequence of images and with their corresponding password [8][9]. Now this is what an authentication scheme, a new concept to differentiate the user is also based on sequence of images. For example:- to enter in administrator account a user have to sequencing image number 3 than 6 than 9. If user select the following sequence and enter a correct password with each images than a user authenticate for an administrator account [9][10].

Otherwise user can't be authenticating as a valid user till the sequence of image is correct.

ALGORITHM:

a. User must select the first image from the group of images.
b. Now input a password corresponding to that image.
c. User select second image from the remaining images.
d. Input password corresponding to second image.
e. Finally user selects the last image from the images.
f. Input password corresponding to that image.
g. First sequence of images is checked from the database whether it is correct or not, if not than it shows invalid user (no authentication provided).
h. If image sequence is correct that system checks that, the following sequence belongs to which user and retrieves the text password corresponding to that user.
i. Finally compare all textual passwords which are entered by user with the password store in the database, if all three passwords are matched than authentication is provided to the user.

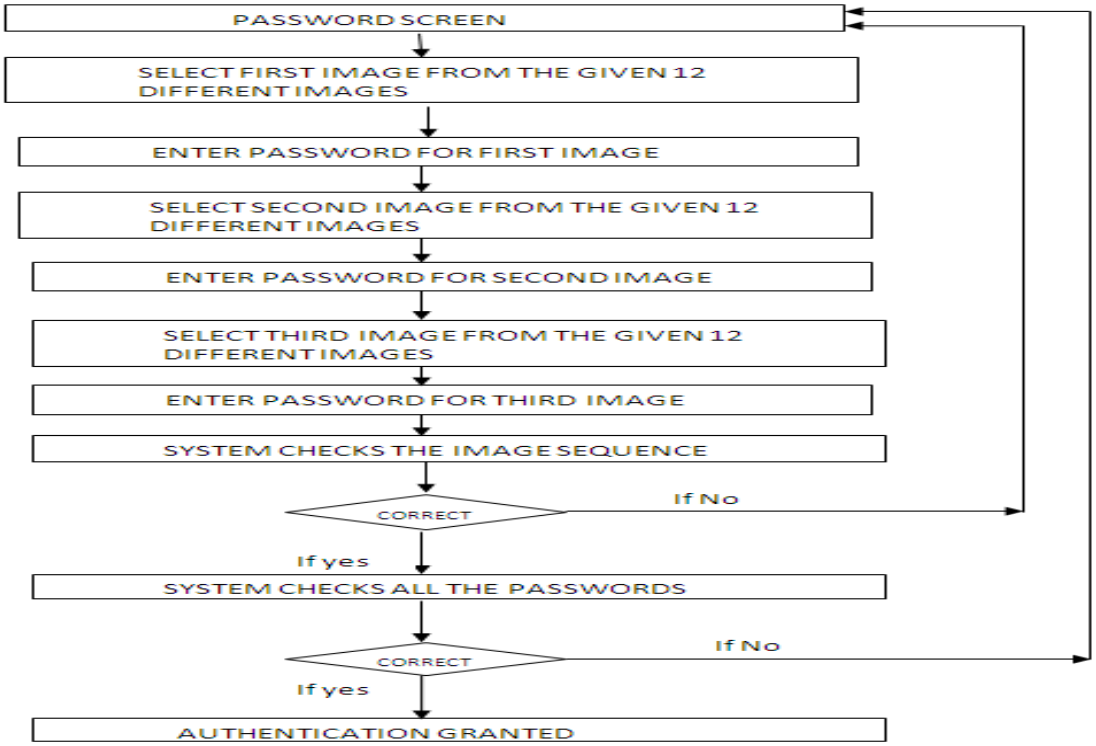

Figure 1: Flow diagram of proposed system

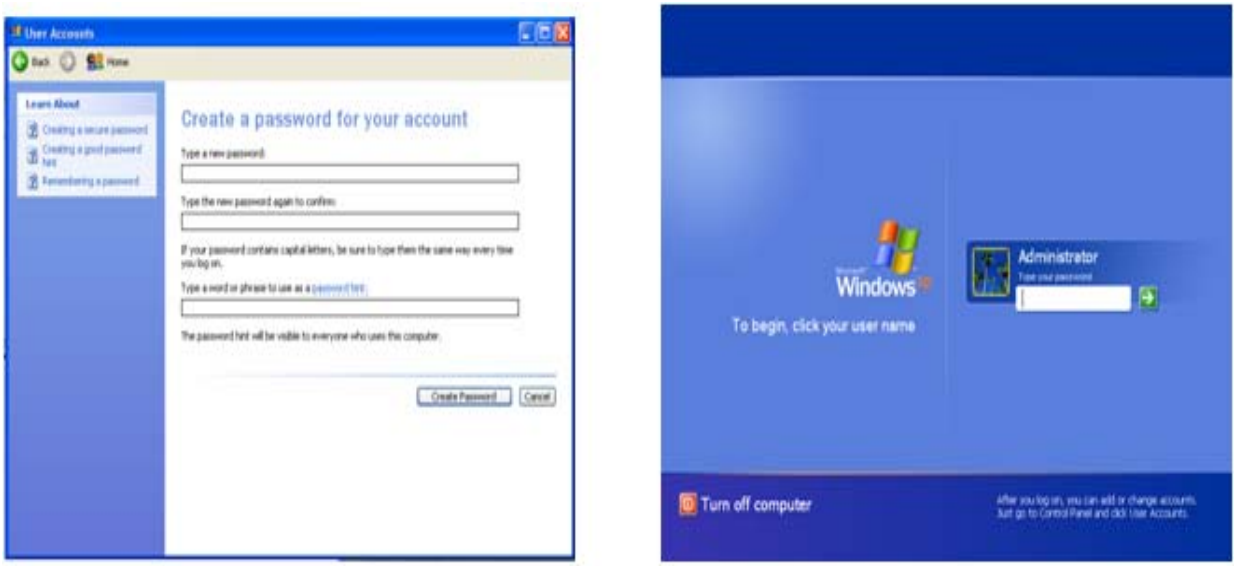

Figure 2: Diagram of Existing System

Figure 3: Diagram of Proposed System

Table1: Comparative analysis of existing and proposed system

S.No	Existing System	Proposed System
1.	In existing system user have to select only one textual password.	In proposed system user have to choose three different textual passwords.
2.	Authentication is based on just one password.	Authentication is based on three textual passwords.
3.	No image matching concept.	Authentication is based on three textual passwords.
4.	It is possible to hack a password with brute force attack or a little personal detail about the user.	This system is more secured because it is based on three textual password and a particular image pattern select by the user.
5.	It is less user friendly.	It is more users friendly.

IV. CONCLUSION

In today's world a user needs security and efficiency for his system, in current authentication system there are some drawbacks regarding to system security. Our system provides more security and efficiency to the user's system and it is more user friendly than existing system.

V. REFERENCES

[1]. Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Common Criteria Portal, September 2006, Version 3.1 Revision.

[2]. Password-Authenticated Group Key Agreement with Adaptive Security and Contributiveness Michel Abdalla 1, Dario Catalano 2, Céline Chevalier 1, and David Pointcheval 1 1 École Normale Supérieure, CNRS-INRIA, Paris, France 2 Università di Catania, Catania, Italy.

[3]. M. Abdalla, J.-M. Bohli, M. I. Gonzalez Vasco, and R. Steinwandt. authenticated key establishment: From 2-party to group. In S. P. Vadhan, editor, TCC 2007, volume 4392 of LNCS, pages 499–514. Springer, Feb 2007.

[4]. Typing Patterns: A Key to User IdentificationAuthor(s): Alen Peacock, Xian KE, Matthew Wilkerson Publication: IEEE Security & Privacy, Volume 2, Number 5 - Date: September 2004.

[5]. E. S. Raymond, The New Hacker's Dictionary, MIT Press, Cambridge, MA (1991)

[6]. Encryption Schemes Secure under Selective Opening Attack MIHIR BELLARE_ SCOTT YILEKy September 2008

[7]. R. Chellappa, C. Wilson,and S. Sirohey,"Human and machine recognisation of faces: A survey," Proceeding of IEEE, vol. 83, May 1995.

[8]. Graphical Password Authentication Using Cued Click PointsAuthor(s): Sonia Chiasson, Paul van Oorschot, Robert Biddle Publication: Proceedings of ESORICS 2007 - Date: September 2007.

[9]. A Second Look at the Usability of Click-Based Graphical Passwords Author(s): Sonia Chiasson, Robert Biddle, Paul van Oorschot .

[10]. The CIS Security Metrics Service, The Center for Internet Security (CIS), July 1, 2008, http://securitymetrics.org/content/attach/Metricon3.0/metricon3-kreitner%20handout.pdf.

