Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 4, April 2015, pg.1 – 4

RESEARCH ARTICLE

Randomise Password using 3D Environment Image

Ms. R. R. Tayade[#1], Prof. V. K. Shandilya[#2]

[#1] Dept.: Master of Engineering (I.T.) Sipna College of Engineering and Technology**,** Amravati (India)

roshani.meit@gmail.com

[#2] Asso. Prof. in Computer Science & Technology Sipna College of Engineering and Technology, Amravati (India)

vkshandilya@rediffmail.com

Abstract— 3D environment image used as a logical password is a new scheme of authentication. This scheme is based on a virtual three-dimensional environment image. We present a 3D virtual environment image where the user navigates and interacts with various objects and action from the virtual 3D environment image. The sequence of actions and interactions toward the objects inside the 3D environment constructs the user's logical password. The logical password specifies some keyword as a logical password. We combine graphical as well as textual password into one.

Keywords — Logical passwords, Textual passwords, Graphical passwords, 3D Virtual Environment image

I. INTRODUCTION

Textual passwords are the most common authentication techniques used in the computer world. Textual password has two conflicting requirements: passwords should be easy to remember and hard to guess and we are providing the same. The strength of graphical password depends on recall and reorganization of pictures more than words. Most graphical passwords are vulnerable for shoulder surfing attacks, where an attacker can observe or record the legitimate user's graphical password by camera. So, they create short, simple, and insecure passwords that are susceptible to attack. Which make textual passwords easy to break and vulnerable to dictionary or brute force attacks. Graphical passwords schemes have been proposed.

The 3-D environment image based password is a multifactor authentication scheme. So that, 3D environment image based password combine's number of existing authentication schemes into one three-dimensional virtual environment. The three-dimensional virtual environment consists of many items or objects. Each item has different responses to actions. The user actions, interactions and inputs towards the objects or towards the three-dimensional virtual environment create the user's 3D environment image based logical password. The 3D password gives users the freedom of selecting what type of authentication techniques they want to be performed as their 3D environment image based logical password. The 3D environment image based logical password has a large number of possible passwords because of the high number of possible actions and interactions towards every object and towards the three dimensional virtual environment.

Therefore we present our idea, the 3D environment image based passwords which are more customizable and very interesting way of authentication. Now the passwords are based on the fact of Human memory. Generally simple passwords are set so as to quickly recall them. The human memory, in our scheme has to undergo the facts of Recognition, Recalling

authentication. Once implemented and you log in to a secure site, the 3D environment image based password GUI opens up. This is an additional textual password which the user can simply put.

II. LITERATURE SURVEY

Blonder introduced the first graphical password schema. Blonder's idea of graphical passwords is that by having a predetermined image, the user can select or touch regions of the image causing the sequence and the location of the touches to construct the user's graphical password. [1]. Another recognition-based graphical password is Passfaces. Passfaces simply works by having the user select a subgroup of k faces from a group of n faces[2]. Another scheme is the Story scheme, which requires the selection of pictures of objects (people, cars, foods, airplanes, sightseeing, etc.) to form a story line. Davis et al. concluded that the user's choices in Passfaces and in the Story scheme result in a password space that is far less than the theoretical entropy. Therefore, it leads to an insecure authentication scheme [3].

PassPoint is a recall-based graphical password schema, where a background picture is presented and the user is free to select any point on the picture as the user's password (user's PassPoint)[4][5]. Draw a Secret, which is a recall-based graphical password schema and introduced by Jermyn et al. [6], is simply a grid in which the user creates a drawing. The user's drawings, which consist of strokes, are considered to be the user's password. The size and the complexity of the grid affect the probable password space. Larger grid sizes increase the full password space. However, there are limitations in grid complexity due to human error[7].

The three dimensional password is a new authentication methodology that combines recognition, recall, and biometrics, what you have, what you know, and what you are in one authentication system. The user navigates through a three dimensional virtual environment. The combination and the sequence of the user's actions and interactions towards the objects in the 125 three-dimensional virtual environments construct the user's 3D password [8][9].

III. PROPOSED SYSTEM

In this work we are implementing the authentication framework by using 3D graphical image as a password. This is very easy to remember instead of remembering a character, numbers and alphanumeric password. Also prevent the key logger software to catch the keystrokes and its monitoring.

In the following fig.1 shows the login process of the system in which user type user name i.e. email id of user and then system check the email id where it is right or wrong. Then for password there is a button i.e. check password after that user select the image and appropriate keyword for the particular action and object. If the password is correct then action granted otherwise not.

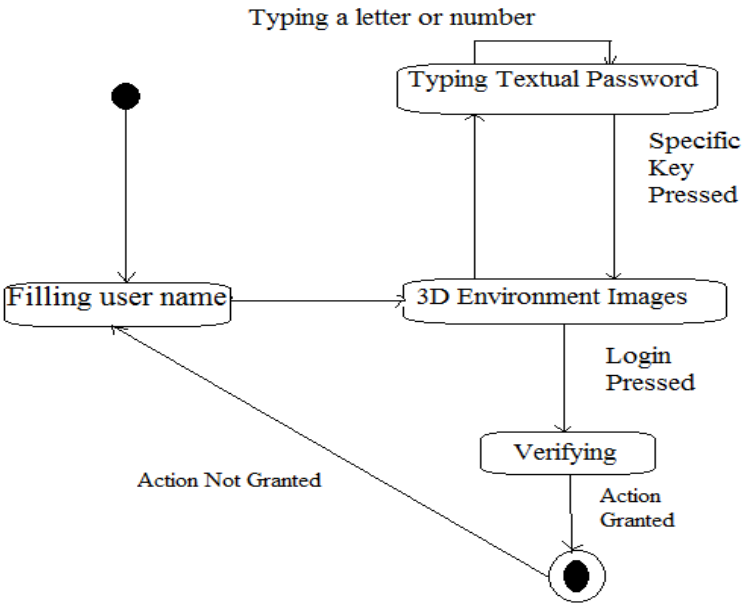

Fig.1 Login Operation Flow Chart

The system proposed the environment in which user interact in normal life. The user will select its convenient environment, and then selects its normal actions which he/she would like to perform. The implementations of modules are given in following section.

IV. MODULES

Three dimensional logical passwords is multi-factorial scheme. Multi-factorial means combination of all existing authentication scheme in one scheme. Different schemes are Textual password, Graphical password. In the paper different environment proposed by which user can registration. By using different environments user can select any environment will be the part of three dimensional passwords. In this paper mainly contain four modules at this stage and other under process. For accessing the system the user must followed the following steps. Modules are as follows,

a) Registration:

While constructing the logical password first the user registers himself by filling all fields, the registration form is consist of different field they are, full name field contain first name and last name of user who wish to register. Mobile number fields store the personal number of user, fax number, Email id provided as a user name into user name fields, and for password goes to next page i.e. next module.

b) Selection of 3D Environment Image:

Selecting one of the image from the three dimensional environment images list. After filling all fields in registration form the different environment are available so that user can select any environments. Now user can select any environment which will be part of his three dimensional password. Here different environment available users may select any one.

The environment in which user interact in normal life. The user will select its convenient environment, and then selects its normal actions which he/she would like to perform. Ex. First user will select room environment and then he will selects the action like opening the door then closing the door and at last opening window. For each particular action there is some keyword (numbers, alphabets, symbols) like for opening the door 1 2 will be the password, for closing the door 3 4 will be the password likewise for opening window 5 6 will be the password. It means user needs to enter this kind of sequence in the password block. So 123456 will be the main logical password for that particular user. In the next login session user only need to understand the logical sequence of action. But the keyword (numbers, alphabets, symbols) in every login of that user will change. In this way 3D graphical password provides authentication to the user.

c) Login

In login form is meanly consist of login name in which user have to mention the login name as an email id. After that it selects the environments which were selected by him at the time of registration. In selection of three dimensional environment image module form the user selects the first environment and selects the correct alphanumeric or symbolic keywords among the list for specific action and object. After the correct sequence and alphabet the user select the alphanumeric password. After that the recorded data field show 3d password which on the basis on how the user interact with different environment. In authentication process this recorded data match with the database if it's same then and then only the user will authenticate and it can access the system otherwise the access denied. At the time of registration the user have different environment lists.

d) Account Details

In this module user enter in main page in which it contain the user interactive other modules and these are follows,
Upload Document, Download Document which will provide user to upload and download files to the server or from the server and also provide felicity to share Documents among different users which are having account in the same.

V. SECURITY ANALYSIS

a) Timing Attack: In this attack, the attacker observes how long it takes the legitimate user to perform a correct sign in using the 3D image logical password. This observation gives the attacker an indication of the legitimate user's 3D image logical password length.

b) Key logger Software Attack: In this type of attack, keyboard record all data in key logger software. So, we used randomization of password at every login.

VI. CONCLUSION

The logical password in 3D environment image is a multi factor authentication scheme that combines the various authentication schemes into a one scheme. We used textual password, graphical password scheme into one. This scheme will give more ease to user to remember his password as well as here we are storing logical password instead of physical password. This password scheme will provides protection from a key logging software's. Which mainly design to store key stokes of the user keyboard. Further working of paper is under process.

REFERENCES

[1] Darren Davis, Fabian Monrose, and Michael K. Reiter. On user choice in Graphical Password Schemes. In Proceedings of the 13th USENIX Security Symposium, San Diego, August, 2004.

[2] Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, Nasir Memon. Authentication using graphical passwords: effects of tolerance and image choice. In the Proceedings of the 2005 symposium on Usable privacy and security, Pittsburgh, Pennsylvania, July 2005.

[3] Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, Nasir Memon. Authentication Using Graphical Passwords: Basic Results. In the Proceedings of Human-Computer Interaction International, Las Vegas, July 25-27, 2005.

[4] Ian Jermyn, Alain Mayer, Fabian Monrose, Michael K. Reiter, And Aviel D. Rubin. The Design And Analysis Of Graphical Passwords, In Proceedings Of The 8th Use-Nix Security Symposium, August, Washington Dc, 1999.

[5] Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, Nasir. Memon. PassPoints: Design and longitudinal evaluation of a graphical password system', International Journal of Human-Computer Studies (Special Issue on HCI Research in Privacy and Security), 63 (2005) 102-127.

[6] J. Thorpe, P.C. van Oorschot. Graphical Dictionaries and the Memorable Space of Graphical Passwords. USENIX Security 2004, San Diego, August 9-13, 2004.

[7] Fawaz A Alsulaiman and Abdulmotaleb El Saddik, A Novel 3D Graphical Password Schema VECIMS 2006 – IEEE International Conference on Virtual Environments, Human-Computer Interfaces, and Measurement Systems La Coruña - Spain, 10-12 July 2006.

[8] Muneshwar R.N. and Sonkar S.K, High Degree of Security Provided By Three- Dimensional Virtual Environment ISSN: 2277-3754 ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 8, February 2013.

[9] C. A. Kurjekar, and S. D. Tatale, S. M. Inzalkar Analysis Of Three Dimensional Password Scheme ISSN 2229-5518 International Journal of Scientific & Engineering Research, Volume 4, Issue 12, December-2013.

