Volume 4, Issue 1, January 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

3d Password –A Secure Tool

Research Scholar,Banita Chadha*
Galaxy Global Imperial Technical Campus
Computer Science Department
Kurukshetra University, India

Dr. Puneet Goswami
Galaxy Global Imperial Technical Campus
H.O.D.Computer Science Department
Kurukshetra University , India

Abstract— To protect our system from intrusion is to use alphanumeric username as well as password. Hacking is very common now days. It becomes very easy for hackers to hack computer system. When user will type password the hacker can trace the number of keystrokes which the user do. By using this hacker can easily hack user login and password? If we talk about the textual password the it must be as easy such that user will remember the same. In this paper we will calculate the probability of finding the password[4] .Using 3D password make the hacker difficult to hack computer system. It includes various strategies in various fields.3D includes the values along x axis, y axis, and z axis. This paper presents the strategy based on 3D virtual environment.3d includes various services like biometrics, ATM, Smart cards etc.

Keywords— Introduction, Graphical Password, Textual Password, 3D Password.

I. INTRODUCTION

Authentication is required while user make login by using its unique username as well password. It is implemented n case of textual password as well as graphical password. Textual password includes only text i.e. the password in textual case includes only text format. Which the user generally types the date of birth or name or any easy text which user can remember (memorable). Incase of textual password there is more probability of hacking because the text format is like full name, date of birth etc. Authentication includes three categories:

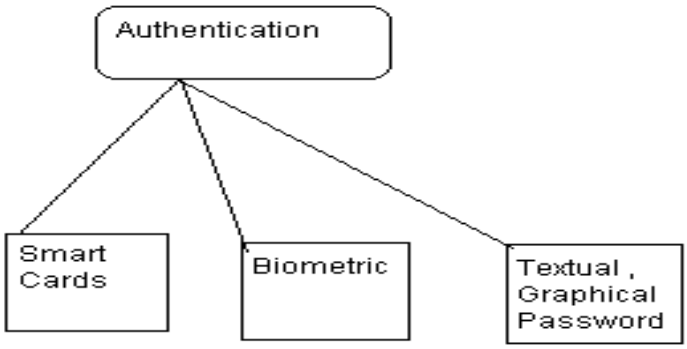


Fig.1 Categories of Authentication

In above figure there are three categoris of Authentication which includes smart cards which is again proceed with the PIN number which is not known to any one else. Another category is biometric which include the scanning if fingerprint which is unique.or it may be of retine scan which is again unique and is used now adays. Boimetrics are used to reduce the redundancy or duplicacy of user identification. Because no two users may have same finger prints.Last section in authentication is textual and graphical password.Textual password based on text and the graphical password is based on selection of images in an appropriate sequence which is again have possibility to hacke by hackers. Textual password include the number of text and it may be easy and shot i.e. atleast 8 characters long password in text format is required. But it may be hacked because of easy password one can easily hack the user login because the password is memorable by user and with the help of shoulder surfering attack hacker can guess ones password by reading the number of keystrokes by user while login.

guidelines, please contact the journal publications committee as indicated on the journal website. Information about final paper submission is available from the conference website.

II. TEXTUAL PASSWORD

Textual password is easy to use and also it is easy for hackers to hack user system with tracing user password. In some cases if the user login on system and somehow system may automatic shut down. Then it doesn't mean that user wills

automatically logout from its account. User must first check for its surety that whether user logged out or not by restarting the system. Also there are various methods to hack computer system out of which some cases are as follows:

a) Automatically shut down of system doesn't results to the logout of user. Meanwhile hacker will turn on system and surf the user site as it was not logged out.
b) Textual password can be copied with the help of shoulder suffering attack. Which can be implemented by counting the keystroke done by user?
c) Textual password is easy to use and of short length of at least 8 characters in length. Which hacker can easily guess because it may be the full name, place of birth or can be date of birth of user which is memorable by user.

Textual password along with graphical usage is also implemented in 1999 in USENIX associations . In this it is implemented that how any textual password is implemented in terms of graphical password. It can be done with the help of total number of text named as 1, 2, and so on .e.g. a textual password potato consists of 6 letters i.e.

$\pi(1) = p, \pi(2) = 0, \pi(3) = t, \pi(4) = a, \pi(5) = t, \pi(6) = 0.$

III. GRAPHICAL PASSWORD

Graphical password is secure as textual password is. Graphical password is based on textual password. With the help of textual password we can construct the graphical password. It basically implemented in grid format. That grid may be of 4*4 size i.e. 4 sections along x axis and 4 sections along y axis. When the user type any textual password then with the help of shoulder surfing attack one can construct the graphical password of actual textual password. It can be firstly represented as the imagination of hacker. Once the graphical representation is correct one can easily access the user's login.

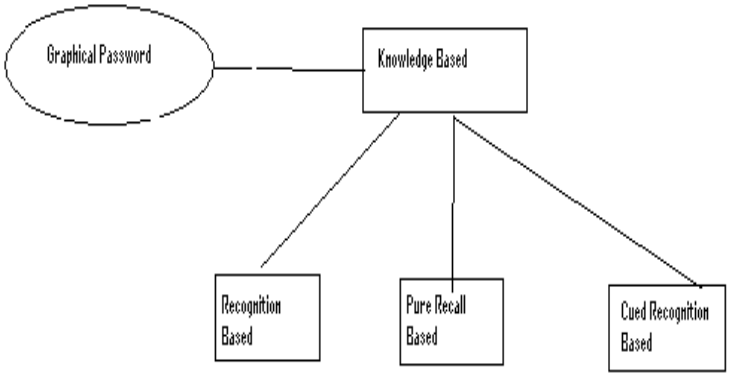


Fig.2 Graphical Password

The very first step in graphical password is recognition bsed . It deals with the study of recognition that whether the user will recognizez its account or not.

Next step is pure recall based.It includes various passpoints as used and implemented in Convex hull scheme[6]. Passpoints are the various points which are used to create one particular shape . The shape which the user enetred while login must be correct to access the account.Passpoints are the best example of pure recall based recognition in terms of graphical password.Another strategy in graphical representation is DAS.It is based on the cancept of deep sceret access of password.

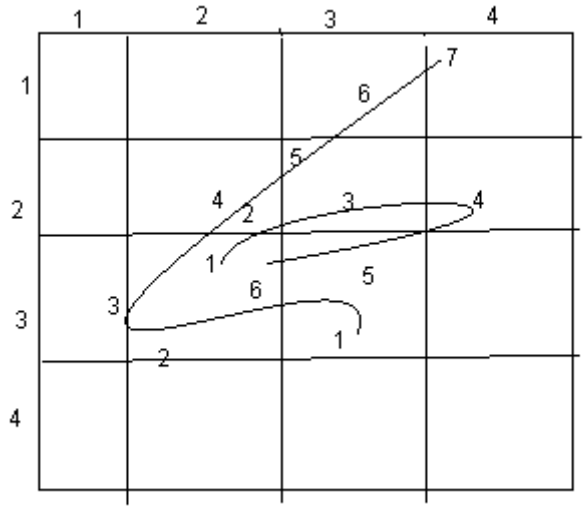


Fig.3: Graphical representation

Above figure represents the two graphical representations of two passwords which user wants to type. It can be implemented in terms of coordinates. There is one new approach for the same i.e. pen up approach which include the coordinates other then keystroke typed by user to make the password correct.This is the case when user generally forget its password and type two different password as indicated in 4*4 grid. the very first password is having coordinates as:

(3,3,) (3,2) (3,1) (2,2) (2,3) (1,3) (1,4)

There are 7 sections because there are 7 keystrokes in user password. i.e. we can detect the actual number of text user by user in password. In above fig. There is a contradiction in one coordinate i.e. whether it is (3, 2) or (3, 1). In this case we generally find the possibility and percentage of keystroke present in which quadrant. Which is clearly identified in graphical representation?

Similarly it can be implemented in second case for graphical password. It includes 6 keystrokes having different quadrant. Graphical password is based on knowledge. We can further elaborate this section in terms of graphical password search method. It deals with the number of characters used by user in its password. It may consist of upper case or may be having lower case. While calculating the probability we first add the both case i.e. 26 alphabets in upper case , 26 alphabets in lower case. 10 is the total number. And rest 30 is the special characters.i.e.

Total number of pictures in each round = 52

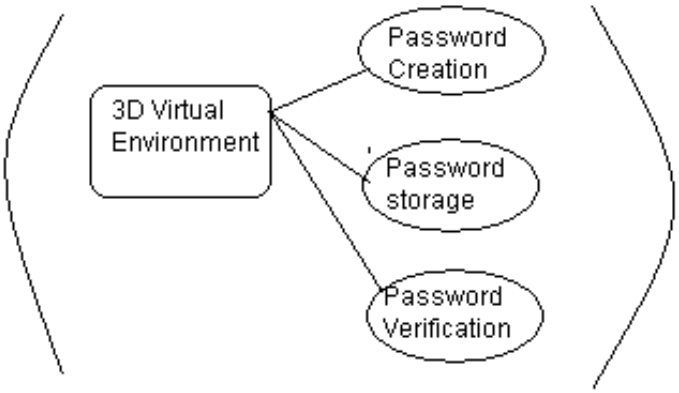
If the password is in upper case e.g. **TRUTH**

Then it can be implemented as: 5^52 [3] .Where 5 is the total number of characters in password. And 52 is the pictures in round. Thus total number of cases are =66 where 26 are upper case characters, 10 are the numbers, 30 are the special characters. We generally set the length of password as $L_{max.}$ This is the maximum limit of the password or we can say the limit of user password in terms of textual or graphical password. The password may be less that or equal to the $L_{max.}$[4]

The basic idea behind the graphical representation is that user may first login its own account along with textual password. After entering the textual password user may enter the graphical password. If the graphical password is correct the it can avail various services such as Uploading, Save Delete, open a file or any data. And after processing completes user may log out from its account. Graphical password can be implemented in terms of images e.g. if there are more than 200 images on screen then user will select the appropriate images in exact pattern which user already done at the time of creation of password. It is as safe as textual password because of its continuous sequence of selecting images. It may be some how not capable to overcome the shoulder surfing attack. Because in shoulder suffering attacks one can easily copy the sequence of selecting images out of 200 images on to screen. But it doesn't result to the concept that interaction of object 1 is equal to interaction of object 2. In case of virtual uniqueness it is observer that interaction of object 1 ≠interaction of objects 2 and vice versa.

IV. 3D – PASSWORD

3D is based on virtual environment. It includes the 3 axis x, y, and z axis. That is the password should be in three axis along x,y,z axis. her is a term of virtual uniqueness. It includes the concept of identification. E.g. if in a certain place there are 10 houses of same color and similar location the user cant judge that which one is visited and which is not visited. This is due to the ideal or similar lookup of the different houses. This result in virtual uniqueness.Passaction is the term where user will perform various actions on virtual environment and this virtual environment is 3D virtual environment.



3D Virtual environment based on three concepts :

i) Password creation: It includes the number of text in case of textual password e.g. say length 8 i.e. here L_{max}=8.[4] Password creation in text and graphical representation includes easy and simple to use which is memorable by user.

ii) Password storage: This comes after completing the step of password creation. If user enters an appropriate password which is memorable to user then user will store the entered password. This password storage deals with the limitation of 3 case . If user somehow forget password the there are maximum three chances to enter password by user. System will not log in until it matches with the created password.

iii) Password Verification: This is the last stage of password registry. It includes the check of user whether the present user is valid to access the account or not. For password verification system will ask some personal queries which is known only to the user but not the hacker.e.g. Date of birth, name of school. Place of birth etc. After verifying the actual information given by user to system it can access the same account further.

Above three concepts are valid in textual , graphical password as well as 3D password.

3D password is very easy to use and is somehow free from shulder surfeing attack.It deals with the random selection of various images which is not viewed by the hacker and thus it is free from hacking at some level.3D password is basically the combination of all the textual password , graphical password and may includes various services such as biometrics, Smart cards.

In term of biometrics user will login with the help of scanning of either fingerprint, thumb print or retina scan etc. This identification is ideal and away from shoulder suffering attack.

V. CONCLUSION

In this paper, we explored the concept of Textual, graphical and 3D password. For future work from this paper we can implement the 3D password using any object such as pass point, images or and activity which must be memorable to the user. This paper also concludes that 3D password is somehow free from shoulder suffering attack and is free from hacking if compared with textual password or graphical password because there is no appropriate sequence of selecting of images as in used in graphical images.

REFERENCES

[1] Fawaz A.Alsulaiman and Abdulmotaleb El Saddik Senior member IEEE:3d Password for more secure authentication Sep:2008
[2] Ali Mohamed Eljetlawi, Norafida Ithnin 2008, Graphical password: prototy usability survey
[3] IJARET Vol.1 Issue VII.August 2013 ISSN 2320-6802.
[4] IJCSITS ISSN:2249-9555 IRACSE April 2012.
[5] New era of authentication:3d Password Volume 1 Issue 5 November 2012
[6] Graphical Password Authentication Based on polygon Visualization IJERA ISSN:2248-9622.

