Account Security using Randomized 3D Environment Image

Ms. R. R. Tayade [#1], *Prof. V. K. Shandilya*[#2], *Prof. K. R. Ingole* [#3]

[#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).

[#3] Asst. Prof. in Computer Science & Technology
Sipna College of Engineering and Technology,
Amravati(India)(kringole@rediffmail.com).

Abstract—***3D environment image with random textual password is a new scheme of authentication. This scheme is based on a virtual three-dimensional environment. To be authenticated, I present a 3-D virtual environment where the user navigates and interacts with various objects. The sequence of actions and interactions toward the objects inside the 3-D environment constructs the user's 3-D password. The 3-D password can combine most existing authentication schemes such as textual passwords, graphical passwords into a 3-D virtual environment. The design of the 3-D virtual environment and the type of objects selected determine the 3-D password key space. The objects and actions contain in 3-D virtual environment specify some random keyword for each at every login. This provides more authenticated technique.***

Keywords — 3D passwords, Textual passwords, Graphical passwords, authentication, 3D Virtual Environment.

I. INTRODUCTION

Current authentication systems suffer from many weaknesses. Textual passwords are commonly used; however, users do not follow their requirements. Users tend to choose meaningful words from dictionaries, which make textual passwords easy to break and vulnerable to dictionary or brute force attacks. Many available graphical passwords have a password space that is less than or equal to the textual password space. Smart cards or tokens can be stolen. Many biometric authentications have been proposed; however, users tend to resist using biometrics because of their intrusiveness and the effect on their privacy.

Now a day's 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. Many graphical passwords schemes have been proposed. 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. The 3-D password is a multifactor authentication scheme. So that, 3D password combines 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 password. The 3D password gives users the freedom of selecting what type of authentication techniques they want to be performed as their 3D password. The 3D 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.

Many graphical passwords schemes have been proposed. The strength of graphical passwords comes from the fact that users can recall and recognize 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. Currently, many types of graphical passwords are under study yet, it might be some time before they can be applied in the real world.

The 3D password combines all 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 creates the user's 3D password.

The 3D password gives users the freedom of selecting what type of authentication techniques they want to be performed as their 3D password. The 3D 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.

II. LITERATURE SURVEY

Many graphical password schemes have been proposed. 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. After Blonde, the notion of graphical passwords was developed. Many graphical password schemes have been proposed [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. For authentication, the system shows m faces and one of the faces belongs to the subgroup k. The user has to do the selection many times to complete the authentication process [2]. A study concluded that the selection of faces in PassFaces[2] can be affected by the attractiveness, gender and race of the selected face which results in an insecure scheme. 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].

The graphical password schema of Blonder is considered to be recall based since the user must remember selection locations. Moreover, PassPoint [3] [4] 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). Draw a Secret, which is a recall-based graphical password schema and introduced by Jermyn et al. [4], 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. It becomes very hard to recall where the drawing started and ended and where the middle points were if we have very large grid sizes.

Today there is an increasing recognition that security issues are also fundamentally human computer interaction issues. Authentication is the process of determining whether a user should be allowed access to a particular system or resource. It is a critical area of security research and practice. Alphanumeric passwords are used widely for authentication, but other methods are also available today, including biometrics and smart cards. However, there are problems of these alternative technologies. Biometrics raise privacy concerns and smart cards usually need a PIN because cards can be lost. As a result, passwords are still dominant and are expected to continue to remain so for some time [5].

The three dimensional password (3D 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 [6].

Therefore, the user can walk in the virtual environment and type something on a computer that exist in (x1 , y1 , z1) position, then walk into a room that has a white board that exist in a position (x2 , y2 , z2) and draw something on the white board. The combination and the sequence of the two actions towards the specific objects construct the user's 3D password [6].

Users can navigate through a three-dimensional virtual environment that can contain any virtual object. The first step in building a 3D password system is designing the three-dimensional virtual environment. The selection of what objects to use, locations, and types of responses are very critical tasks. The design affects the strength, usability and performance of the 3D password. User actions, interactions and inputs towards the objects and towards the three-dimensional virtual environment are mapped into a sequence of three-dimensional coordinates and actions, interactions and input [7].

Two 3D passwords are equal to each other when the sequence of actions towards every specific object are equal and the actions themselves are equal towards the objects. The objects are distributed in the three-dimensional virtual environment. Every object has its own (x,y,z) coordinates. Assume the user can navigate and walk through the three-dimensional virtual environment and can see the objects and interact with the objects. The input device for interactions with objects can be a mouse, a keyboard, styles, a card reader, a microphone…etc [8].

Yet traditional alphanumeric passwords have drawbacks from a usability standpoint, and these usability problems tend to translate directly into security problems. That is, users who fail to choose and handle passwords securely open holes that attackers can exploit. The "password problem," as formulated by Birget in, arises because passwords are expected to comply with two conflicting requirements, namely:

- Passwords should be easy to remember, and the user authentication protocol should be executable quickly and easily by humans.
- Passwords should be secure, i.e., they should look random and should be hard to guess; they should be changed frequently, and should be different on different accounts of the same user; they should not be written down or stored in plain text.

Meeting these conflicting requirements is almost impossible for humans, with the result that users compensate by creating weak passwords and handling them in an insecure way. Many problems that users have with alphanumeric passwords are related to memorability of secure passwords. In an attempt to create more memorable passwords, graphical password systems have been devised [9].

Table of Work to date:-

Sr. No	Author name	year	Problem
1	Draw a Secret (DAS) which is a recall-based graphical password schema and introduced by Jermyn	1999	limitations in grid complexity due to human error.
2	Blonder introduce Graphical password Schema	1996	shoulder suffering attacks and less protected
3	Davis proposed grapical password i.e. user's choices in Passfaces	2004	password space that is far less than the theoretical entropy
4	Davis proposed Story scheme in graphical password	2005	password space that is far less than the theoretical entropy
5	3D password authentication methodology that combines recognition, recall, and biometrics	2006	complexity is very high and lots of external devices are used which will be reduces reliability of system

III. PROPOSED SYSTEM

Here, In this work we are implementing the authentication framework which is working on 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.

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. 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.

IV. CONCLUSION

The 3D password is a multi factor authentication scheme that combines the various authentication schemes into a single 3D virtual environment. The virtual environment can contain any existing authentication scheme or even any upcoming authentication scheme by adding it as a response to actions performed on an object. Therefore the resulting password space becomes very large compared to any existing authentication schemes.

The design of the 3D virtual environment the selection of activities and objects inside the environment and the activities and object's type reflect the resulted password space. It is the task of the system administrator to design the environment and to select the appropriate object that reflects the protected system requirements. Designing a simple and easy to use 3D virtual environment is a factor that leads to a higher user acceptability of a 3D password system. The choice of what authentication scheme will be part of user's 3D password reflects the user's preferences and requirements.

The 3D Passwords are also useful in critical systems and resources. Critical systems such as military facilities, critical servers and highly classified areas can be protected by 3D Password system with large three-dimensional virtual environment and a small three-dimensional virtual environment can be used to protect less critical systems such as handhelds, ATM's and operating system's logins.

V. 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.