Passaction: A New User Authentication Strategy Based on 3D Virtual Environment

Praseeda K Gopinadhan
MTech Student, IGNOU

Renjith P R
Department of Computer Science
Rajagiri College of Social Sceinces

Biju Abraham Naremparambil
Computer Science Department,
Rajagiri School of Engineering and Technology

Abstract— **User authentication is a key security process that either allows or denies access to a system or resource depending on the credentials presented. The credentials that the user presents may be classified under three main categories - what you know (token-based), what you have (knowledge-based), and who you are (biometric-based). The token based authentication system is a two factor system makes use of the pin number and the physical card to operate it. The card and pin number should be secured enough and memorisable. Text and graphical passwords comes under knowledge-based authentication system.**

Graphical passwords reduces user's burden to remember different passwords instead it experiences actions and reactions. Iris scanner, fingerprint recognitions, palm recognition are some of the biometric based authentication system. Its intrusiveness and equipment cost make them down and difficult to use with real world. This paper proposes a new virtual password authentication system based on a virtual three-dimensional environment. Three dimensional objects are propagated in the virtual environment. The users navigate through the 3D environment and perform a sequence of actions with these objects (called as passaction) . This sequence of interactions will create the virtual 3D password. The design of 3D environments and the type of object selected determine the password space.

Keywords **-Security, User Authentication, Graphical Password, Virtual Password. Passaction**

INTRODUCTION

Lack of security has become a major concern, given the occurrence of attackers, hackers, crackers, scammers and spammers. A key area in security research and practice is authentication, the determination of whether a user should be allowed to access a given system or resource. In general the human authentication system can be classified into recognition based, knowledge based and recall based authentication systems. The graphical password strategy comes under knowledge based can be divided into Recognition based, Pure-recall based and cued recognition based authentication systems [1]. The choice of alphanumeric password is troublesome as a strong password is very difficult to remember and a weak password is very easy to attack. The invention of graphical password [2] (e.g. passpoints, passgo, draw a secret) solved the above issues to an extent. But those algorithms need to have a trade-off between limited password space and complexity. Most of the graphical password systems are vulnerable to shoulder surfing attacks, where a third party can observe and record the legitimate user"s password.

LITERATURE SURVEY

Now days the IT industries are fast going and people living in an electronic world, where all their needs are met through internet. Obviously different authentication mechanisms have emerged and came into existence. In this situation people started to consent one of the human authentication methods for their secure web services. These authentication methods are based on what you know, what you have and finally what you are.

Textual passwords are the widely used, easy to implement and common. The password should be easy to remember, user authentication protocol should be executed quickly and it should be secure. It is a great burden to select a good password. Selecting a good password may face restriction on at least eight characters long and it is vulnerable to dictionary attack if any meaningful words are used.

Token based techniques, such that ATM cards, smart cards are widely used. This is also working with the help of knowledge-based mechanism to enhance security. With the ATM card magnetic strips details the user should enter four-digit pin number for secure access to the transaction.

Many biometric schemes have been proposed; fingerprints, palm prints, hand geometry, face recognition, voice recognition, iris recognition, and retina recognition are all different biometric schemes. Each biometric recognition scheme has its advantages and disadvantages based on several factors such as consistency, uniqueness, and acceptability. One of the main drawbacks of applying biometrics is its intrusiveness upon a user"s personal characteristic. Moreover, retina biometrical recognition schemes require the user to willingly subject their eyes to a low-intensity infrared light. In addition, most biometric systems require a special scanning

device to authenticate users, which is not applicable for remote and Internet users. With effect of all these, it is highly expensive to implement and consume more time to authenticate.

However the knowledge based mechanism is the widely use one. It can be of text based or picture based. Blonder‟s [3] ideas about graphical password system were the starting of the graphical password era. In which predefined image positions are selected at the registration stage. Then applying a recall based techniques to reproduce something that selected earlier at registration stage. Later Dhamija and Perring [4] introduced a new method based on hash Visualization. In which the user is asked to select number of images from a set of random pictures. Later the user will require identifying preselected images in order to be authenticated.

OVERVIEW OF PROPOSED SYSTEM

Graphical password schemes are the alternative to the alphanumeric or text based password system. The simplicity to remember graphical passwords is the advantage of this over normal text passwords. Consider a situation where we want to perform some web-services online. The user is starting the normal login procedures at his/her desk computer and the co-workers may see the computer and observing the graphical password. This emphasis that the existing graphical password system is vulnerable to shoulder surfing attack. Later passpoints are introduced; where passwords are the selection of certain areas in the 2D scene. It started with the user to select a predefined area on digital images. Similarly pass objects [5] make up with invisible boundaries and get authenticated. All these graphical password systems provide a limited password space and vulnerable to shoulder surfing attacks. Other 3D graphical password systems are compromising recognition-based, recall-based and token-based graphical password systems [6]. In which the user is about to choose any of the authentication mechanism virtually. Depending upon the choices it also making burden to remember a password or text, remember the exact dimension of the secret draw and passpoints. The proposed system is completely three-dimensional and creating an effective password space over 2D.The idea behind the proposed 3D graphical password system is, Pass-actions where the user does a set of actions on a 3D virtual environment. These actions are recorded, encrypted and stored by using watermarking for authentication. The proposed method has 3 phases – password creation, password storage and password verification.

3D virtual environment system

The effective designing of virtual world increases the probability of number of passwords. The designing phase of this is depending upon the requirements and security features of the system. In proposed virtual world system a three be [1...G] × [1...G] × [1...G]. The virtual objects are scattered over the virtual world and each will be having their own properties. It is important to specify the properties of the objects at the 3D environment design. The individual object constitutes a single pixel or a number of pixels to represent it. Every object coordinates (x,y,z) will be point out particular location in the virtual world. The things to be considered is

A. Physical world to virtual world correspondence

The physical to virtual world correspondence defines a single common space, where an action taken by an end-user affects objects within the virtual world and where any activity by objects in the virtual world affect the end-user's view. This is same as we are performing with real time object in real world. The original world space is represented using a virtual environment.
dimensional coordinate system is used and its resolution can

B. Virtual uniqueness and the type of the objects

Every virtual object or item in the 3-D virtual environment is different from any other virtual object. The uniqueness comes from the fact that every virtual object has its own attributes such as position, size and properties. Thus, the prospective interaction with object 1 is not equal to the interaction with object 2. However, having similar objects such as 20 computers in one place might confuse the user. Therefore, the design of the 3-D virtual environment should consider that every object should be distinguishable from other objects. A simple real-life example is home numbering. Assume that there are 20 or more homes that look like each other and the homes are not numbered. It would be difficult to distinguish which house was visited a month ago. Similarly, in designing a 3-D virtual environment, it should be easy for users to navigate through and to distinguish between objects. The distinguishing factor increases the user‟s recognition of objects. Therefore, it improves the system usability.

C. Password space and number of objects

The three dimensional password spaces can be calculated by considering all the possible actions and interactions towards the virtual objects in the environment. With reference to the paper [6], [7] the length of the graphical password can be L_{max}. The probability of graphical password to exceed the size than L_{max} is zero. To measure the 3-D password space, we will calculate $\Pi (L_{max},G)$ on a 3-D virtual environment that has the space $G \times G \times G$) for a 3-D password of a length (number of actions, interactions, and inputs) of L_{max} or less.

In the following expression, AC represents the possible actions toward the 3-D virtual environment, where the following expression represents total number of possible 3-D passwords of length L_{max} or less:

$$\prod(\mathbf{Lmax}, G) = \sum_{N=1}^{N=Lmax} \left(m + g(AC)\right)^N$$

The possible number of objects for a virtual world is related to the size of the 3D environment. It can be let O_{max}. and the possible number of actions and interactions are

$$m = \sum_{i=1}^{i=Omax} h(Oi, Ti, xi, yi, zi)$$

Where xi = xj , yi = yj , and zi = zj , only if i = j. The design of the 3-D environment will determine the value of O_{max}. The variable m represents all possible actions and interactions toward all existing objects O_i. However, g (AC) counts the tot al number of actions and inputs toward the 3-D virtual environment, whereas m, as we mentioned before, counts the actions and interactions toward the objects. An example of g(AC) can be a user movement pattern, which can be considered as a part of the user's 3-D password. The function

h(Oi,Ti,xi,yi,zi)= f(Oi,Ti,xi,yi,zi)

is the number of possible actions and interactions toward the object O_i based on the object type Ti. Object types can be the response to the user depending upon the action.

Implementation Details

In this, a simple 3D virtual environment having large password space since all the items inside the virtual environment is moving. Therefore, to ensure high user acceptability, the user's freedom of selection of items is important. The function f is determined from the object type. It counts the possible actions and interactions can be performed with the object. For example the black board of size n[redacted] located in object space (x0, y0, z0) of type textual password will respond as we were writing on it, f will count the possible locations where we can be write, which is around (n*m) possibilities. As we mentioned before, an object type is one of the important factors that affects the overall password space. Therefore, higher outcomes of function f mean larger 3-Dpassword space size. From the previous equations, we observe that the number of objects and the type of actions and interactions determines the probable password space. Therefore, the design of the 3-D virtual environment is a very critical part of the 3-D password system.

Algorithm for Proposed System

The proposed system can be implemented with three stages. The initial stage is the predominant one, which requires intense use with the objects in the environment [8]. The 3D virtual environment must be responsive enough to set the password. The real life situations will be having high responsive rate as it is using every day and it won't be a forgettable one. The three stages of this algorithm are Password creation stage, Password storage case and password verification stage. The explanation is given below.

a. Password Creation Stage

1. The user is asked to select the virtual environment, which is familiar to the user. It is selected from the virtual environment gallery of server.
2. As shown in fig: 1 the user has to perform sequence actions and interactions with the selected objects in the virtual environment. These details regarding selected object will be recorded. A new linked list is created in which each node will contain data for one object.
3. This sequence of value is used as the graphical password for the user.

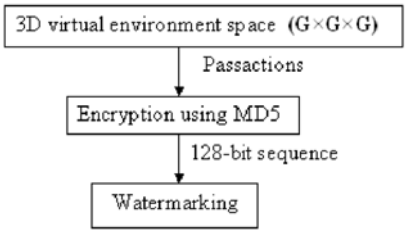

Figure 1: Password creation

b. Password Storage Stage

1. MD5 algorithm is used for the authentication purpose. The linked list is stored in a buffer where padding and appending is done to make its length 128 bits.
2. 128-bit sequence is generated by MD5 algorithm.
3. User selects an object in the virtual environment, where password can be stored.
4. As user click on store the password, the 128-bit sequence generated by MD5 is watermarked with the object selected by the user.

c. Password Verification Stage

1. The user should select the same virtual environment that has been chosen at the registration time.
2. User selects an object in the virtual environment, where password was stored and extracting from the object.
3. The user needs to repeat the same sequence of user‟s actions and interactions towards the selected object in the virtual environment 3D for making the password.
4. This new linked list link list is appended and padded to send as an input for MD5 algorithm.
5. The new MD5 128 bit string is compared to the 128 bit MD5 value is extracted from the object as shown in fig: 2. If there is any matching the login will be successful.

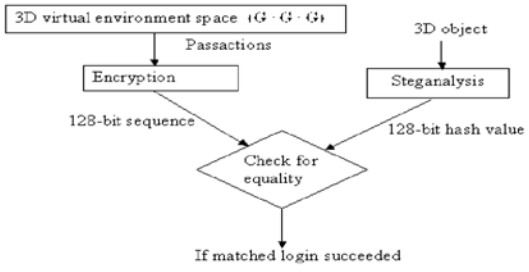

FIGURE 2: PASSWORD VERIFICATION

EXPERIMENTAL RESULTS

The virtual library shown in the figure 3 having shelves and books. From this 3D environment we can take and return the books which are needed. It can be extended to support automatic library functions for increasing the password space of the system. Here shows the importance of alternative 3D environments.

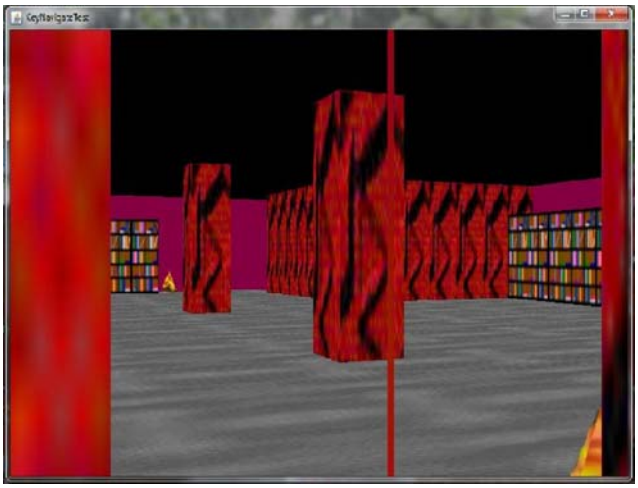

FIGURE 3: VIRTUAL ENVIRONMENT HAVING SHELVES, BOOKS AND PILLOWS

SECURITY ANALYSIS

As the graphical passwords are not being used widely in any of the web services. It is somewhat difficult to identify the threats related to it. This is one of the secured authentication mechanisms, which require more research works to make it into existence. Here we briefly exam some of the graphical password threats and try to do a comparison with text-based passwords.

RESISTANCE TO SHOULDER SURFING ATTACK

Even though the graphical password is easily memorisable and simple to use with. But its emphasis threat is the shoulder surfing attack. Graphical passwords are vulnerable to shoulder surfing attack [11], [12]. Shoulder-surfing attack takes place when an authorised user is being monitored by a person and remarks the legitimate user's password, or the authorised user is being observed over his shoulder directly for the password, In proposed system the user could navigate through the 3D environment and doing actions as per his/her demand. Additional security is providing by reducing the tolerance [9], [10] as well as the reducing size

Attacks	Text-Based	Graphical password
Brute Force Attack	The possible password space is 94 ^ n, where n is the length of password and 94 is the number of printable characters.	It needs The attack programs to automatically generate accurate mouse motion and possible actions and reactions to an object are large in 3D.
Dictionary Attacks	Dictionary attack is possible with text-based passwords	Graphical passwords involve mouse input instead of keyboard input
Guess password	Vulnerable to weak passwords that can be easily guess.	Difficult to guess the actions towards the object and it depends on the user.

TABLE 1: COMPARISON OF DIFFERENT PASSWORD ATTACKS

of the mouse point. When the user navigates through the password selection area the mouse pointer will be a small one so it could not be easily recognisable. The output obtained from the action will be encrypted and watermarked with another object. So that even if the sequence of action is recorded the attacker has to identify the watermarked object in the 3D environment.

REFERENCES

[1] Xiaoyuan Suo, Ying Zhu, G. Scott. Owen, 2005 Graphical *Password : a survey,* Computer Security Applications Conference 21st Annual.

[2] Wiedenbeck S, Waters J, Briget J.C, 2005, *Passpoints: Design and longitudinal evaluation of a graphical password system"*. International Journal of Human-Computer Studies, vol.63,pp.102-127

[3] Greg E. Blonder, *Graphical Password*, United State Patent 5559961, September 1996.

[4] Rachna Dhamija, Adrian Perrig, Déjà Vu: *A User Study Using images* for Authentication. In the 9th USINEX Security Symposium, August 2000, Denver, Colorado, pages 45-58.S.

[5] M.ArunPrakash, T.R.Gokul; "*Network Security-Overcome Password Hacking Through Graphical Password Authentication*". Proceedings of the National Conference on Innovations in Emerging Technology-2011.

[6] Fawaz A. Alsulaiman and Abdulmotaleb El Saddik, Senior Member, IEEE: "*Three-Dimensional Password for More Secure Authenticatio*n" ieee transactions on instrumentation and measurement, vol. 57, no. 9, september 2008.

[7] Ali Mohamed Eljetlawi, Norafida Ithnin, 2008, *Graphical Password:prototype usability survey", International Conference on* Advanced Computer Theory and Engineering (ICACTE '08).

[8] M. N. Doja and Naveen Kumar, "*Virtual Password: Virtual Environment Based User Authentication"*, published in proceedings of the 2008 International Conference on Security & Management, SAM 2008.

[9] Susan Wiedenbeck, Jean-Camille Birget, Alex Brodskiy – "*Authentication Using Graphical Passwords*: *Effects of Tolerance and Image Choice."*

[10] M.Samuel John, V.Siva Parvathi, M.Raja Sekhar, P.Raveendra Babu – "*Enhancing security of Pass Points system using variable tolerance"*.

[11] Takao Miyachi, Keita Takahashi, Madoka Hasegawa, Yuichi Tanaka, Shigeo Kato – "*A study on memorability and shoulder-surfing robustness of graphical password using dwt-based image blending"*.

[12] Impro Passwving Graphicalord Resistant to Shoulder-Surfing Using 4-way Recognition-Based Sequence Reproduction (RBSR4).