Research Paper Engineering

Virtual World Security

Vishal Bhogate, Rohit Patil, Hardik Trivedi, Sanjay Nandiwale

Department of Information Technology, Padmabhushan Vasant-dada Patil Pratishthan's College Of Engineering Mumbai,India

ABSTRACT

Providing Authentication to any system leads to provide more security to that system. There are many authentication techniques available, such as textual password, graphical password, etc. but each of these individually having some limitations & drawbacks. To overcome the drawbacks of previously existing authentication technique a new improved authentication technique is used, this authentication scheme is called as 3D password. The 3D password is multi-password & multi-factor authentication system as it uses various authentication techniques such as textual password, graphical password etc. Most important part of 3D password scheme is inclusion of 3D virtual environment. 3D virtual environment is virtual environment which is consisting of real time object scenarios. It is not actual real time environment, it is just user interface provided to scheme which looks same as real environment. 3D password is more secure authentication scheme than any other authentication techniques. This authentication scheme is more advanced than any other schemes. Also this scheme is hard to break and easy to use. In this paper we have introduced our contribution towards 3D Password to become more secure and more user friendly to users of all categories.

KEYWORDS

INTRODUCTION

In this multi-factor authentication scheme the basic building block used is 3D virtual environment. 3D virtual environment is created inside a 2D screen, refer fig.1. 3D environment is a real time scenario seen by peoples in day to day life which is created virtually in 3D virtual environment. We can use any real time object as an environment like any room or village but for simplicity we suggest to use small environment like room.

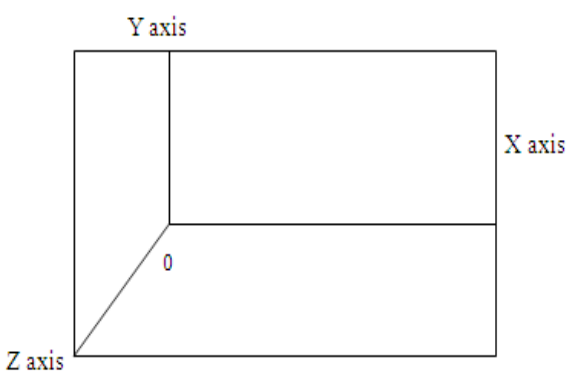

Figure 1. 3D Virtual Environment

- Virtual environment selected in such a way so that it is similar to real life object.
- Every object is unique & distinct from other.
- Virtual environment size should be considered

Features of system

- To provide more secure authentication technique than existing one.
- To design & develop more user friendly & easier authentication scheme and giving user to freedom of selecting more than one password scheme as single system.
- To overcome the drawbacks & limitations of previously existing systems (textual password, graphical password.etc).
- New scheme should be combination of recall-, recognition -, biometrics-, and token based authentication schemes.

ARCHITECTURE

Proposed authentication scheme is combination of many other authentication schemes together. 3D password is combination of both recall-based (i.e. textual password, etc) & recognition based (i.e. graphical password, biometrics, etc) so that 3D password is multifactor & multi password authentication scheme. Refer figure1.

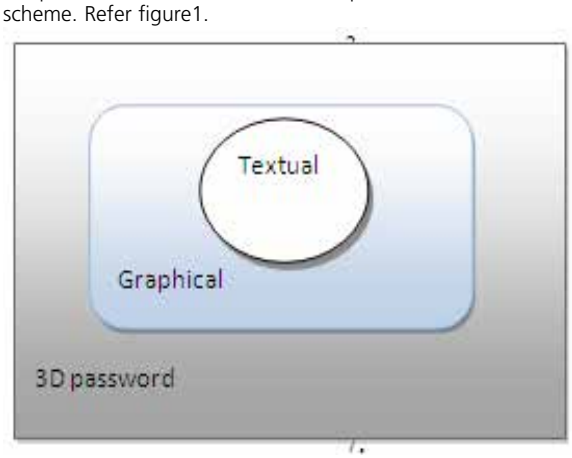

Figure 2. Multifactor authentication scheme

For authentication with 3D password a new virtual environment is introduced called as 3D virtual environment where user navigate , moving in 3D virtual environment to create a password which is based on both the schemes. We don't use biometric scheme because biometric has some

major drawbacks (like h/w cost is more). Biometric authentication is efficient in case of shoulder surfing attacks but it is vulnerable to other attacks. Also inclusion of biometric may lead to increasing the cost of scheme & more hardware parts needed.

System Architecture

This section tell about that how to create 3D password & what are different schemes used to form a complete 3D password.. 3D password is multi-factor & multi password authentication scheme. So that many password schemes like textual password, graphical password, biometric, etc. password schemes can be used as a part of 3D password. Choosing of different schemes are based on category of user who are going to use this scheme to there system. Figure 3., shows Architecture of Virtual World Security.

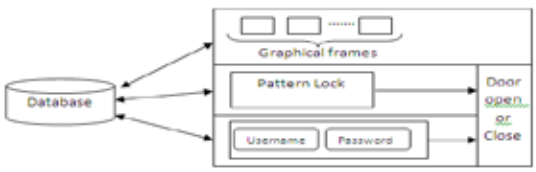

Figure 3. Architecture of Virtual World Security

Operational Architecture

In 3D password user has to first authenticate with simple textual password module on main door. Once authentication is successful then user moves in 3D virtual environment where he/she has to face multiple doors. Each door is locked with a module of Pattern Lock (that is found on android phones) user has to select correct door with correct pattern which will open the door. Here user goes through another module of authentication i.e. Graphical Authentication. The wall will contain multiple graphical image frames and user needs to select a correct frame from which he/she must select correct unique object. This is the last level of authentication. Successful completion of all the modules will authenticate the user. 3D password working algorithm is shown in figure.4.Which will give the flowchart for 3D password creation & authentication process.

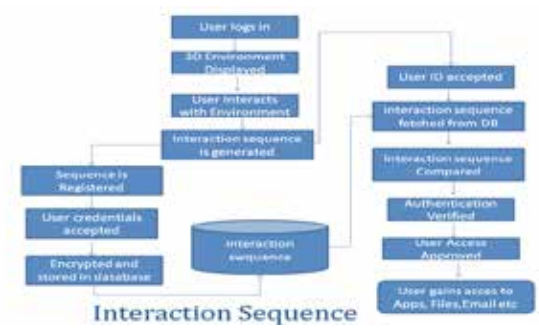

Figure 4. 3D password creation & authentication process

Literature Survey

Authentication is one of the most important security service provided to system by the different authentication schemes or algorithms. To protect any system authentication must be provided, so that only authorized persons can have right to use or handle that system & data related to that system securely. There are many authentication algorithms are available some are effective & secure but having some drawback. Previously there are many authentication techniques were introduced such as graphical password, text password, Biometric authentication, etc. generally there are four types of authentication techniques are available such as:

Knowledge based. Means what you know. Textual password is the best example of this authentication scheme.

Token based. Means what you have. This includes Credit cards, ATM cards, etc as an example.

Biometrics. This means authentication using human body parts e.g. Iris recognition, face recognition, etc

Recognition Based. Includes graphical password.

Ideally there are two types of Authentication schemes are available according to nature of scheme & techniques used, those types are:

Recall based. In this authentication tech. user need to recall or remember his/her password which is created before [1]. Knowledge based authentication is a part of this technique, E.g. Textual password, graphical password etc. this technique is commonly used all over the world where security needed.

Recognition based. In this user need to identify, recognize password created before. Recognition based authentication can be used in graphical password. Generally this technique is not use much more as Recall based is used. Still both recall based & recognition based authentication techniques having some drawbacks & limitations when they are used separately or used single authentication scheme at a time. To overcome these drawbacks & limitations of previously existing authentication schemes. We have introduced a new authentication scheme which is based on previously existing schemes. This authentication scheme is based on combination of passwords called as "3D Password". Which is a multifactor scheme uses combination of above discussed scheme as well as biometric & many other schemes [1]. All these schemes are implemented in virtual 3D environment while creating 3D Password. Where this environment contain various virtual objects through which user interacts with. The interaction with 3D environment changes as per user changes. The 3-D password is constructed by observing the actions and interactions of the user and by observing the sequences of such actions.

Attacks & countermeasures

As mentioned earlier 3D password is most secure authentication. We will see different kinds of attacks & how 3D password scheme is more secure against different attacks.

Timing Attacks. This attack is based on how much time required completing successful sign-in using 3D password scheme. Timing attacks can be very much effective while Authentication scheme is not well designed. But, as our 3D password scheme is designed more securely, these kinds of attacks are not easily possible on 3D Password & also not much effective as well.

Brute force Attacks. In This kind of attacks the attacker has to try n number of possibilities of 3D Password. As these attacks considers following two points.

- Required time to login: as in 3D password time required for successful login varies & is depend on number of actions & interactions, the size of 3D virtual environment.
- Cost required to attack: as 3D password scheme requires 3D virtual environment & cost of creating such a environment is very high.

Well-studied attacks .In this attack attacker has to study whole password scheme. After studied about scheme the attacker tries combination of different attacks on scheme. As 3D password scheme is multi-factor & multi-password authentication scheme, attacker fail to studied whole scheme. this attacks also not much effective against 3D password scheme

Key logger. In this attack attacker install as software called key logger on system where authentication scheme is used [7]. This software stores text entered through keyboard & those text are stored in text file. In this way this attacks is more effective & useful for only textual password, but as 3D password is multi password authentication scheme. So that this kind of attacks are not much effective in this case .

Shoulder Surfing attacks. Attacker uses camera for capturing & recording of 3D password. This attack is more effective than any other attacks on 3D password. So that 3D password must be performed in a secure place where this attack can't be performed. Shoulder surfing attacks is still effective & easily possible against 3D password [1].

CONCLUSION

In this paper, Virtual World Security (VWS) application is implemented using Java technology. This application is developed using Unity3D, jMonkey3.0 and Blender. Thus using the security module the user is secured about his/her system and the further services are provided according to the user's choice. Using Ms-Access Database handling is made easy at the administrator side. The front end (GUI) is user friendly and thus the application is easy to understand and use. Due to the use of easily understandable open source software's the application can be further extended to become a social networking site as well thus increasing the market value.

REFERENCES

[1] Fawaz A. Alsulaiman and Abdulmotaleb El Saddik, IEEE Paper "Three-Dimensional Password for More Secure Authentication". | [2]International Journal of Engineering Science and Innovative Technology (IJESIT),Volume 2, Issue 2 Paper for "Secure Authentication with 3D Password". | [3]Unity 3D Game Engine Tutorials , http://unity3d.com/learn/tutorials/modules. | [4]jMonkeyEngine Tutorials and Documentation to get familiar with basic 3D game development ,http://hub.jmonkeyengine.org/wiki/doku.php/jme3 |