ijecs open access www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 7 July, 2014 Page No. 7093-7096

Enhanced Authentication by Virtual World

Pradeep Yadav

Department of Computer Science & Engineering, MDU University Rohtak,
R.P.S College of Engineering & Technology
Mohindergarh, Haryana, India
pradeepyadav1988@gmail.com

Abstract: ***Authentication is the process of verifying credentials of user and guarantees the user what it claims to be. Many ways of authentications are proposed starting from Textual Passwords, Graphical passwords, Biometrics etc. But all have certain limitations or drawbacks. Hence I propose a new way of Authentication which has capability of all existing authentication systems and is also suited for Client Server Architecture. This technique is based on real world simulation hence called Virtual World. User is given freedom to interact with virtual things and select his authentication mode i.e textual, graphical, Biometrics, OTP, Voice etc. This scheme provides more options and freedom to user along with have higher password space and hence difficult to break and thus more secured.***

*Keywords**: Authentication, Virtual World, Multi-password, SHA256***

1. Introduction

Information has been valuable since the dawn of mankind: e.g. where to find food, how to build shelter, etc. Over the time accumulated information kept increasing and hence the need of computer for its storage and quick access. As access to computer stored data has increased, Information Security has become correspondingly important. Information is the most valuable asset, and protecting this is known as Information Security, sometimes also referred as InfoSec. The main goals of InfoSec are: Availability, Confidentiality, Integrity, and Authentication. Authentication is the important aspect under information security and is derived from Greek word means real or genuine. Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. There are many existing means of Authentication:

Textual Password: This is the most common form of authentication used today having major drawback with its two conflicting requirements: the selection of passwords that are easy to remember and, at the same time, are hard to guess. People normally keep nick names, place, and family name or dictionary words as the password, which are easy to guess and hence weak. Below are the other limitations of Textual passwords:

- Password may be easy to guess.
- Writing the password down and placing it on highly visible areas.
- Dictionary word, which can be guessed by brute force attack.
- Discovering passwords by eavesdropping or even social engineering.
- Same password being used under multiple sites including social sites, where password is sometimes shared.

Token Based: This type of authentication is based on "What the user has" A simple example of this is credit card number and grid. Another example is a token, which is allotted to individual user. If user is entering the token number it is assumed he is the correct user. But people don't like to carry these cards or tokens daily and many times people tend to forget these as well. Additionally in adhoc requirements people can't use the service as they don't have these tokens.

***Biometrics*:** This type of Authentication is based on "What the user is". Many biometrics approaches are proposed like fingerprints, palm prints, hand geometry, face recognition, voice recognition, iris recognition, and retina scan.
Limitations of Biometrics are as follows:

- Human properties are vulnerable to change from time to time due to scarring, face makeup, change of hairstyle, and sickness (change of voice).
- People tend to resist biometrics for personal reasons like Iris scan.
- Biometrics cannot be revoked.
- Additional hardware device is required for Biometrics.
- Not feasible for Client – Server Architecture.

Graphical Passwords: In this user has to remember the pattern of selection made. It may be pattern user created or may be sequence of clicks on an Image. But this is not adapted to a very large scale and is in its preliminary stages only.
To overcome all the limitations of existing system, following model is proposed:

Virtual World Authentication:

This is a multi-factor model, which is suitable for all kinds of authentications be it stand alone computer login, be it Computer present in highly secure area like Armed forces, be it in research and development, be it with nuclear reactors or be it a light weight client and having Client –Server Architecture. Additional advantage of this is, it has the capability to incorporate all existing authentication techniques

like textual password, Graphical password, Biometrics and even OTP (One time password) into it.

Virtual World is configurable, extendable and very interesting way of providing authentication. In this approach passwords are based on linking, storing and remembering structure of Human Memory. Normally we keep simple passwords, because they are easy to remember and faster to recall. User selects among a list of available environments, and then user is put inside the environment. Environment is configured to resemble as close as to the real world. User interacts with relevant objects placed in any specific selected environment. Example list of environments could be: Flat, Kitchen, Park, Mall, City, Country, World etc.

2. Enhanced Authentication

High are the modules of the proposed system:

2.1 Registration

This is the first step, when user is registered to the system. In this step all user details are feed to the system and are stored in a DB. Details may vary from one type of complex/secure system to another. In the demo version of same I have considered below:

Fig. 1 *Registration form*

2.2 Password Set

After registration the next phase is Password Set. User is presented a virtual world, which is very close to real world with buildings, schools, malls etc. User is given freedom to select any environment, once selected that specific virtual environment will be loaded, and user will have a feel as if he is actually in that area. For example user selected a Museum Building, in that user will be shown many models as they are present in a real museum. User is given freedom to select any model as per his wish, or even interact with object on which operations are allowed, like opening a door, switch on/off a light in museum. A computer will be there in all virtual environments, where users who prefer to have textual passwords, can select this and set the password. Even User can stand at a place and speak something via head phone. A virtual environment to have integration with bio-metrics can also be there, Even for banking purposes an option of OTP will be there, on selecting it an OTP from bank will also be send to your mobile. Hence password can be Objects selected + Objects interaction + Textual password + Biometrics+ OTP + Graphical password. Above all operations form a sequence and this is encrypted using one way hash function i.e. SHA256. This encrypted string is stored in a binary format in DB. If password is set as part of registration, a unique auto system generated User Id will be created; and user can always use this User Id for all operations.

2.3 Password Reset

Change is in human nature hence the necessity of having the option of password change. In case whenever user is bored with existing password, or due to safety concern he wants to change his password, or he want to try new options available or want to increase the security by adding more objects to be part of password, User is given freedom to change it.

User has to use his unique Generated User Id for all operations, including this as well. For password reset below are high level operations:

1. Select Reset Password.
2. Authenticate using existing password.
3. If password is correct user is given option to select a new password, else operation denied.

3. Architecture

3.1 Architecture Diagram

The architecture of my proposed model is below:

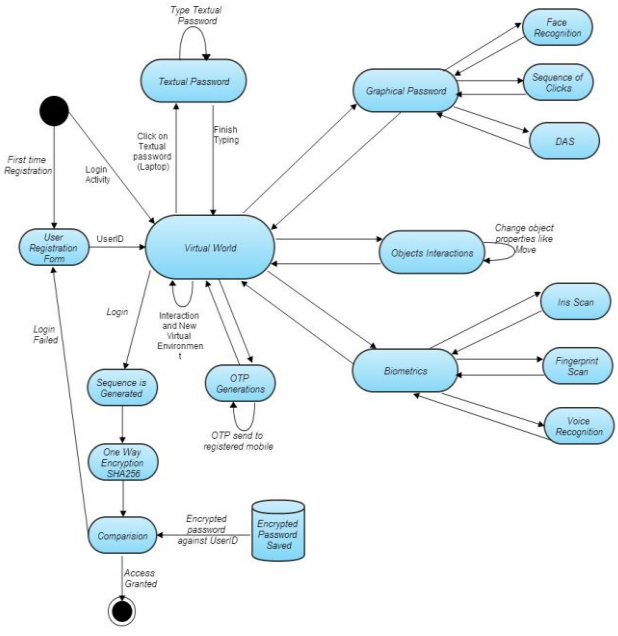

Fig. 2 *Proposed Architecture*

After setting the password using registration page, user can login into the environment by using the generated user id. After entering the user id, user is put inside the Virtual world, which is the simulation of real world. The simulation of user in virtual world is known as "Avatar". The complexity and number of objects in virtual world is security dependent

design principal. For example, once user logs into the virtual world, an individual building representing the Bank will be visible. User can select the bank; on selection a new environment i.e. Environment of Bank will be loaded. Further user clicks on a Computer where a pop-up of textual password will appear, User can set the textual password, User can even turn on/off the lights of Bank and even he can click on OTP generation m/c. On doing that OTP will be send to the registered mobile. Additionally bio-metrics and graphical passwords can be selected to integrate them into password. All above mentioned operations will form a sequence; this sequence will be given as input to encryption algorithm i.e. SHA256. This is most secured one way encryption and digest generated by this is compared with the one already residing in DB.

If both are same then only user is given permission to login into the system otherwise not.

This approach is even suitable for client server architecture, where all the Environment details will be residing on the server. Based on user inputs, selections and operations requests will be send to server and environment changes and new configurations will be provided by server. Hence this is a suitable and more secure approach for Banking systems as well. Banking systems currently have OTP and textual passwords only, which are just a sub part of my approach and even user has various other means and more operations as per his wish, which makes this more flexible, suitable, remember able and yet much stronger.

3.2 Screen Shots of Demo

Below are some of the examples of Virtual worlds:

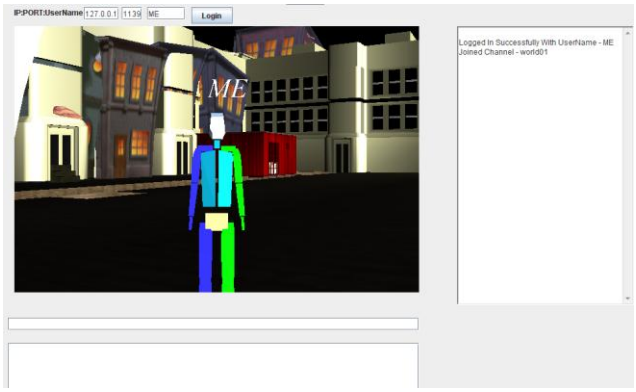

Fig. 3 *User in Virtual World*

Once user selects a specific building, a new virtual environment will be loaded on the client screen giving the feel as if user is moved to that building. For example if user selects the room below appears, which has books, table, chairs and sofa. Number of objects in a virtual environment can be increased depending on complexity and security needed. This is a just a design principal, but object should relate very closely to real world object along with their size and shapes. To avoid ambiguity usually single copy of each object is placed in every environment.

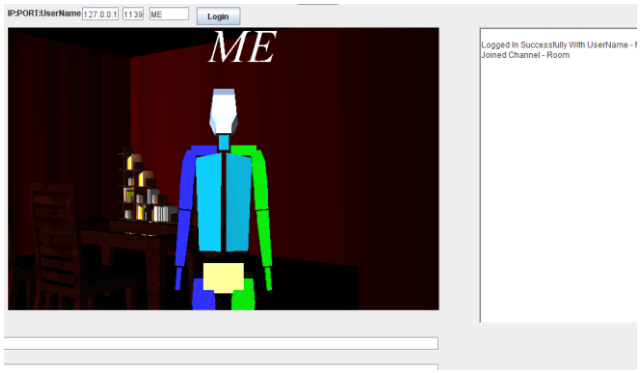

Fig. 4 *After selecting a specific environment*

3.3 Password Space

To determine password space of this scheme, we have to count all possible passwords that have a certain number of actions, interactions, and inputs towards all objects that exist in the 3D virtual environments. As the complexity an design of virtual world increase, i.e. number of objects in virtual world, number of virtual environments one inside the another, operations and properties on objects, along with existing passwords the password space of this scheme increases drastically.

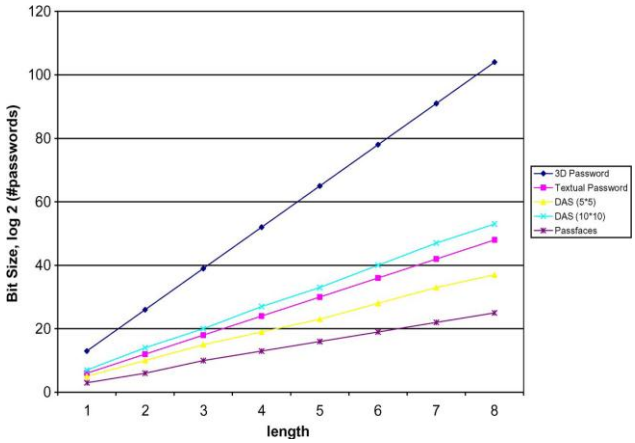

Fig. 5 *Password Space*

Password space of the Virtual password, textual password, Pass faces, and DAS with grid sizes of 5 × 5 and 10 × 10. Length is the number of actions and interactions for a Virtual world password, the number of characters for textual passwords, the number of selections for Pass faces, and the number of points that represent the strokes for DAS. The length is up to eight.

4. Conclusion

There are many authentication schemes being used some of them are based on user's physical and behavioral properties, and some other authentication schemes are based on user's knowledge such as textual and graphical passwords. Moreover, there are some other important authentication schemes that are based on what you have, such as smart cards. Among the various authentication schemes, textual password and token-based schemes, or the combination of both, are commonly applied. However, with the advanced technology and the limitation of both the schemes as

mentioned before, both authentication schemes are vulnerable to certain attacks. Moreover, there are many authentication schemes that are currently under study and they may require additional time and effort to be applicable for commercial use. This Virtual World authentication is a multifactor scheme that combines these various authentication schemes into a single 3-D virtual environment. The virtual environment can contain any existing authentication scheme or even any upcoming authentication schemes by adding it as a response to actions performed on an object. Therefore, the resulted password space becomes very large compared to any existing authentication schemes.

The designing of the 3-D virtual environment, selections of objects inside the environment, and the object's type reflect the resulted password space. The choice of what authentication schemes will be part of the user's password reflects the user's preferences and requirements, this scheme gives more freedom to user to select the type of password. A user who prefers to remember and recall a password might choose textual and graphical passwords apart of their virtual password. On the other hand, user's who have more difficulty with memory or recall might prefer to choose smart cards or biometrics as part of their password. Therefore, it is the user's choice and decision to construct the desired and preferred virtual password.

Thus, this proposed scheme has a great potential and capable of replacing the existing authentication system and can start a new era of easy, flexible, user driven yet robust and secure password which is more resistant to timing, well studied and brute force type of attacks.

References

[1] Alsulaiman, F.A. and El Saddik, A. "Three- for Secure," IEEE Transactions on Instrumentation and measurement. 57(9) :1929-1938, 2008.

[2] Gadicha, A. B.; Gadicha, V. B.Virtual Realization using 3D Password. International Journal of Electronics and Computer Science Engineering. ISSN 2277-1956. 1(2) : 216-222.

[3] Dhamija, R.; Adrian, P. D. V. 2000. A User Study Using Images for Authentication. In Proceedings of USENIX Security Symposium, Denver, Colorado : 45-58.

[4] Alsulaiman, F. A. and A. El Saddik. "A novel 3D graphical password schema," in Proc. IEEE Int. Conf. Virtual Environ., Human-Comput. Interfaces, Meas. Syst.: 125–128, 2006.

[5] Suo, X.; Zhu, Y. and Owen, G. S. "Graphical passwords: A survey".Computer Security Appl. Conf.: 463–472, 2005.

[6] Weinshall, D. and Kirkpatrick, S. "Passwords You'll Never Forget, but Can't Recall," in Proceedings of Conference on Human Factors in Computing Systems (CHI).

[7] Alsulaiman, F. A. and El Saddik, A. A Novel 3D Graphical Password Schema, IEEE. International Conference on Virtual Environments, Human-Computer Interfaces, and Measurement Systems, 2006.

[8] Tejal Kognule and Yugandhara Thumbre and Snehal Kognule, ―3D password, International Journal of Computer Applications (IJCA), pp. 6-10 2012.

[9] Vishal Kolhe, Vipul Gunjal, Sayali Kalasakar, Pranjal Rathod, Volume 2. Secure Authentication with 3D Password (IJESI), pp. 99-105, 2013.

[10] Swati Bilapatte and Sumit Bhattacharjee, Volume 5, No 2. A novel approach of more secure Authentication (IJCSET) pp. 150-157, 2014.

Author Profile

Pradeep Yadav received the Bachelor of Engineering in IT from Pune University. He has experience in IT software Development Company. He is currently pursuing degree in Master of Engineering in the field of Computer Engineering, From R.P.S College of Engineering, Mohindergarh, Haryana. He is interested in developing security and authentication systems in IT.