IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 1, March, 2013
ISSN: 2320 - 8791
www.ijreat.org

A Novel Revolutionary highly secured Object authentication schema

S.Jayaprakash[1], Madhubala.C[2] and Rifaya Farvin.A[3]

[1]*Assistant Professor Computer science and Engineering ,Idhaya Engineering college for women,Chinnasalem*

[2,3] *Computer science and Engineering ,Idhaya Engineering college for women,Chinnasalem.*

Abstract

Though the technology has developed, authentication seems to be weak in its approach .It is easy for others to steal or hack our password in day to day life object password is an multifactor authentication scheme, that is inclusion of textual password , biometric , graphical passwords . here user navigates and interacts with various objects and set password by new technique called object password technique . In this paper we show that the space is reduced and increase the security. Therefore many algorithms have come up each with an interesting approach toward calculation of a secret key. Mostly textual passwords follow an encryption algorithm, Biometric scanning is your "natural" signature and Cards or Tokens prove your validity. But some people hate the fact to carry around their cards. Some refuse to undergo strong IR exposure to their retinas (Biometric scanning). Mostly textual passwords, nowadays, are kept very simple say a word from the dictionary or their pet names, Girlfriends etc. As per tests a professional could crack 10-15 passwords per day. Here we present a idea of 3D passwords which are more Customizable, and very interesting way of authentication. The human memory in our scheme has to undergo the facts of Recognition, Recalling, Biometrics or Token based authentication.

Keywords: *Authentication, Biometrics (finger print),Graphical password ,Textual passwords, Virtual Environment.*

1.INTRODUCTION

With all the means of technology developing, it can be very easy for 'others' to fabricate or to steal identity or to hack someone's password. Therefore many algorithms have come up each with an interesting approach toward calculation of a secret key. The algorithms are such based to pick a random number in the range of 10^6 and therefore the possibilities of the same number coming is rare. Users nowadays are provided with major password stereotypes such as textual passwords, biometric scanning, tokens or cards (such as an ATM) etc .Mostly textual passwords follow an encryption algorithm as mentioned above. Biometric scanning is your "natural" signature and Cards or Tokens prove your validity. But some people hate the fact to carry around their cards, some refuse to undergo strong IR exposure to their retinas(Biometric scanning).Mostly textual passwords, nowadays, are kept very simple say a word from the dictionary or their pet names, girlfriends etc. Years back

Klein performed such tests and he could crack 10-15 passwords per day. Now with the technology change, fast processors and many tools on the Internet this has
become a Child's Play. Therefore we present our idea, the 3D passwords which are more customizable and very interesting way of authentication. Now the passwords are based on the fact of Human memory. Generally simple passwords are set so as to quickly recall them. The human memory, in our scheme has to undergo the facts of Recognition, Recalling, Biometrics or Token based authentication. Once implemented and you log in to a secure site, the 3D password GUI opens up This is an additional textual password which the user can simply put. This is the Recall and Recognition part of human memory coming into play. Interestingly, a password can be set as approaching a radio and setting its frequency to number only the user knows. Security can be enhanced by the fact of including cards and biometric scanner as input

2. EXISTING SYSTEM

Current authentication systems suffer from many weaknesses. Textual passwords are commonly used. 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. Moreover, biometrics cannot be revoked. The 3D password is a multi factor authentication scheme. The design of the 3D virtual environment and the type of objects selected determine the 3D password key space. User

have freedom to select whether the 3D password will be solely recall, recognition, or token based, or combination of two schemes or more.

3.PROPOSED SYSTEM

The proposed system is a multi factor authentication scheme that combines the benefits of various authentication schemes. Users have the freedom to select whether the 3D password will be solely recall, biometrics, recognition, or token based, or a combination of two schemes or more. This freedom of selection is necessary because users are different and they have different requirements. Therefore, to ensure high user acceptability, the user's freedom of selection is important. The following requirements are satisfied in the proposed scheme

1. The new scheme provide secrets that are easy to remember and very difficult for intruders to guess.
2. The new scheme provides secrets that are not easy to write down on paper. Moreover, the scheme secrets should be difficult to share with others.
3. The new scheme provides secrets that can be easily revoked or changed.

4. BRIEF DESCRITION OF THE SYSTEM

The proposed system is a multi factor authentication scheme. It can combine all existing authentication schemes into a single 3D graphical virtual environment .This 3D graphical virtual environment contains several objects or items with which the user can interact. The user is presented with this 3D object environment where the user navigates and interacts with various objects. The sequence of actions and interactions toward the objects inside the 3D environment constructs the user's 3D password.

The 3D password can combine most existing authentication schemes such as textual passwords, graphical passwords, and various types of graphics into a 3D object virtual environment. The choice of what authentication schemes will be part of the user's 3D password reflects the user's preferences and requirements. A user who prefers to remember and recall a password might choose textual and graphical password as part of their 3D object password. On the other hand users who have more difficulty with memory or recall might prefer to choose smart cards or biometrics as part of their 3D password. Moreover user who prefers to keep any kind of biometric data private might not interact with object that requires position information. Therefore it is the user's choice and decision to construct the desired and preferred 3D object password.

fig.1.main page

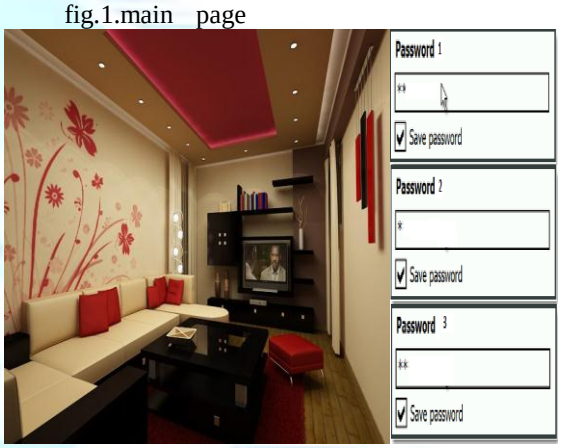


Fig.2.work page

5. SYSTEM IMPLEMENTATION

The 3D object password is a multi factor authentication scheme. The 3D object password presents a 3D virtual environment containing various virtual objects. The user navigates through this environment and interacts with the objects. The 3D password is simply the combination and the sequence of user interactions This means interacting with the same objects that reside at the exact locations and perform the exact actions in the proper sequence.

```
public class AddEmployee extends Activity {
        EditText txtName;
        EditText txtAge;
        TextView txtEmps;
        DatabaseHelper dbHelper;
        Spinner spinDept;

        @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.addemployee);
        txtName=(EditText)findViewById(R.id.txtName);
        txtAge=(EditText)findViewById(R.id.txtAge);
        txtEmps=(TextView)findViewById(R.id.txtEmps);
        spinDept=(Spinner)findViewById(R.id.spinDept);
    }

void CatchError(String Exception)
{
        Dialog diag=new Dialog(this);
        diag.setTitle("Add new user");
        TextView txt=new TextView(this);
        txt.setText(Exception);
        diag.setContentView(txt);
        diag.show();
}

void NotifyuserAdded()
{
        Dialog diag=new Dialog(this);
        diag.setTitle("Add new user");
        TextView txt=new TextView(this);
        txt.setText("usern account created Successfully");
        diag.setContentView(txt);
        diag.show();
        try {
                diag.wait(1000);
        } catch (InterruptedException e) {
                // TODO Auto-generated catch block
                CatchError(e.toString());
        }
        diag.notify();
        diag.dismiss();
}
```

6. 3D OBJECT PASSWORD SELECTION AND INPUT

Let us consider a 3D virtual environment space of size G ×G. The 3D object environment space is represented by the coordinates (x, y) ∈ [1, . . . , G] ×[1, . . . , G]. The objects are distributed in the 3D objects environment with unique (x, y) coordinates. We assume that the user can navigate into the 3D object virtual environment and interact with the objects using any input device such as a mouse, key board. We consider the sequence of those actions and interactions using the previous input devices as the user's 3D object password.

7. 3D VIRTUAL ENVIRONMENT GUIDELINES

The design of the 3D object virtual environments affects the usability, effectiveness, acceptability of 3D password. The first step in building a 3D object password system is to design a 3D object environment that reflects the administration needs and the security requirements. The design of 3D virtual environments should follow these guidelines

1) Real Life Similarity : The prospective 3D object virtual environment should reflect what people are used to seeing in real life. Objects used in virtual environments should be relatively similar in size to real objects (sized to scale). Possible actions and interactions toward virtual objects should reflect real life situations. Object responses should be realistic. The target should have a 3D object virtual environment that users can interact

2) Object uniqueness and distinction every virtual object or item in the 3D object 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. 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 3D object virtual environment should consider that every object should be distinguishable from other objects. Similarly, in designing a 3D object 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.

3) Three Dimensional Virtual Environment Size A 3D object virtual environment can depict a city or even the world. On the other hand, it can depict a space as focused as a single room or office. A large 3D virtual environment will increase the time required by the user to perform a 3D object password. Moreover, a large 3D object virtual environment can contain a large number of virtual objects. Therefore, the probable 3D object password space broadens. However, a small 3D object virtual environment usually contains only a few objects, and thus, performing a 3D password will take less time.

4) Number of objects and their types Part of designing a 3D object virtual environment is determining the types of objects and how many objects should be placed in the environment. The types of objects reflect what kind of responses the object will have. For simplicity, we can consider requesting a textual password or a fingerprint as an object response type. Selecting the right object response types and the number of objects affects the probable password space of a 3D object password.

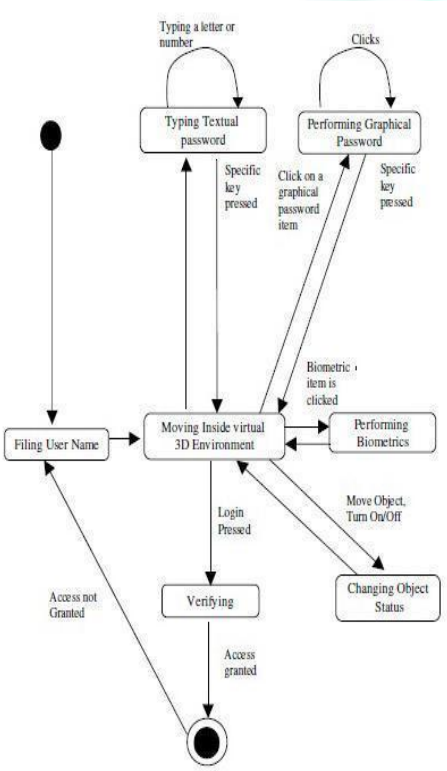
5) System Importance The 3D object virtual environment should consider what systems will be protected by a 3D object password The number of objects and the types of objects that Have been used in the 3D object virtual environment should reflect the importance of the protected system.

8. 3D PASSWORD APPLICATION

A small virtual environment can be used in the following systems like

1) ATM
2) Personal Digital Assistance
3) Desktop Computers & laptop logins
4) Web Authentication
5) Security Analysis

9. STATE DIAGRAM OF A3D OBJECT PASSWORD APPLICATION



10. SECURITY ANALYSIS

3D password space size to determine the password space, we have to count all possible 3D passwords that have a certain number of actions,interactions, and inputs towards all objects that exist in the 3D virtual environments.

10.1 3D PASSWORD DISTRIBUTION KNOWLEDGE

Users tend to use meaningful words for textual passwords. Therefore finding these different words from dictionary is a relatively simple task which yields a high success rate for breaking textual passwords. Pass faces users tend to choose faces that reflect their own taste on facial attractiveness, race, and gender. Every user has different requirements and preferences when selecting the appropriate 3D Password. This fact will increase the effort required to find a pattern of user's highly selected 3D password. In addition, since the 3D password combines several authentication schemes into a single authentication environment, the attacker has to study every single authentication scheme and has to discover what the most probable selected secrets are. Since every 3D password system can be designed according to the protected system requirements, the attacker has to separately study every 3D password system. Therefore, more effort is required to build the knowledge of most probable 3D passwords.

10.2 ATTACKS AND COUNTER MEASURES

To realize and understand how far an authentication scheme is secure, we have to consider all possible attack methods.We have to study whether the authentication scheme proposed is immune against such attacks or not. Moreover, if the proposed authentication scheme is not immune,we then have to find the countermeasures that prevent such attacks. In this section, we try to cover most possible attacks and whether the attack is valid or not. Moreover, we try to propose countermeasures for such attacks.

1)Brute Force Attack: The attacker has to try all possible 3D passwords. This kind of attack is very difficult for the following reasons.

a. Time required to login: The total time needed for a legitimate user to login may vary depending on the number of interactions and actions, the size of the 3D virtual environment, and the type of actions and interactions. Therefore, a brute force attack on a 3D password is very difficult and time consuming

b. Cost of attacks the 3D virtual environment contains biometric recognition objects and token based objects. The attacker has to forge all possible biometric information and forge all the required tokens. The cost of forging such information is very high, therefore cracking the 3D password is more challenging. The high number of possible 3D password spaces leaves the attacker with almost no chance of breaking the 3D password.

3)Shoulder Surfing Attack : An attacker uses a camera to record the user's 3D password or tries to watch the legitimate user while the 3D password is being performed. This attack is the most successful type of attack against 3D passwords and some other graphical passwords. However, the user's 3D password may contain biometric data or textual passwords that cannot be seen from behind. Therefore, we assume that the 3D password should be performed in a secure place where a shoulder surfing attack cannot be performed.

4)Timing Attack: In this attack, the attacker observes how long it takes the legitimate user to perform a correct sign in using the 3D password. This observation gives the attacker an indication of the legitimate user's 3D password length. However, this kind of attack alone cannot be very successful since it gives the attacker mere hints. Therefore, it would probably be launched as part of a well studied or brute force attack. Timing attacks can be very effective if the 3D virtual environment is poorly designed.

11. EXPERIMENTAL RESULTS

As a proof of concept we have built an experimental three dimensional virtual environment that consist of many objects. Objects initially have two kinds of responses to reactions, they are, objects that accept textual passwords and objects that accept graphical passwords. Almost 8 users have tested the experimental environment . Nearly 90% we have succeeded in our Experimental Virtual Three-Dimensional Environment

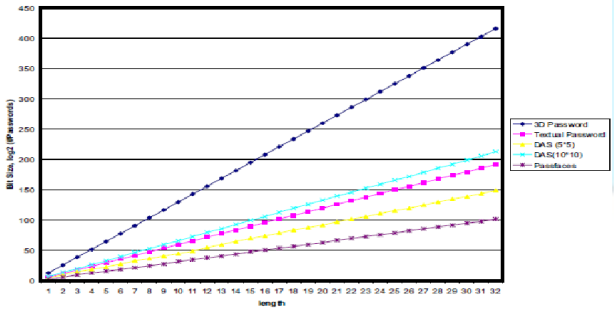


Fig.3. A comparison between object password , biometrics, textual password

12.CONCLUSION

The 3D object password is a multi factor authentication scheme that combines the various authentication schemes into a single 3D object virtual environment. The virtual environment can contain any existing authentication scheme or even any upcoming authentication scheme or even any upcoming authentication schemes 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 object virtual environment the selection of objects inside the environment and the 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 object virtual environment is a factor that leads to a higher user acceptability of a 3D object password system. The choice of what authentication scheme will be part of user's 3D object password reflects the user's preferences and requirements.

13. REFERENCES

[1] Alsulaiman, F.A.; El Saddik, A., "Three- for Secure,"IEEE Transactions on Instrumentation and measurement, vol.57, no.9, pp 1929-1938.Sept. 2008

[2] X. Suo, Y. Zhu, and G. S. Owen, "Graphical passwords: A survey," in Proc. 21st Annu. Comput. Security Appl.Conf., Dec. 5–9, 2005, pp. 463–472.

[3] D. V. Klein, "Foiling the cracker: A survey of, and improvement to passwords security," in Proc. USENIX SecurityWorkshop, 2007, pp. 5–14.

[4] NBC news, ATM Fraud: Banking on Your Money, Dateline Hidden Cameras Show Criminals Owning ATMs, Dec.11, 2003.

[5] D. V. Klein, ―Foiling the cracker: A survey of, and to passwords security,‖ in Proc. USENIX Security, , pp.–14

[6] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition (Second Edition)*. Springer, 2009.

[7] A. K. Jain and J. Feng, "Latent palmprint matching," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 31, no. 6, pp. 1032–1047, 2009.

[8] Y. Wang, J. Hu, and D. Phillips, "A fingerprint orientation model based on 2D Fourier expansion (FOMFE) and its application to singular-point detection and fingerprint indexing," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 29, no. 4, pp. 573– 585, 2007.

[9] T. Kitten, Keeping an Eye on the ATM. (2005, Jul.11).[Online]. Available: ATMMarketPlace.com
[10] BBC news, Cash Machine Fraud up, Say Banks, Nov, 2010.
[11] G. E. Blonder, "Graphical password," U.S. Patent 5 559 961, Sep. 24, 1996.
[12] R. Dhamija and A. Perrig, "Déjà Vu: A user study using images for authentication," in Proc. 9th USINEX SecuritySymp., Denver, CO, Aug. 2000, pp. 45–58
[13] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A.D. Rubin, ―The design and analysis of graphical passwords,‖ in Proc. 8th USENIX Security
Symp,Washington DC, Aug.1999, pp.1-14.
[14] X. Suo, Y. Zhu, and G. S. Owen, ―Graphical passwords: A survey,‖ in Proc. 21st Annual. Computer Security Appl. Conf., Dec. 5–9, 2005, pp. 463–472.
[15] D. Weinshall and S. Kirkpatrick, "Passwords You'll Never Forget, but Can't Recall," in Proceedings of Conference on Human Factors in Computing Systems (CHI). Vienna, Austria: ACM, 2004, pp. 1399-1402.
[16] L. Sobrado and J.-C. Birget, "Graphical passwords," The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4, 2002.
[17] D. Hong, S. Man, B. Hawes, and M. Mathews, "A password scheme strongly resistant to spyware," in Proceedings of International conference on security andmanagement. Las Vergas, NV, 2004.
[18] S. Man, D. Hong, and M. Mathews, "A shouldersurfing resistant graphical password scheme," in Proceedings of International conference on security and management.Las Vegas, NV, 2003.
[19] Two Factor Authentication for the Enterprise, http://realuser.com/realuser.
[20] C. I. Watson, "NIST Special Database 14: Mated Fingerprint Card Pairs 2," June 2000, http://www.nist.gov/srd/nistsd14.cfm.