3D PASSWORD

Tejal Kognule
Dept. of Comp. Sc.,
Padmabhushan Vasantdada
Patil Pratishthan's College of
Engineering,
Mumbai University, India

Yugandhara Thumbre
Dept. of Comp. Sc.,
Padmabhushan Vasantdada
Patil Pratishthan's College of
Engineering,
Mumbai University, India

Snehal Kognule
Dept. of Comp. Sc.,
Padmabhushan Vasantdada
Patil Pratishthan's College of
Engineering,
Mumbai University, India

ABSTRACT

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. Once he goes through the first authentication, a 3D virtual room will open on the screen

General Terms

Secuirity, authentication,password,virtual

Keywords

VIRTUAL ENVIRONMENT, 3D password,input

1. INTRODUCTION

Normally the authentication scheme the user undegoes is paticularly very lenient or very strict.Throughout the yeras authentication has been a very interesting approach.With all the means of technology developing ,it can be very easy for 'others' to fabricate or to steal identity or to hack someones 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 possbilities of the sane number coming is rare.

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 3Dpassword 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.

4. BRIEF DESCRIPTION OF SYSTEM

The proposed system is a multi factor authentication scheme. It can combine all existing authentication schemes into a single 3D virtual environment .This 3D virtual environment contains several objects or items with which the user can interact. The user is presented with this 3D virtual 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 biometrics into a 3D 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 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 biometric information. Therefore it is the user's choice and decision to construct the desired and preferred 3D password.

5. SYSTEM IMPLIMENTATION

The 3D password is a multi factor authentication scheme. The 3D 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 that occur in the 3D virtual environment. The 3D password can combine recognition, recall, token, and biometrics based systems into one authentication scheme. This can be done by designing a 3D virtual environment that contains objects that request information to be recalled, information to be recognized, tokens to be presented, and biometric data to be verified.

Virtual objects can be any object that we encounter in real life. Any obvious actions and interactions toward the real life objects can be done in the virtual 3D environment toward the virtual objects. Moreover, any user input (such as speaking in a specific location) in the virtual 3D environment can be considered as a part of the 3D password.

We can have the following objects:

1) A computer with which the user can type;

2) A fingerprint reader that requires the user's fingerprint;

3) A biometric recognition device;

4) A paper or a white board that a user can write, sign, or draw on;

5) An automated teller machine (ATM) that requests a   token;

;6) A light that can be switched on/off;

7) A television or radio where channels can be selected

8) A staple that can be punched;

9) A car that can be driven;

10) A book that can be moved from one place to another;

11) Any graphical password scheme;

12) Any real life object;

13) Any upcoming authentication scheme.

The action toward an object (assume a fingerprint recognition device) that exists in location (x_1, y_1, z_1) is different from the actions toward a similar object (another fingerprint recognition device) that exists in location (x_2, y_2, z_2), where $x_1 = x_2$, $y_1 = y_2$, and $z_1 = z_2$. Therefore, to perform the legitimate 3D password, the user must follow the same scenario performed by the legitimate user. This means interacting with the same objects that reside at the exact locations and perform the exact actions in the proper sequence.

6. 3D PASSWORD SELECTION AND INPUT

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

For example, consider a user who navigates through the 3D virtual environment that consists of an office and a meeting room. Let us assume that the user is in the virtual office and the user turns around to the door located in (10, 24, 91) and opens it. Then, the user closes the door. The user then finds a computer to the left, which exists in the position (4, 34, 18), and the user types "FALCON." Then, the user walks to the meeting room and picks up a pen located at (10, 24, 80) and draws only one dot in a paper located in (1, 18, 30), which is the dot (x, y)

coordinate relative to the paper space is (330, 130). The user then presses the login button. The initial representation of user actions in the 3Dvirtual environment can be recorded as follows:
(10, 24, 91) Action = Open the office door;

(10, 24, 91) Action = Close the office door;

(4, 34, 18) Action = Typing, "F";

(4, 34, 18) Action = Typing, "A";

(4, 34, 18) Action = Typing, "L";

(4, 34, 18) Action = Typing, "C";

(4, 34, 18) Action = Typing, "O";

(4, 34, 18) Action = Typing, "N";

Fig 1: 3d password selection and inputs

7. 3D VIRTUAL ENVIRONMENT DESIGN GUIDELINES

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

7.11 Real Life Similarity The prospective 3D 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 virtual environment that users can interact

7.12 Object uniqueness and distinction every virtual object or item in the 3D 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. How ever, having similar objects such as 20 computers in one place might confuse the user. Therefore, the design of the 3D virtual environment

should consider that every object should be distinguishable from other objects. Similarly, in designing a 3D 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.

7.13 Three Dimensional Virtual Environment Size A 3D 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 password. Moreover, a large 3D virtual environment can contain a large number of virtual objects. Therefore, the probable 3D password space broadens. However, a small 3D virtual environment usually contains only a few objects, and thus, performing a 3D password will take less time.

7.14 Number of objects and their types Part of designing a 3D 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 password.

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

8. 3D PASSWORD APPLICATION

The 3D password can have a password space that is very large compared to other authentication schemes, so the 3D password's main application domains are protecting critical systems and resources.

1. Critical server many large organizations have critical servers that are usually protected by a textual password. A 3D password authentication proposes a sound replacement for a textual password.

2. Nuclear and military facilities such facilities should be protected by the most
Powerful authentication systems. The 3D password has a very large probable password space, and since it can contain token,biometrics, recognition and knowledge basedAuthentications in a single authentication system, it is a sound choice for high level security locations.

3. Airplanes and jet fighters Because of the possible threat of misusing airplanesand jet fighters for religion, political agendas, usage of such airplanes should be protected by a powerful authentication system.In addition, 3D passwords can be used in less critical systems because the

3D virtual environment can be designed to fit to any system needs. 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

Fig 2:3d man secure login with administrator ID and password

To analyze and study how secure a system is, we have to consider,

• How hard it is for the attacker to break such a system

▪ A possible measurement is based on the information content of a   password space. It is important to have a scheme that has a very large possible password space which increases the work required by the attacker to break the authentication system.

▪ Find a scheme that has no previous or existing knowledge of the most   probable user password selection.
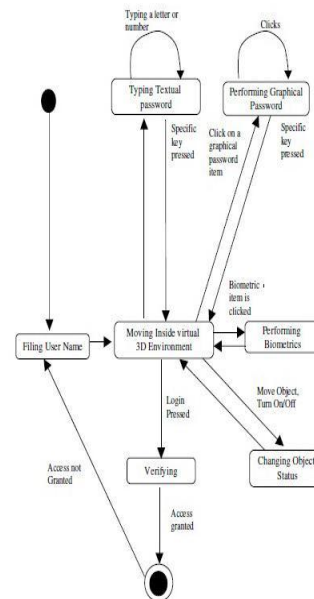

Fig 3: STATE DIAGRAM OF A 3D PASSWORD APPLICATION

9. SECURITY ANALYSIS

9.1. 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.

9.2. 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.

9.3. Attacks and Countermeasures

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.

2) Well-Studied Attack : The attacker tries to find the highest probable distribution of 3D passwords. In order to launch such an attack, the attacker has to acquire knowledge of the most probable 3D password distributions. This is very difficult because the attacker has to study all the existing authentication schemes that are used in the 3D environment. It requires a study of the user's selection of objects for the 3D password. Moreover, a well studied attack is very hard to accomplish since the attacker has to perform a customized attack for every different 3D virtual environment design. This environment has a number of objects and types of object responses that differ from any other 3D virtual environment. Therefore, a carefully customized study is required to initialize an effective attack.

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.

10. ADVANTAGES

1. Provides security.
2. This 3D password can't take by any other person.
3. 3D graphical password has no limit.
4. Password can change easily.
5. Implementation of the system is easy.
6. Password can remember easily.
7. This password helps to keep lot of personal details.

11. DISADVANTAGES

1. Difficult for blind people to use this technology.
2. Requires sophisticated computer technology.
3. Expensive.
4. A lot of program coding is required.

12. FUTURE SCOPE

The 3-D password is a multifactor authentication 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 design of the 3-D virtual environment, the selections 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. Additionally, designing a simple and easy to use 3-D virtual environment is a factor that leads to a higher user acceptability of a 3-D password system. The choice of what authentication schemes will be part of the user's 3-D password reflects the user's preferences and requirements. A user who prefers to remember and recall a password might choose textual and graphical passwords as part of their 3-D 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 3-D password. Moreover, users who prefer to keep any kind of biometrical data private might not interact with objects that require biometric information. Therefore, it is the user's choice and decision to construct the desired and preferred 3-D password. The 3-D password is still in its early stages. Designing various kinds of 3-D virtual environments, deciding on pass-word spaces, and interpreting user feedback and experiences from such environments will result in enhancing and improving the user experience of the 3-D password. Moreover, gathering attackers from different backgrounds to break the system is one of the future works that will lead to system improvement and prove the complexity of breaking a 3-D password. Moreover, it will demonstrate how the attackers will acquire the knowledge of the most probable 3-D passwords to launch their attacks. Shoulder surfing attacks are still possible and effective against 3-D passwords. Therefore, a proper solution is a field of research.

13. 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 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 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 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.

14. REFERENCES
[1] Novel 3D graphical password schema-Fawaz A Alsulaiman and Abdulmotaleb El Saddik

[1] Daniel V.Klein. Foiling the Cracker: A Survey of, and Improvement to Passwords Security

[2] Greg E. Blonder, Graphical Password, United State Patent 5559961

[3] 4.Rachna Dhamija, Adrian Perrig, Déjà Vu: A User Study Using Images for Authentication. 2000, Denver, Colorado, pages 45-58.

[4] shutterstock.com

[5] seminartopicsforcomputerscience A.com

[6] ztronicz.com

[7] 1000projects.com

[8] *en.wikipedia.org/wiki/3-D_Secure*