3-Dimensional Virtual Authentication Techniquewith Chronological Scheduling

Ragavi.E
Department of Computer Science and Engineering
Easwari Engineering College,
Anna University
Chennai 600089, India
ragavi.star@gmail.com

Srinevetha.A.R
Department of Computer Science and Engineering,
EaswariEngineering College,
Anna University
Chennai 600089, India
arsrinevetha@gmail.com

Ragavi.N
Department of Computer Science and Engineering
Easwari Engineering College,
Anna University
Chennai 600089, India
ragavirajan3108@gmail.com

Abstract—**Authentication is a process of validating who are you to whom you claimed to be or a process of identifying an individual, usually based on a username and password. We have many authentication schemes but they have some drawbacks. So, 3-D password is introduced. The 3-D password is a multifactor authentication scheme. It combines all existing authentication schemes into a single 3-D virtual environment. This 3-D virtual environment contains several objects or items with which the user can interact. The type of interaction varies from one item to another. The 3-D password is constructed by observing the actions and interactions of the user and by observing the sequences of such actions. In other words, the 3-D Password scheme is a new authentication scheme that combine RECOGNITION+RECALL+TIMESCHEDULING+TOKENS+ BIOMETRIC in one virtual authentication system. 3-D passwords are flexible and at the same time, provide a more secured system.**

Keywords-Biometrics; Brute force attack; authentication; recognition; recall; time scheduling;3Dimensional password; virtual environment.

I. INTRODUCTION

Authentication is one of the most important security services provided to a system by 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 and data related to that system securely. Many authentication algorithms are available for securing passwords. Some are effective andsecure but have certaindrawbacks. Various authentication techniques like graphical passwords, text passwords and Biometric authentication were introduced.

Normally, the authentication scheme is particularly very lenient or very strict. Throughout the years, authentication has been a very interesting approach. With the aid of latest technologies, 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 aninteresting approach towards calculation of a secret key. The algorithms are based on generating a random number in the range of 10^6 and possibilities of repetition of same number is rare.

Nowadays users are provided with various password stereotypes like textual passwords, biometric scanning, tokens or cards (such as ATM) etc. Biometric scanning is the "natural" signature and Cards or Tokens prove the validity. But some people do not like to carry their cards, some refuse to undergo strong Infrared exposure to their retinas (Biometric scanning). Nowadaystextual passwords are kept very simple say a word from the dictionary or their pet names, girlfriends, etc. Around 1990, Klein performed such tests and he could crack 10-15 passwords per day[1]. Now with the advent of new technologies, 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, Time Scheduling, Biometrics or Token based authentication [2].

Once implemented and the user logsinto a secure site, the 3D password GUI opens up.It's a three stage process.This is an additional textual password which the user can simply enter. Once the user goes through the first authentication, a 3D virtual room will open on the screen. In our case, let's say a virtual garage. Now in a day to day garage one will find all sorts of tools, equipments, etc. Each of them hasunique properties. The user will then interact with these properties accordingly. Each object in the 3D space, cannavigate around in an (x,y,z) plane.This property is common to all the objects in the space. Suppose a user logs in and enters the garage. The user sees and picks a screw-driver (initial position in xyz coordinates (5,5,5)) and moves it 5 places to theright (in XY plane i.e. (10,5,5)).That can be identified as an authentication. Similarly, another object or objects chosen by the particular user can be moved to some other specific location of the garage.Only the true user can remember and recall the objects that were moved for authentication.In this stage the Recall and Recognition part of human memory comes into play.

The second level of authentication includes the Time Scheduling Part. The true user schedules particular span of time within which the objects have to be moved.Thirdly, an additional security can be enhanced by including cards/tokens and Biometric scanner as input.In this way, the three levels of authentication of securing application is implemented.

II. EXISTING SYSTEM

Current authentication systems suffer from many weaknesses.Even the best laid plans have their faults. Textual passwords are commonly used.Users tend to choose meaningful words from dictionaries, which make textual passwords easy to break and vulnerable to Brute force attacks. Many available graphical passwords have a password space that is less than or equal to the textual password space[3]. During 2002, the total number of identity fraud cases in the UK rose by 55% to 42,029, collectively costing victims an estimated £62.5m a year, according to the credit industry fraud avoidance system [4]. Identity fraud ranges from application fraud, where someone uses a stolen identity to apply for financial products in their victim's name,to account take-over, where a fraudster obtains sufficient information on a victim's bank account (from discarded bank statements, for example) to convince the bank that they are the account holder.Many biometric authentications have already been proposed.Smart cards or tokens can be stolen.

However, users tend to resist using biometrics because of their intrusiveness and the effect on their privacy. Moreover, Biometrics cannot be revoked. The effective sample collection process in Biometric systems is strongly influenced by environmental conditions, user training and usability. For example, lighting, facial orientations, expressions, image resolution, wearing of different attires and accessories, ageing or injury.

III. 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 and recognition, time scheduled, biometrics 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 user requirements are satisfied in the proposed scheme:

1. The new scheme provides 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 aredifficult to share with others.
3. The new scheme has the provision for revoking and changing the secrets in an easy manner.

IV. BRIEF DESCRIPTION OF THE SYSTEM

Being a multi-factor authentication scheme, this scheme combines 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 timely 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 authentication schemes depends on the user's 3D password that reflects the user's preferences and requirements. 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 have more difficulty in recalling mightprefer to choose smart cards or biometrics as part of their 3D password.

V. SYSTEM IMPLEMENTATION

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, sequence of time to be followed for navigation and interaction of every object chosen by the true user, tokens to be presented and biometric data to be verified.

For example, user can enter the virtual environment and type something on a computer that exists in (x1, y1, z1) position, then enter a room that has a fingerprint recognition device that exists in a position (x2, y2, z2) and provide his/her fingerprint. Then, the user can go to the virtual garage, open the car door, and turn on the radio to a specific channel. All these actions can be scheduled and performed in a particular sequential order as set by the user.The combination and the sequence of the previous actions towards the specific objects construct the user's 3D password.

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 in the virtual environment:

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 car that can be driven;
9) A book that can be moved from one place to another;
10) Any graphical password scheme;
11) Any real life object;
12) Any upcoming authentication scheme.

The action towards an object (assume a fingerprint recognition device) that exists in location (x1,y1,z1) is different from the actions towards a similar object (another fingerprint recognition device) that exists in location (x2, y2, z2), where x1 = x2, y1 = y2 and z1 = z2. 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 and within a particular duration. If the particular duration of time within which the actions have to performed exceeds, the user has to retry. If this process repeats for more than three times, then the account gets locked.

VI. 3D PASSWORD SELECTION AND INPUT

Let us consider a 3D virtual environment space of size G ×G × G. The 3D environment space is represented by the coordinates (x, y, z) ∈ [1. . . G] × [1, . . . , G] × [1, . . . , 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, keyboard, fingerprint scanner, iris scanner, stylus, touch screen, card reader, or microphone

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 (15, 28, 80) and opens it. Then, the user closes the door. The user then finds a computer to the left, which exists in the position (3, 32, 15), and the user types "FALCON." Then, the user walks to the meeting room and picks up a pen located at (15, 28, 79) and draws only one dot in a paper located in (1, 18, 30), and position of dot 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:
(15, 28, 80) Action = Open the office door;
(15, 28, 80) Action = Close the office door;Delay (5);
(3, 32, 15) Action = Typing, "F";
(3, 32, 15) Action = Typing, "A";
(3, 32, 15) Action = Typing, "L";
(3, 32, 15) Action = Typing, "C";
(3, 32, 15) Action = Typing, "O";
(3, 32, 15) Action = Typing, "N";Delay (10);
(15,28,79)Action= "Picks up the pen";
(330,130)Action = "Presses the login button";

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 security requirements. The design of 3D virtual environments should follow these guidelines:

1. *Real life similarity*: The prospective 3D virtual environment should reflect real life scenario that people face in their day to day 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.
2. *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 [5]. Thus, the prospective interaction with object1 is not equal to the interaction with object2. However, having similar objects such as 20 computers in one place might confuse the user. Therefore, the design of the 3D virtual environment should be such that every object should be distinguishable from other objects.Similarly, while 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.

Figure 1. Objects uniqueness and disitinction in a 3D virtual environment

3. *Three Dimensional Virtual Environment Size*: A 3D virtual environment can depict a city, country or even the world. On the other hand, it can depict a space 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.

Figure 2: Snapshot of virual office
and meeting environment

4. *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. Selecting the right object response types and the number of objects affects the probable password space of a 3D password.

Figure 3. Objects in a study room
3D virtual environment

5. *System Importance*: 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.

VII. 3D PASSWORDAPPLICATION

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 for security issues. Few applications that require 3D passwords are discussed below

1. Critical server

Many large organizations have critical servers that are usually protected by a textual password. 3D password authentication provides better security than a textual password.

2. Nuclear and military systems

Applications supporting Nuclear and military systems should be protected by most powerful authentication systems. 3D password authentication has a very large password space, and since it can contain token, biometrics, recognition and knowledge based authentications in a single authentication system, it is the best choice for high level security systems.

3. Airplanes and Jet fighters

Because of the possible threat of misusing airplanes and jet fighters for religion and political agendas, they should be protected by a powerful authentication system.

In addition to the above scenarios, 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:

1. Personal Digital Assistance
2. Desktop Computers and laptop logins
3. Web Authentication
4. Security Analysis

VIII. 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.

3D Password distribution knowledge

Users tend to use meaningful words for textual passwords. Every user has different requirements and preferences when selecting the appropriate 3DPassword. 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.

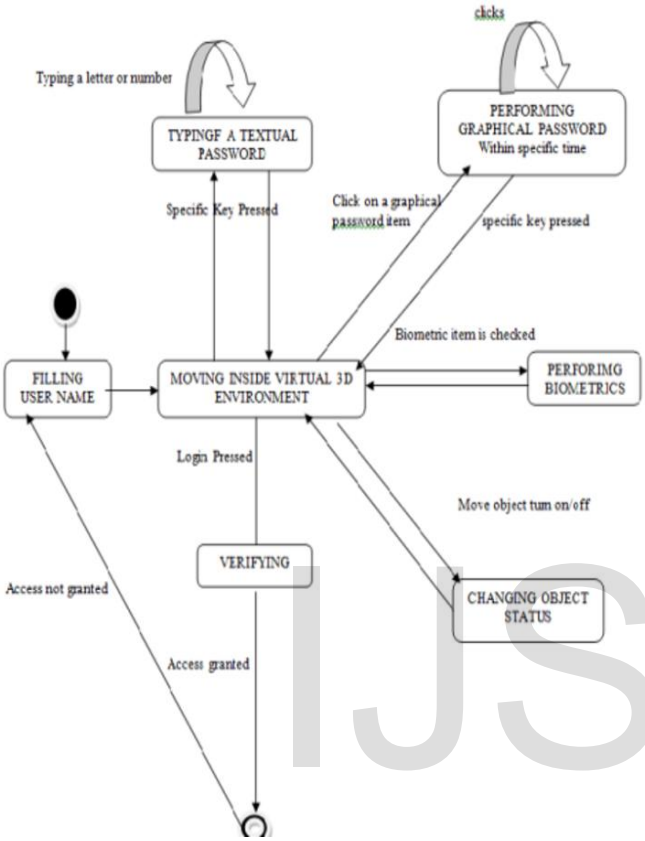

Figure4. State diagram of a 3D password application showing X attacks and counter measures

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 customized study is required to initialize an effective attack which is a cumbersome task.

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 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.

IX. 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 [6]. Almost 8 users have tested the experimental environment. Nearly 90% we have succeeded in our Experimental Virtual Three-Dimensional Environment.

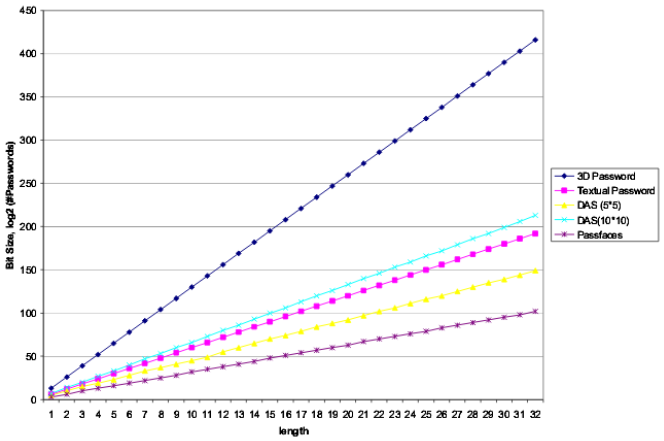

Figure5. A comparison between object password, biometrics and textual password

X.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 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.

In 3D password system as number of series of action and interaction in the hypothetical 3D application increases the length of the code word also increases. The amount of memory that is required to store a 3D password is large when compared to a textual password.

There are two applications in which the space required to store the 3D password is reduced. The first application is a chess game in which user creates the 3D password by moving the chess pieces in valid places on chessboard. The second application is a cube in which user constructs the 3D password by moving the cube left, right, up, down and by turning around the axis of the cube along with choice of placing the input images on each side of cube. In the secondapplication, cube without any image input, a user can perform a greater number of actions and interactions as compared with first application and it is noticed that the region necessary to store the 3D password is comparatively very less, and the password created is very strong.

REFERENCES

[1] D. V. Klein, “Foiling the cracker: A survey of, and improvement to passwords security,” in Proc. USENIX Security Workshop, 1990, pp. 5–14.

[2] T. Kitten, Keeping an Eye on the ATM. (2005, Jul. 11). [Online]. Available: ATMMarketPlace.com

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

[4] BBC news, Cash Machine Fraud up, Say Banks, Nov. 4, 2006.

[5] R. Dhamija and A. Perrig, “Déjà Vu: A user study using images for authentication,” in Proc. 9th USINEX Security Symp., Denver, CO, Aug. 2000, pp. 45–58.

[6]G. E. Blonder, “Graphical password,” U.S. Patent 5 559 961, Sep. 24, 1996.