A Secure Authentication Mechanism using 3D Password

Mr. Namdev A. Anwat **Mr. Dattatray S. Shingate** **Dr. Varsha H. Patil**

Department of Computer Engineering,
Matoshri College of Engineering,
Eklahare, Nashik, Maharashtra, India – 422105
namdev.anwat@gmail.com
ursdattu@gmail.com

***Abstract*— A secure authentication system is the important aspect of any computer based system but current authentication system suffers from many weaknesses. Textual passwords are the most commonly used mechanism but many users never follow the requirements of password selection. Due to user's habit of choosing meaningful words for password, it can be easily breakable and vulnerable to many attacks. The physical instruments, smart cards or debit cards can be stolen. Many users resist the biometric system because of their intrusive responses and their effects on privacy.**

In this paper, we present and evaluate our contribution, i.e. A secure authentication mechanism using 3D password. It is a multifactor authentication scheme. For authentication purpose, here we use a 3D virtual environment where user interact and navigate with various objects. The sequence of actions and interactions towards the objects inside 3D environment constructs the 3D password for user. It combines the existing authentication schemes such as textual passwords, graphical passwords and various types of biometrics into 3D environment. The environment and selected objects determine the 3D key space for password.

***Key Words* — Authentication, graphical passwords, biometrics, textual passwords, 3D passwords, 3D environment.**

I. INTRODUCTION

The increased usage of computer applications has given a rise for many security concerns. Out of these security concerns the authentication is one of the most serious issues of security. Authentication is a process of validating who you are and to whom you claimed to be. In general, human authentication techniques can be classified as knowledge based (what you know), token based (what you have), and biometrics (what you are).

Knowledge-based authentication can be further divided into two categories as follows: 1) recall based and 2) recognition based [1]. Recall-based techniques require the user to repeat or reproduce a secret that the user created before. Recognition based techniques require the user to identify and recognize the secret, or part of it, that the user selected before [1]. One of the most common recall-based authentication schemes used in the computer world is textual passwords. One major drawback of the textual password is its two conflicting requirements: the selection of passwords that are easy to remember and, at the same time, are hard to guess.

Klein [2] collected the passwords of nearly 15000 accounts that had alphanumerical passwords and he reached the following observation: 25% of the passwords were guessed by using a small yet well-formed dictionary of 3×10^6 words. Furthermore, 21% of the passwords were guessed in the first week and 368 passwords were guessed within the first 15 min. Klein [2] stated that by looking at these results in a system with about 50 accounts, the first account can be guessed in 2 min and 5–15 accounts can be guessed in the first day. Klein [2] showed that even though the full textual password space for eight-character passwords consisting of letters and numbers is almost 2×10^{14} possible passwords, it is easy to crack 25% of the passwords by using only a small subset of the full password space. It is important to note that Klein's experiment was in 1990 when the processing capabilities, memory, networking, and other resources were very limited compared to today's technology.

Many authentication systems, particularly in banking, require not only what the user knows but also what the user possesses (token-based systems). However, many reports [3]–[5] have shown that tokens are vulnerable to fraud, loss, or theft by using simple techniques.

Graphical passwords can be divided into two categories as follows: 1) recognition based and 2) recall based [1]. Various graphical password schemes have been proposed [6]–[8], [10]–[12]. Graphical passwords are based on the idea that users can recall and recognize pictures better than words. However, some of the graphical password schemes require a long time to be performed. Moreover, most of the graphical passwords can be easily observed or recorded while the legitimate user is performing the graphical password; thus, it is vulnerable to shoulder surfing attacks. Currently, most graphical passwords are still in their research phase and require more enhancements and usability studies to deploy them in the market.

Many biometric schemes have been proposed; fingerprints, palm prints, hand geometry, face recognition, voice recognition, iris recognition, and retina recognition are all different biometric schemes. Each biometric recognition scheme has its advantages and disadvantages based on several factors such as consistency, uniqueness, and acceptability. One of the main drawbacks of applying biometrics is its intrusiveness upon a user's personal characteristic. Moreover, retina biometrical recognition

schemes require the user to willingly subject their eyes to a low-intensity infrared light. In addition, most biometric systems require a special scanning device to authenticate users, which is not applicable for remote and Internet users.

In this paper, we comprehensively analyze and discuss the 3-D password [16]. The 3-D password is a multifactor authentication scheme. It can combine 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.

It is the user's choice to select which type of authentication techniques will be part of their 3-D password. This is achieved through interacting only with the objects that acquire information that the user is comfortable in providing and ignoring the objects that request information that the user prefers not to provide. For example, if an item requests an iris scan and the user is not comfortable in providing such information, the user
simply avoids interacting with that item. Moreover, giving the user the freedom of choice as to what type of authentication schemes will be part of their 3-D password and given the large number of objects and items in the environment, the number of possible 3-D passwords will increase. Thus, it becomes much more difficult for the attacker to guess the user's 3-D password.

The remainder of this paper is organized as follows: Section II discusses related works. Section III introduces the 3-D password. It also discusses the guidelines of building the 3-D virtual environment and its possible applications. Section IV discusses the security analysis, including possible attacks and countermeasures. Section V presents the experimental results. Finally, Section VI concludes and discusses future work.

II. RELATED WORKS

Many graphical password schemes have been proposed [6]–[8], [10]–[12]. Blonder [6] introduced the first graphical password schema. Blonder's idea of graphical passwords is that by having a predetermined image, the user can select or touch regions of the image causing the sequence and the location of the touches to construct the user's graphical password. After Blonder [6], the notion of graphical passwords was developed. Many graphical password schemes have been proposed. Existing graphical passwords can be categorized into two categories as follows: 1) recall based and 2) recognition based [1].

Dhamija and Perrig [7] proposed Déjà Vu, which is a recognition-based graphical password system that authenticates users by choosing portfolios among decoy portfolios. These portfolios are art randomized portfolios. Each image is derived from an 8-B seed. Therefore, an authentication server does not need to store the whole image; it simply needs to store the 8-B seed. Another recognition-based graphical password is Passfaces [8]. Passfaces simply works by having the user select a subgroup of k faces from a group of n faces. For authentication, the system shows m faces and one of the faces belongs to the subgroup k. The user has to do the selection many times to complete the authentication process. Another scheme is the Story scheme [9], which requires the selection of pictures of objects (people, cars, foods, airplanes, sightseeing, etc.) to form a story line. Davis *et al.* [9] concluded that the user's choices in Passfaces and in the Story scheme result in a password space that is far less than the theoretical entropy. Therefore, it leads to an insecure authentication scheme.

The graphical password schema of Blonder [6] is considered to be recall based since the user must remember selection locations. Moreover, PassPoint [10]–[12] is a recall-based graphical password schema, where a background picture is presented and the user is free to select any point on the picture as the user's password (user's PassPoint). Draw A Secret (DAS), which is a recall-based graphical password schema and introduced by
Jermyn *et al.* [13], is simply a grid in which the user creates a drawing. The user's drawings, which consist of strokes, are considered to be the user's password. The size and the complexity of the grid affect the probable password space. Larger grid sizes increase the full password space. However, there are limitations in grid complexity due to human error. It becomes very hard to recall where the drawing started and ended and where the middle points were if we have very large grid sizes.

One important type of authentication is based on who you are or, in other words, biometrics. Biometric recognition systems have been exhaustively studied as a way of authentication. Fingerprints, palmprints, face recognition, voice recognition, and iris and retina recognition are all different methodologies of biometric recognition systems. However, some human properties are vulnerable to change from time to time due to several reasons such as aging, scarring, face makeup, change of hairstyle, and sickness (change of voice). Moreover, people tend to resist biometrics for different reasons. Some people think that keeping a copy of the user's fingerprints is not acceptable and is a threat to the user's privacy. In addition, some users resist the idea of a low-intensity infrared light or any other kind of light directed at their eyes, such as in retina recognition systems. Moreover, biometrics cannot be revoked, which leads to a dilemma in case the user's data have been forged. Unlike other authentication schemes where the user can alter his/her textual password in case of a stolen password or replace his/her token if it has been stolen or forged, a user's biometrics cannot be revoked.

Many authentication systems are based on tangible objects and are referred to as token-based systems. Many token-based systems are vulnerable to theft and loss. Therefore, most token based systems require a personal identification number (PIN) for authentication. The 3-D password [16] has been proposed and initial results have been presented.

III. 3D PASSWORD SCHEME

In this section, we present a multifactor authentication scheme that combines the benefits of various authentication

schemes. We attempted to satisfy the following requirements.

1. The new scheme should not be either recall based or recognition based only. Instead, the scheme should be a combination of recall-, recognition-, biometrics-, and token-based authentication schemes.
2. Users ought to have the freedom to select whether the 3-D 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. Some users do not like to carry cards. Some users do not like to provide biometrical data, and some users have poor memories. Therefore, to ensure high user acceptability, the user's freedom of selection is important.
3. The new scheme should provide secrets that are easy to remember and very difficult for intruders to guess.
4. The new scheme should provide secrets that are not easy to write down on paper. Moreover, the scheme secrets should be difficult to share with others.
5. The new scheme should provide secrets that can be easily revoked or changed.

Based on the aforementioned requirements, we propose our contribution, i.e., the 3-D password authentication scheme.

A. 3D Password Overview

The 3-D password is a multifactor authentication scheme. The 3-D password presents a 3-D virtual environment containing various virtual objects. The user navigates through this environment and interacts with the objects. The 3-D password is simply the combination and the sequence of user interactions that occur in the 3-D virtual environment. The 3-D password can combine recognition-, recall-, token-, and biometrics-based systems into one authentication scheme. This can be done by designing a 3-D virtual environment that contains objects that request information to be recalled, information to be recognized, tokens to be presented, and biometrical data to be verified. For example, the user can enter the virtual environment and type something on a computer that exists in (x_1, y_1, z_1) position, then enter a room that has a fingerprint recognition device that exists in a position (x_2, y_2, z_2) 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. The combination and the sequence of the previous actions toward the specific objects construct the user's 3-D 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 3-D environment toward the virtual objects. Moreover, any user input (such as speaking in a specific location) in the virtual 3-D environment can be considered as a part of the 3-D 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 biometrical 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 3-D 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.

B. 3D Password Selection and Inputs

Let us consider a 3-D virtual environment space of size $G \times G \times G$. The 3-D 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 3-D virtual environment with unique (x, y, z) coordinates. We assume that the user can navigate into the 3-D virtual environment and interact with the objects using any input device such as a mouse, keyboard, 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 3-D password. For example, consider a user who navigates through the 3-D 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 3-D virtual 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”;
(10, 24, 80) Action = Pick up the pen;
(1, 18, 80) Action = Drawing, point = (330, 130).

This representation is only an example. The extensive real representation will not be discussed in this paper. In order for a legitimate user to be authenticated, the user has to follow the same sequence and type of actions and interactions toward the objects for the user’s original 3-D password. Fig. 1 shows a virtual computer that accepts textual passwords as a part of a user’s 3-D password.

Fig.1: Snapshot of a proof-of-concept 3-D virtual environment, where the user is typing a textual password on a virtual computer as a part of the user’s 3-D password.

Fig.2: Snapshot of a proof-of-concept virtual art gallery, which contains 36 pictures and six computers.

Three-dimensional virtual environments can be designed to include any virtual objects. Therefore, the first building block of the 3-D password system is to design the 3-D virtual environment and to determine what objects the environment will contain. In addition, specifying the object’s properties is part of the system design. The design of the 3-D virtual environment influences the overall password space, usability, and performance of the 3-D password system. Fig. 2 shows a snapshot of an experimental 3-D virtual environment.

To simplify the idea of how a 3-D password works, Fig. 3 shows a state diagram of a possible 3-D password authentication system.

C. 3D Virtual Environment Guidelines

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

1. *Real-life similarity:* The prospective 3-D 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 3-D virtual environment that users can interact with, by using common sense.
2. *Object uniqueness and distinction:* Every virtual object or item in the 3-D 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 3-D virtual environment should consider that every object should be distinguishable from other objects. A simple real-life example is home numbering. Assume that there are 20 or more homes that look like each other and the homes are not numbered. It would be difficult to distinguish which house was visited a month ago. Similarly, in designing a 3-D 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 3-D 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. The size of a 3-D environment should be carefully studied. A large 3-D virtual environment will increase the time required by the user to perform a 3-D password. Moreover, a large 3-D virtual environment can contain a large number of virtual

objects. Therefore, the probable 3-D password space broadens. However, a small 3-D virtual environment usually contains only a few objects, and thus, performing a 3-D password will take less time.

4. *Number of objects (items) and their types:* Part of designing a 3-D 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 3-D password.
5. *System importance:* The 3-D virtual environment should consider what systems will be protected by a 3-D password. The number of objects and the types of objects that have been used in the 3-D virtual environment should reflect the importance of the protected system.

D. 3D Password Applications

Because a 3-D password can have a password space that is very large compared to other authentication schemes, the 3-D password's main application domains are protecting critical systems and resources. Possible critical applications include the following.

1. *Critical servers:* Many large organizations have critical servers that are usually protected by a textual password. A 3-D password authentication proposes a sound replacement for a textual password. Moreover, entrances to such locations are usually protected by access cards and sometimes PIN numbers. Therefore, a 3-D password can be used to protect the entrance to such locations and protect the usage of such servers.
2. *Nuclear and military facilities:* Such facilities should be protected by the most powerful authentication systems. The 3-D password has a very large probable password space, and since it can contain token-, biometrics-, recognition-, and knowledge-based authentications in a single authentication system, it is a sound choice for high level security locations.
3. *Airplanes and jetfighters:* Because of the possible threat of misusing airplanes and jetfighters for religio-political agendas, usage of such airplanes should be protected by a powerful authentication system. The 3-D password is recommended for these systems.

In addition, 3-D passwords can be used in less critical systems because the 3-D virtual environment can be designed to fit any system's needs. A small 3-D virtual environment can be used in many systems, including the following:

1) ATMs;
2) Personal digital assistants;
3) Desktop computers and laptop logins;
4) Web authentication.

IV. SECURITY ANALYSIS

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, which is defined in [13] as "the entropy of the probability distribution over that space given by the relative frequencies of the passwords that users actually choose." We have seen that textual password space may be relatively large; however, an attacker might only need a small subset of the full password space as Klein [2] observed to successfully break such an authentication system. As a result, it is important to have a scheme that has a very large possible password space as one factor for increasing the work required by the attacker to break the authentication system. Another factor is to find a scheme that has no previous or existing knowledge of the

Most probable user password selection, which can also resist the attack on such an authentication scheme. In Section IV-A, we will discuss the size of the 3-D password space. Then, we will study the knowledge distribution of the 3-D password. Afterward, we will analyze the possible attacks on the 3-D password.

D. 3D Password Space Size

One important factor to determine how difficult it is to launch an attack on an authentication system is the size of the password space. To determine the 3-D password space, we have to count all possible 3-D passwords that have a certain number of actions, interactions, and inputs toward all objects that exist in the 3-D virtual environment.We assume that the length of the 3-D password is L_{max}, and the probability of the 3-D password of size greater than L_{max} is zero. To measure the 3-D password space, we will calculate_(L_{max},G) on a 3-D virtual environment that has the space ($G \times G \times G$) for a 3-D password of a length (number of actions, interactions, and inputs) of L_{max} or less. In the following expression, AC represents the possible actions toward the 3-D virtual environment, whereas_represents the total number of possible 3-D passwords of length L_{max} or less:

$$\prod(L_{\max}, G) = \sum_{n=1}^{n=L_{\max}} (m + g(AC))^n . \qquad (1)$$

In the following expression (2), O_{max} is the number of objects in the 3-D virtual environment:

$$m = \sum_{i=1}^{i=O^{\max}} h(O_i, T_i, x_i, y_i, z_i) \qquad (2)$$

Where $x_i = x_j$, $y_i = y_j$, and $z_i = z_j$, only if $i = j$. The design of the 3-D environment will determine the value of O_{max}. The variable m represents all possible actions and interactions toward all existing objects O_i. However, $g(AC)$ counts the total number of actions and inputs

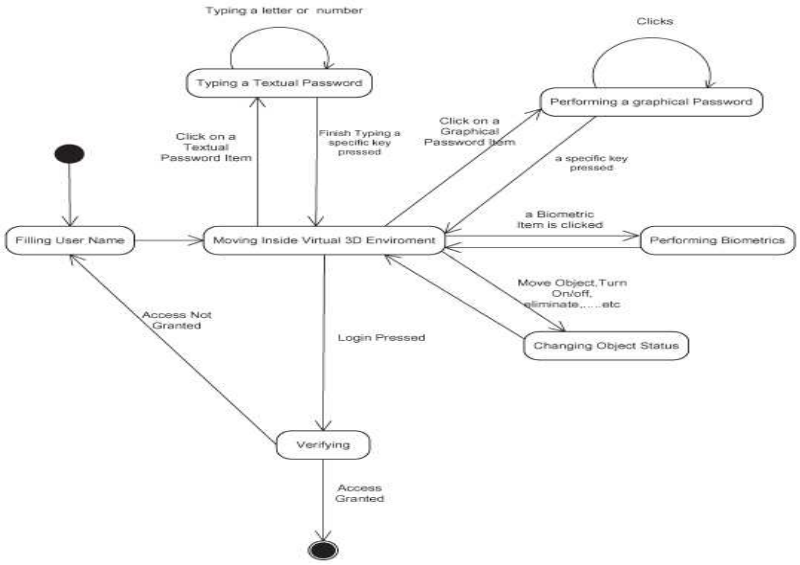

Fig.3: State diagram of a possible 3-D password application.

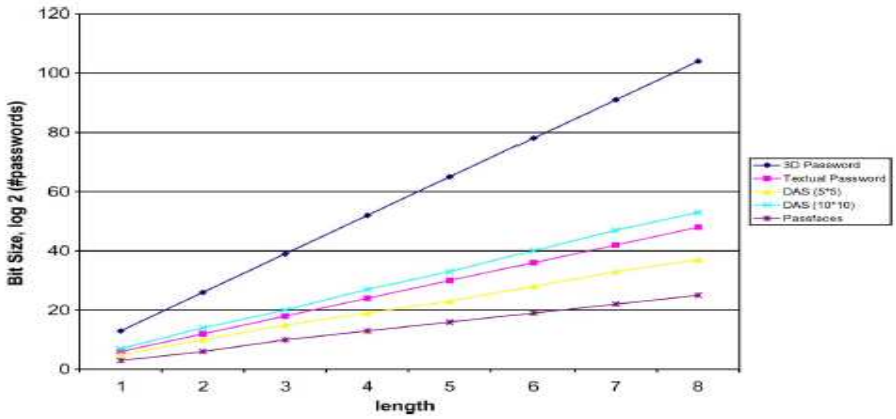

Fig.4: Password space of the 3-D password, textual password, Passfaces, and DAS with grid sizes of 5 × 5 and 10 × 10. Length is the number of actions and interactions for a 3-D password, the number of characters for textual passwords, the number of selections for Passfaces, and the number of points that represent the strokes for DAS. The length is up to eight (characters/actions, interactions, inputs/selections). The 3-D password virtual environment is as specified in Section V-A; bit size is the $\log_2$ of the entire probable password space.

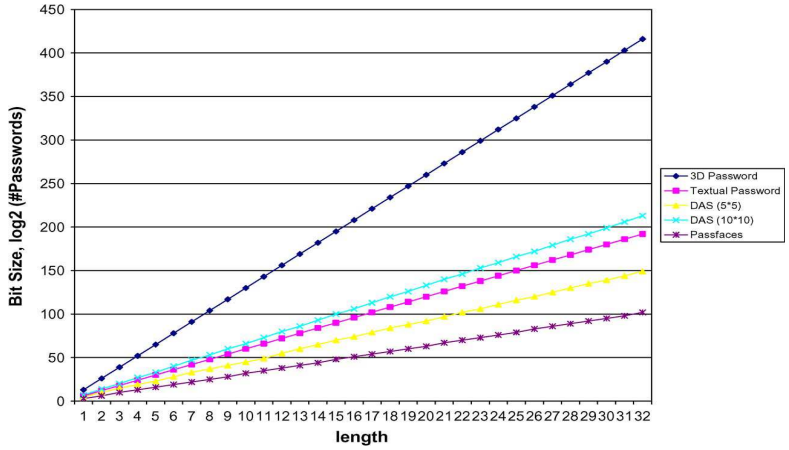

Fig.5: Password space of the 3-D password, textual password, Passfaces, and DAS with grid sizes of 5 × 5 and 10 × 10. Length is the number of actions and interactions for a 3-D password, the number of characters for textual passwords, the number of selections for Passfaces, and the number of points that represent the strokes for DAS. The length is up to eight (characters/actions, interactions, inputs/selections). The 3-D password virtual environment is as specified in Section V-A; bit size is the $\log_2$ of the entire probable password space.

toward the 3-D virtual environment, whereas m, as we mentioned before, counts the actions and interactions toward the objects. An example of $g(AC)$ can be a user movement pattern, which can be considered as a part of the user's 3-D password. The function:

$$h(O_i, T_i, x_i, y_i, z_i) = f(O_i, T_i, x_i, y_i, z_i) \qquad (3)$$

is the number of possible actions and interactions toward the object O_i based on the object type T_i. Object types can be textual password objects, DAS objects, or any authentication scheme.

The function f is determined from the object type. It counts the possible actions and interactions that the object can accept. If we assume that an object "Keyboard" is in location (x_0, y_0, z_0) of type = textual password, f will count the possible characters and numbers that can be typed, which is around 93 possibilities. As we mentioned before, an object type is one of the important factors that affects the overall password space. Therefore, higher outcomes of function f means larger 3-D password space size.

From the previous equations, we observe that the number of objects and the type of actions and interactions determines the probable password space. Therefore, the design of the 3-D virtual environment is a very critical part of the 3-D password system. Figs. 4 and 5 illustrate the resulting password space of the proposed 3-D password compared to textual password, Passfaces, and DAS of a grid of 5 × 5 and 10 × 10, respectively. Notice the difference between a 3-D password built on a simple 3-D virtual environment compared to the other authentication schemes.

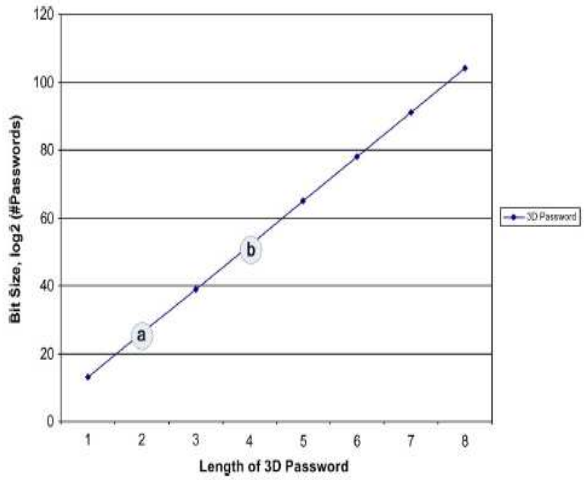

Fig. 6. Observing the number of possible actions/interactions of a 3-D password within a 3-D environment specified in Section V-A compared to the two critical points of textual passwords. Point "a" is the bit size of Klein [2] (3×10^6) dictionary of eight-character textual passwords. Point "b" represents the full password space of eight-character textual passwords.

Fig. 6 shows the points where the 3-D password exceeds two important textual password points. Point "a" shows that by having only two actions and interactions as a 3-D password, the 3-D password exceeds the number of textual passwords used by Klein [2] to break 25% of textual passwords of eight characters. Point "b" represents the full textual password space of eight characters or less. It shows that by performing only four interactions, actions, and inputs as a 3-D password, the 3-D password space exceeds the full textual passwords of eight characters or less.

E. 3D Password Distribution Knowledge

Studying the user's behavior of password selection and knowing the most probable textual passwords are the key behind dictionary attacks. Klein [2] used such knowledge to collect a small set of 3×10^6 words that have a high probability of usage among users. The question is how has such information (highly probable passwords) been found and why. Users tend to choose words that have meaning, such as places, names, famous people's names, sports terms, and biological terminologies. Therefore, finding these different words from the dictionary is a relatively simple task. Using such knowledge yields a high success rate for breaking textual passwords. Any authentication scheme is affected by the knowledge distribution of the user's secrets. According to Davis *et al.* [9], Passfaces[8] users tend to choose faces that reflect their own taste on facial attractiveness, race, and gender. Moreover, 10% of male passwords have been guessed in only two guesses. Another study [14] about user selection of DAS [13] concluded that for their secret passwords, users tend to draw things that have meaning, which simplifies the attacker's task.

Currently, knowledge about user behaviors on selecting their 3-D password does not exist. Every user has different requirements and preferences when selecting the appropriate 3-D password. This fact will increase the effort required to find a pattern of user's highly selected 3-D password. In addition, since the 3-D 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. For textual password, the highly probable selected textual password might be determined by the use of dictionaries. However, there are many authentication schemes with undiscovered probable password space. Since every 3-D password system can be designed according to the protected system requirements, the attacker has to separately study every 3-D password system. This is because objects that exist in one 3-D password system might not exist on other 3-D password systems. Therefore, more effort is required to build the knowledge of most probable 3-D passwords.

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

1. Time required to login: The total time needed for a legitimate user to login may vary from 20 s to 2 min or more, depending on the number of interactions and actions, the size of the 3-D virtual environment, and the type of actions and interactions done by the user as a 3-D password. Therefore, a brute force attack on a 3-D password is very difficult and time consuming.
2. Cost of attacks: In a 3-D virtual environment that 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 3-D password is more challenging. Moreover, the high number of possible 3-D password spaces (as shown in Table I) leaves the attacker with almost no chance of breaking the 3-D password.

Well-Studied Attack: The attacker tries to find the highest probable distribution of 3-D passwords. However, to launch such an attack, the attacker has to acquire knowledge of the most probable 3-D password distributions. Acquiring such knowledge is very difficult because the attacker has to study all the existing authentication schemes that are used in the 3-D environment. Moreover, acquiring such knowledge may require forging all existing biometrical data and may require forging token-based data. In addition, it requires a study of the user's selection of objects, or a combination of objects, that the user will use as a 3-D password. Moreover, a well-studied attack is very hard to accomplish since the attacker has to perform a customized attack for every different 3-D virtual environment design. Every system can be protected by a 3-D password that is based on a unique 3-D virtual environment. This environment has a number of objects and types of object responses that differ from any other 3-D virtual environment. Therefore, a carefully, customized study is required to initialize an effective attack.

TABLE I
RESULTING NUMBER OF POSSIBLE 3-D PASSWORDS OF TOTAL LENGTH L_{max} IN A 3-D VIRTUAL ENVIRONMENT AS SPECIFIED IN SECTION V-A

# of Actions, Interactions and Inputs (L_{max})	Log_2 (# of 3D Passwords)	# of Actions, Interactions and Inputs (L_{max})	Log_2 (# of 3D Passwords)
1	13	17	221
2	26	18	234
3	39	19	247
4	52	20	260
5	65	21	273
6	78	22	286
7	91	23	299
8	104	24	312
9	117	25	325
10	130	26	338
11	143	27	351
12	156	28	364
13	169	29	377
14	182	30	390
15	195	31	403
16	208	32	416

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

Timing Attack: In this attack, the attacker observes how long it takes the legitimate user to perform a correct sign-in using the 3-D password. This observation gives the attacker an indication of the legitimate user's 3-D 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 3-D virtual environment is poorly designed.

V. EXPERIMENTAL RESULTS

We have built an experimental 3-D virtual environment that contains several objects of two types. The first type of response is the textual password. The second type of response is requesting graphical passwords. Almost 30 users volunteered to experiment with the environment. We asked the users to create their 3-D password and to sign-in using their 3-D password several times over several days.

G. Experimental Virtual 3D Environment

In our experiment, we have used Java Open GL to build the 3-D virtual environment and we have used a 1.80-GHz Pentium M Centrino machine with 512-MB random access memory and ATI Mobility Radeon 9600 video card. The design of the experimental 3-D virtual environment represents an art gallery that the user can walk through and is depicted in Fig. 2.

H. User Study

We conducted a user study on 3-D passwords using the experimental 3-D virtual environments. The study reviewed the usage of textual passwords and other authentication schemes. The study covered almost 30 users. The users varied in age, sex, and education level. Even though it is a small set of users, the study produced some distinct results [13], [15]. We observed the following regarding textual

passwords, 3-D passwords, and other authentication schemes.

1. Most users who use textual passwords of 9–12 character lengths or who use random characters as a password have only one to three unique passwords.
2. More than 50% of user's textual passwords are eight characters or less.
3. Almost 25% of users use meaningful words as their textual passwords.
4. Almost 75% of users use meaningful words or partially meaningful words as their textual passwords. In contrast, only 25% of users use random characters and letters as textual passwords.
5. Over 40% of users have only one to three unique textual passwords, and over 90% of users have eight unique textual passwords or less.
6. Over 90% of users do not change their textual passwords unless they are required to by the system.
7. Over 95% of users under study have never used any graphical password scheme as a means of authentication.
8. Most users feel that 3-D passwords have a high acceptability.
9. Most users believe that there is no threat to personal privacy by using a 3-D password as an authentication scheme.

VI. CONCLUSION AND FUTURE WORK

There are many authentication schemes in the current state. 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. Among the various authentication schemes, textual password and token-based schemes, or the combination of both, are commonly applied. However, 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.

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 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 password 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.

REFERENCES

[1]. 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.

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

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

[4]. T. Kitten, *Keeping an Eye on the ATM*. (2005, Jul. 11). [Online]. Available: ATMMarketPlace.com BBC news, *Cash Machine Fraud up, Say Banks*, Nov. 4, 2006.

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

[6]. 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.

[7]. Real User Corporation, *The Science Behind Passfaces*. (2005, Oct.). [Online]. Available: http://www.realusers.com D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes," in *Proc. 13th USENIX Security Symp.*, San Diego, CA, Aug. 2004, pp. 1–14.

[8]. S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Effects of tolerance and image choice," in *Proc. Symp. Usable Privacy Security*, Pittsburgh, PA, Jul. 2005, pp. 1–12.

[9]. S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, " Authentication using graphical passwords: Basic results," in *Proc. Human-Comput. Interaction Int.*, Las Vegas, NV, Jul. 25–27, 2005.

[10]. S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system," *Int. J. Human-Comput. Stud. (Special Issue on HCI Research in Privacy and Security)*, vol. 63, no. 1/2, pp. 102–127, Jul. 2005.

[11]. 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.

[12]. J. Thorpe and P. C. van Oorschot, "Graphical dictionaries and the memorable space of graphical passwords," in *Proc. USENIX Security*, San Diego, CA, Aug. 9–13, 2004, p. 10.

