Virtual Realization using 3D Password

A.B. Gadicha 1, V.B. Gadicha 2,
1,2 Department of Computer Science & Engineering
1,2 P.R. Patil College of Engg & Technology, Amravati, India
Email- 1 ajjugadicha@gmail.com

Abstract- Current authentication systems suffer from many weaknesses. Textual passwords are commonly used; however, users do not follow their requirements. 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. In this paper, we present and evaluate our contribution, i.e., the 3D password. The 3D password is a multifactor authentication scheme. To be authenticated, we present a 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 design of the 3D virtual environment and the type of objects selected determine the 3D password key space.

1. INTRODUCTION

The dramatic increase of computer usage has given rise to many security concerns. One major security concern is authentication, which is the process of validating who you are 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. 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. 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 collected the passwords of nearly 15,000 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 $3 \times 10^6$ words. Klein showed that even though the full textual password space for eight-character passwords consisting of letters and numbers is almost $2 \times 10^{14}$ 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 – 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. Various graphical password schemes have been proposed. 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.

The 3D password is a multifactor 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 type of interaction varies from one item to another. The 3D password is constructed by observing the actions and interactions of the user and by observing the sequences of such actions.[1-2]

2. RELATED WORKS

Many graphical password schemes have been proposed. Blonder 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, 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. Recognition-based graphical password is Passfaces. 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, which requires the selection of pictures of objects (people, cars, foods, airplanes, sightseeing, etc.) to form a story line. Davis et al. 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 is considered to be recall based since the user must remember selection locations. Moreover, Pass Point – 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 Pass Point). Draw A Secret (DAS), which is a recall-based graphical password schema and introduced by Jermyn et al., 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 [2].

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, palm prints, 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 3D password has been proposed, and initial results have been presented.

3. 3D PASSWORD IMPLEMENTATION

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 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. 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.

3.1. 3D Password Overview

The 3D password is a multifactor 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 biometrical data to be verified.

For example, the 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. The combination and the sequence of the previous actions toward 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:

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 3D password, the user must follow the same scenario performed by the legitimate user.

### 3.2. 3D Password Selection and Inputs

Let us consider a 3D virtual environment space of size \(G \times G \times G\). The 3D environment space is represented by the coordinates \((x, y, z) \in [1. . . G] \times [1. . . G] \times [1. . . G]\). 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, 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 3D virtual environment can be recorded as follows:

\[(10, 24, 91)\] Action = Open the office door;
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 3D password. Three-dimensional virtual environments can be designed to include any virtual objects. Therefore, the first building block of the 3D password system is to design the 3D 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 3D virtual environment influences the overall password space, usability, and performance of the 3D password system [1].

3.3. 3D Virtual Environment Design Guidelines

Designing a well-studied 3D virtual environment affects the usability, effectiveness, and acceptability of a 3D password system. Therefore, 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.

1) **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 with, by using common sense.

2) **Object uniqueness and distinction:** Every virtual object/item in the 3D virtual environment is different from many other virtual objects. The uniqueness comes from the fact that every virtual object has its own attributes such as

(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).

Figure 2 3D Virtual Environment of HARD ROCK CAFE
position. Thus, the prospective interaction with object 1 is not equal to the interaction with object 2. However, having similar objects such as 20 computers in one place might confuse the user. Therefore, the design of the 3D virtual environment should consider that every object should be distinguishable from other objects. 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.

3) 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. The size of a 3D environment should be carefully studied. 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.

4) Number of objects (items) 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.

5) 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.

4. 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 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 observed to successfully break 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.

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 3D 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 seconds to 2 min or more, depending on the number of interactions and actions, the size of the 3D virtual environment, and the type of actions and interactions done by the user as a 3D password. Therefore, a brute force attack on a 3D password is very difficult and time consuming.

2) Cost of attacks: In a 3D 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 3D password is more challenging. Moreover, the high number of possible 3D password spaces leaves the attacker with almost no chance of breaking the 3D password[1].
**Well-Studied Attack:** The attacker tries to find the highest probable distribution of 3D passwords. However, to launch such an attack, the attacker has to acquire knowledge of the most probable 3D password distributions. Acquiring such knowledge is very difficult because the attacker has to study all the existing authentication schemes that are used in the 3D 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 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. Every system can be protected by a 3D password that is based on a unique 3D virtual environment. This environment as 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 [1].

**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 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 3D password. Therefore, we assume that the 3D 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 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 [1].

5. 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. Moreover, there are some other important authentication schemes that are based on what you have, such as smart cards. Among the various authentication schemes, textual password and token-based schemes, or the combination of both, are commonly applied. However, 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 3D password is a multifactor authentication scheme that combines these various authentication schemes into a single 3D 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. 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 passwords 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, 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 3D password. The 3D password is still in its early stages. Designing various kinds of 3D 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 3D 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 3D password. Moreover, it will demonstrate how the attackers will acquire the knowledge of the most probable 3D passwords to launch their attacks. Shoulder surfing attacks are still possible and effective against 3D passwords. Therefore, a proper solution is a field of research [1].

6- REFERENCES


Virtual Realization using 3D Password

“Graphical Passwords: A Survey” by Xiaoyuan Suo, Ying Zhu and G. Scott Owen, Department of Computer Science, Georgia State University.