INTELLIGENT INDEMNITY USING 3D PASSWORD

Aman Gupta*

*PGT (Computer Science), Madurai.

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 3-D password. 3-D password is a multifactor authentication scheme. To be authenticated, we present a 3-D virtual environment where the user navigates and interacts with various objects. The sequence of actions and interactions toward the objects inside the 3-D environment constructs the user’s 3-D password. The 3-D password can combine most existing authentication schemes such as textual passwords, graphical passwords, and various types of biometrics into a 3-D virtual environment. The design of the 3-D virtual environment and the type of objects selected determine the 3-D password key space.

1.1 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 conlicting requirements: The selection of passwords that are easy to remember and, at the same time, are hard to guess.
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 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, palmprints, hand geometry, face recognition, voice recognition, iris recognition, and retina recognition are all different biometric schemes. 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.

1.2 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.
1.3 3D PASSWORD OVERVIEW

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 (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 3-D password.

Virtual objects can be any object that we encounter in real life. 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 (x1,y1,z1) is different from the actions toward a similar object (another fingerprint recognition device) that exists in location (x2,y2,z2) where x1 ≠ x2 , y1 ≠ y2 , z1 ≠ z2. 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.

3-D PASSWORD SELECTION AND INPUTS

Let us consider a 3-D virtual environment space of size G x G x G. The 3-D environment space is represented by the co-ordinates (x,y,z) [1,........G] x [1,........G] x [1,........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 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.

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. Fig. 2 shows the 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.

3-D VIRTUAL ENVIRONMENT DESIGN GUIDELINES

The design of 3-D virtual environments should follow these guidelines:

1) REAL-LIFE SIMILARITY

The prospective 3-D virtual environment should react what people are used to seeing in real life.

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. A simple real-life example is home numbering. 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 lesstime.

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. Selecting the right object response types and the number of objects affects the probable password space of a 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
FIG. 3. STATE DIAGRAM OF A POSSIBLE 3-D PASSWORD APPLICATION

3-D 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.

1.4 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 [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 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.

1.5 ATTACKS AND COUNTER MEASURES

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

1) 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 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 leaves the attacker with almost no chance of breaking the 3-D password.

1.6 CONCLUSION AND FUTURE WORKS

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 pass words. 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.

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 user’s choice and decision constructs the desired and preferred 3-D password.

The 3-D password is still in its early stages. Designing various kinds of 3-D virtual environments, deciding on pass- word spaces, and interpreting user feedback and experiences from such environments will result in enhancing and improving the user experience of the 3-D password.

REFERENCE


2. D.V.Klein,”Foiling the cracker: survey improvement to pass security in proc.USEM security workshop.

3. T.Kitten, “Keeping an eye on the ATM” available: ATM marketplace.com


6. Adams and M.A. Sasse, “Users are not the enemy: Why users compromise computer security mechanisms and how to take remedial measures”