ADVANCED AUTHENTICATION SYSTEM

Pushpak Khapke
Pushpak.khapke@gmail.com

Amol Wale
waleamol@gmail.com

Sandip Kote
sandipvkote@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 3-D password. The 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.

Keyword: Authentication, biometrics, graphical passwords, multifactor, textual passwords, 3-D passwords, 3-D virtual environment.

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), 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. Recognitionbased 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 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 3×10^6 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.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 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.

2. 3-D 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.

2)The new scheme should provide secrets that are easy to remember and very difficult for intruders to guess.

3) 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.
4) 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. 3-D 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. 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 ,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)any graphical password scheme;
3) any real-life object;
4) any upcoming authentication scheme.

B. 3-D 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 withunique (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. 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 acomputer 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.

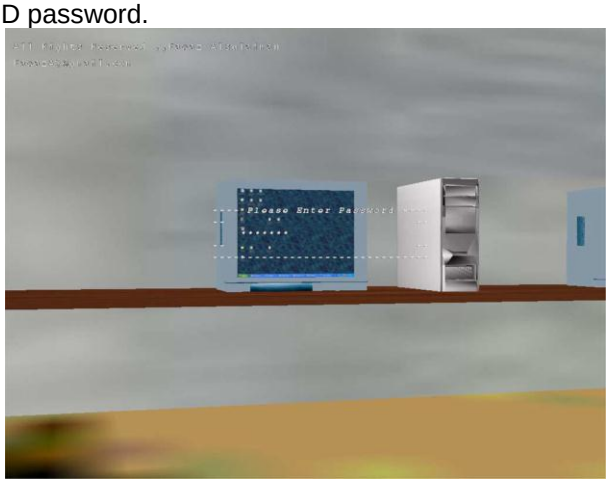

Fig. 1. Snapshot of a proof-of-concept 3-D virtual environment, where the user is typing a textual password on a virtual computer as a part of the user's 3-D password.

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

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. 3-D Virtual Environment Design 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.

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. 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

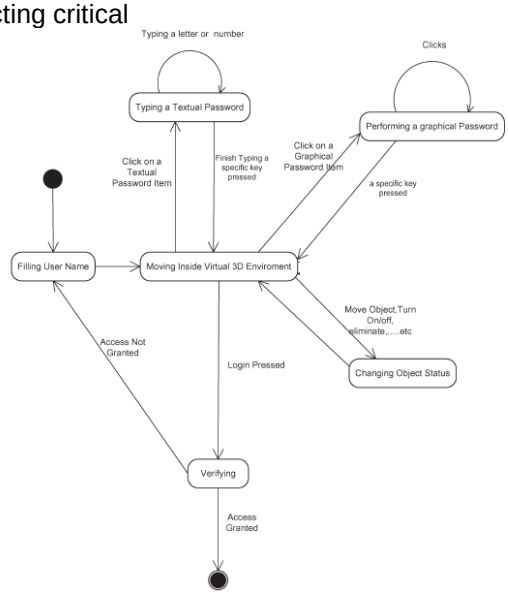

Fig. 3. State diagram of a possible 3-D password application.

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 highlevel 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.

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

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

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

[7] 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.

[8] Real User Corporation, *The Science Behind Passfaces*. (2005, Oct.). [Online]. Available: http://www.realusers.com

[9] 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.
[10] 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.
[11] 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.
[12] 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.
[13] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The design
and analysis of