ISSN 2229-5518

4-D Password: Strengthening the Authentication Scene.

Grover Aman, Narang Winnie

Abstract—We have had many authentication schemes presently, but they all have some drawbacks. So lately, the 3D password paradigm was introduced. The 3-D password is a multifactor authentication scheme. It can combine all existing authentication schemes into a single 3-D virtual environment. However 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. This paper presents a study of the 3D password and an approach to strengthen it by way of adding a Fourth dimension, that deals with gesture recognition and time recording, and that would help strenghthen the authentication paradigm altogether. Hence we attempt to propose a 4-D password as a one-up method to the 3-D password.

Index Terms— Authentication, Privacy,Virtual, 3-D Environment, Biometrics.

1 Introduction

AUTHENTICATION is a process of validating who you are to whom you claimed to be, or in other words a process of identifying an individual, usually based on a username and password. Currently what we have in the field, are the following set of techniques:

Human Authentication Techniques are as follows:

1. Knowledge Base (What you know)
2. Token Based(What you have)
3. Biometrics(What you are)
4. Recognition Based(What you recognise)

Computer Authentication Techniques are as follows:

1. Textual Passwords
2. Graphical Passwords
3. Biometric schemes (fingerprints, voice recognition etc.)

Since many years it has become an interesting field of study. Also, with the development in means of technology, improvement in the methods for authentication has also given way to more sophisticated means of attacking an individual's privacy, or what we know as 'hacking'.

We are provided with many password types such as textual passwords, biometric scanning, tokens or cards (such as an ATM card) etc. But there are many weaknesses in current authentication systems. The most common computer authentication method is to use alphanumerical usernames and passwords. One of the main problems is the difficulty of remembering passwords. Studies have shown that users tend to pick short passwords or passwords that are easy to remember [1]. Unfortunately, these passwords can also be easily guessed or broken.

According to a recent Computerworld news article, the security team at a large company ran a network password cracker and within 30 seconds, they identified about 80% of the passwords [2]. On the other hand, passwords that are hard to guess or break are often hard to remember. Studies showed that since user can only remember a limited number of passwords, they tend to write them down or will use the same passwords for different accounts [3, 4].

To address the problems with traditional usernamepassword authentication, alternative authentication methods, such as biometrics [2, 6] have been used. Biometric scanning is your "natural" signature and Cards or Tokens prove your validity. To test this, many years back Klein performed tests. And he could crack almost 15 passwords per day.

Graphical passwords can also be used. One of the main arguments for graphical passwords is that pictures are easier to remember than text strings. Preliminary user studies presented in some research papers seem to support this. However, current user studies are still very limited, involving only a small number of users. We still do not have convincing evidence demonstrating that graphical passwords are easier to remember than text based passwords.

Token based techniques, such as key cards, bank cards and smart cards are widely used. Many token-based authentication systems also use knowledge based techniques to enhance security. For example, ATM cards are generally used together with a PIN number. Biometric based authentication techniques, such as fingerprints, iris scan, or facial recognition, are not yet widely adopted. The major drawback of this approach is that such systems can be expensive, and the identification process can be slow and often unreliable. However, this type

- *Winnie Narang is currently working with Servigistics Inc. She pursued her bachelors degree in I.T. engineering in Bharati Vidyapeeth's College of Engineering, India. E-mail: Narang.winnie@yahoo.com*
- *Co-Author Aman Grover also pursued his bachelors degree in I.T. engineering in Bharati Vidyapeeth's College of Engineering, India. E-mail: aman.grover@ieee.org*

of technique provides the highest level of security.

Knowledge based techniques are the most widely used authentication techniques and include both text-based and picture-based passwords. The picture-based techniques can be further divided into two categories: recognition-based and recall-based graphical techniques. Using recognition-based techniques, a user is presented with a set of images and the user passes the authentication by recognizing and identifying the images he or she selected during the registration stage. Using recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage.

As the technology has changed many fast processors and tools are available on internet it has become very easy. The 3D passwords scheme has been introduced as a one up solution to these issues.

2 THE 3D PASSWORD SCHEME

The 3D Password scheme is a relatively new authentication scheme that combines RECOGNITION +RECALL + TOKENS+ BIOMETRIC in one authentication system. 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 [7] 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 3D passwords will increase. Thus, it becomes much more difficult for the attacker to guess the user's 3-D password.

2.1 System Implementation

Since the 3D password is a multifactor authentication scheme [8], it 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 ombination and the sequence of the 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 biometric 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 towards 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 virtual objects, for instance:

1. A keyboard wherein the user can type.
2. A fingerprint reader that requires the user's fingerprint.
3. A biometric recognition device.
4. A paper or a white board that a user can write, sign or draw on.
5. An ATM machine that requires a smart card and PIN.
6. An appliance 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 chair that can be moved from one place to another.
11. Any graphical password scheme.

2.2 Working

Consider a three dimensional virtual environment space that is of the size S×S×S. Each point in the three dimensional environment space represented by the coordinates (x, y, z) € [1..S] × [1..S]×[1..S]. The objects are distributed in the three-dimensional virtual environment. Every object has its own (x,y,z) coordinates. Assume the user can navigate and walk through the three-dimensional virtual environment and can see the objects and interact with the objects. The input device for interactions with objects can be a mouse, a keyboard, stylus, a card reader, a microphone etc. For example, consider a user who navigates through the 3D virtual environment that consists of a ground and a classroom. Let us assume that the user is in the virtual ground and the user turns around to the door located in (10,16,80) and opens it. Then, the user closes

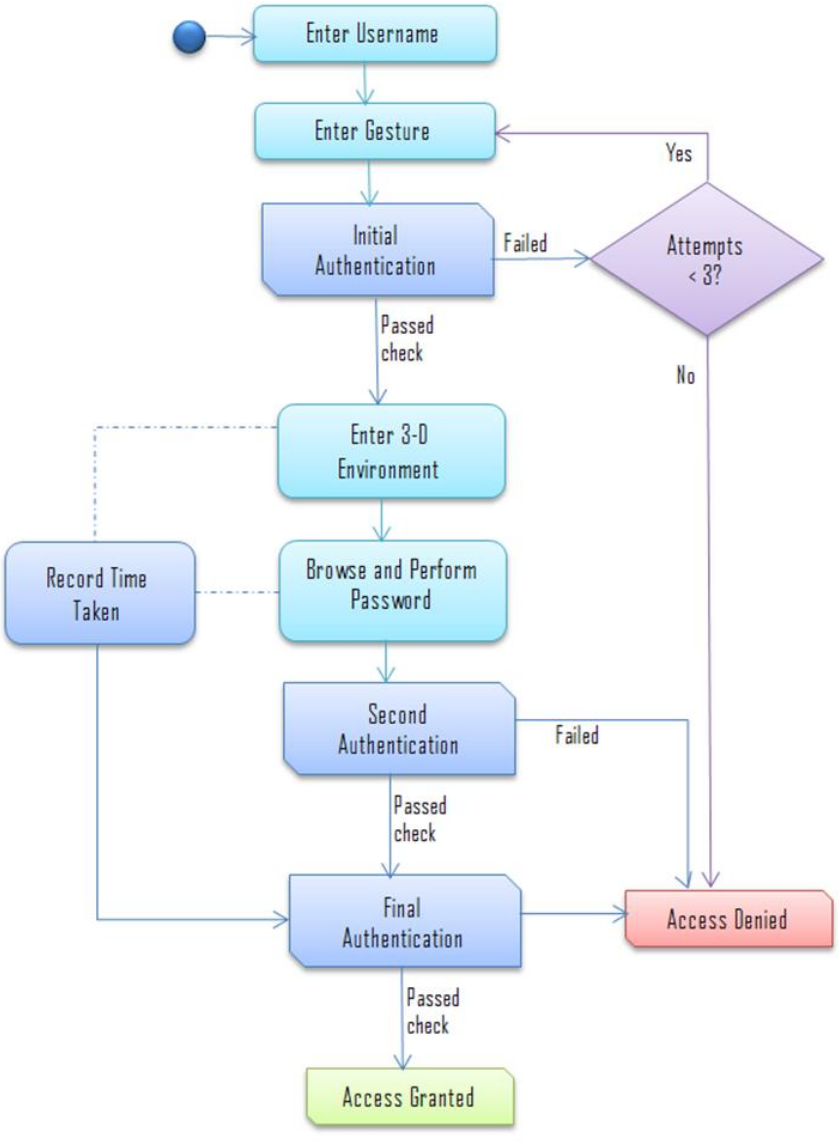
the door. The user types "WAFFLE" into a computer that exists in the position of (18, 5, 20). The user then walks over and turns off the light located in (15, 6, 20), and then goes to a white board located in (55, 3, 30) and draws just one dot in the (x,y) coordinate of the white board at the specific point of (420,170). The user then presses the login button. The initial representation of user actions in the 3D virtual environment can be recorded as follows:

(10, 16, 80) Action = Open the office door;
(10, 16, 80) Action = Close the office door;
(18, 5, 20) Action = Typing, "W";
(18, 5, 20) Action = Typing, "A";
(18, 5, 20) Action = Typing, "F";
(18, 5, 20) Action = Typing, "F";
(18, 5, 20) Action = Typing, "L";
(18, 5, 20) Action = Typing, "E";
(15, 6, 20) Action = Turning the Light Off;
(55, 3, 30) Action = drawing , point = (420,170);

After the user has performed these actions, he will exit out of the 3-D environment. After backend verification, access will be granted.

3 INTRODUCING THE FOURTH DIMENSION

The 4-D Password scheme is an attempt to make the existing scheme even more robust and powerful. We propose to add another key to the current scheme, and this will lend more stability and make the attacks on user privacy even more difficult to succeed in.



This key, what we propose to refer to as the 'FOURTH DIMENSION' would be an encrypted string that encapsulates a gesture that the user is supposed to make with his hands, in front of a webcam, apart from his password. This will help ensure that the user is physically present for login.Hence, the final password of the user would be:

Hand Gesture + 3-D Password .

Now let's have a closer look as to how this gesture would be generated and saved. We have a mapping function F(x), such that if we put V as the input string, then it creates F(V), which is our final encrypted key.

The user does not need to bother with any of these.All he needs to do is remember the gesture, which would be captured as a binary string S. This would be saved as a precursor to his 3-D password. The String V would then be encrypted and appended to the already existing password.

Hence, the end result would be a password that looks like this:

P = 3-D password + F(V).

The addition of F(V) at the end would actually increase the complexity of the password. The attacker will now have to guess the string V as well as try to decipher function F(x), in addition to the complex techniques required to decipher a user's 3-D password itself.

3.1 Signup Process

Consider a web-based repository of research work for scientists, wherein each scientist has his own account which stores his files and folders. This repository employs the 4-D password scheme.

As a new user, I will sign up as follows:

1. Choose a username.
2. I will be redirected to the password generation page.
3. I will enter the 3-D environment.
4. Inside the environment, I will perform certain actions, as have been discussed before.
5. I will exit out of the environment and submit my actions.
6. I will then be asked to perform a gesture in front of the webcam. This gesture, once successfully captured, will be saved. I will be notified of the time that I had taken to perform this gesture this time.
7. I will need to remember it for subsequent attempts at login Sign up process is complete.

3.2 Logging In

Now when I log in, I will have to enter my username, and then perform my gesture. Once this is submitted and verified, I will enter the 3-D environment and perform my password. I will exit and submit it.

Once that is verified, will be granted access to my account.

3.3 Significance

The addition of an extra gesture will create an unlimited host of password combinations. Also it will ensure that there is a person attempting to login, and not some automated program, or bot.

Another check that can be applied here, is the measure of the total time taken for the 3-D Authentication by the user. This time can be considered a part of the user's authentication, and the user must perform subsequent attempts within the same time limit, give or take a few more seconds. So each password can then have a time window associated with it.

On later attempts, a timer can be made to run in parallel to the 3-D browsing session. Based on the total time taken, certain conclusions can be drawn out:

1. If time taken tends to zero, it might be an attempt made by an automated hacking process.
2. If time taken is very large, it may well be possible that another user is attempting to replicate the user's actions, step by step.

This additional check will provide more soundness to the 4-D password scheme.

4 SECURITY ANALYSIS

4.1 Keylogger

In many cases, the attacker installs an invisible software called a keylogger, which is designed to capture all keys typed through the user's keyboard and output them as a stream in a text file.This way the attacker finds out the user's password by browsing through the file. But here, since the nature of password is not textual, this attempt will be a total failure.

4.2 Well-Studied Attack

The attacker tries to find the highest probable distribution of 3D passwords. In order to launch such an attack, the attacker has to acquire knowledge of the most probable 3D passworddistributions. This is very difficult because the attacker has to study all the existing authentication schemes that are

used in the 3D environment. It requires a study of the user's selection of objects for the 3D password. Moreover, a well studied attack is very hard to accomplish since the attacker has to perform a customized attack for every different virtual environment design. This environment has a number of objects and types of object responses that differ from any other 3D virtual environment. Therefore, a carefully customized study is required to initialize an effective attack. Even then, the probability of a successful attack is extremely scarce.

With a 4-D password, there is the extra process of determining the gesture as well. The chances that an attacker can guess the gesture, out of thousands of possible human movements, is going to be as hard as it sounds. Plus,both the gesture and the 3-D password need to guessed correctly. So chances of a successful attack in this case are bleak, to mention the least.

4.3 Shoulder Surfing Attack

An attacker uses a camera to record the user's 3D password or tries to watch the legitimate user while the 3D password is being performed. This attack is the most successful type of attack against 3D passwords and some other graphical passwords.

However, the user's 3D password may contain biometric data or textual passwords that cannot be seen from behind.

Therefore, we assume that the 3D password should be performed in a secure place where a shoulder surfing attack cannot be performed. Also, with the 4-D password, the nuances of the gesture, even if visible to the attacker, may not be emulated successfully, and also the physique will have to match with the user, since the system would compare it with the earlier recording.

4.4 Timing Attack

The Attacker observes how long it takes the legitimate user to perform correct log in using 3D Password which gives an indication of 3-D Passwords length. This attack cannot be successful since it gives the attacker mere hints. Also this would lend the attacker no help in finding out the extra gesture; which is exclusive of the 4D password only.

4.5 Brute Force Attack

The attack is very difficult because

1. Time required to login may vary form 20s to 2 min there fore it is very time consuming.

2. Cost of Attack: A 3D Virtual environment may contain a biometric object, and the attacker has to forge all biometric information.

5 WHAT MAKES IT CLICK

5.1 4D Password Differentiators

1. Flexibility: 4D Passwords allows Multifactor Authentication. Biometric, graphical and textual passwords can be embedded in 4D password technology.

2. Strength: This scenario provides almost unlimited passwords possibility. Hence, the strength.

3. Easy to Remember: Can be remembered in the form of short story.

4. Privacy: Organizers can select authentication schemes that respect the user's privacy.

5.1 Application Areas

1. Critical Servers: Many organizations are using critical servers which are protected by a textual password. 4D password authentication scheme proposes sound replacement for these textual passwords.

2. Banking: Almost all the Indian banks started 3D Password service for security of buyer who wants to buy online or pay online. "How to Create 3D password for my master card? Our online payment will fail, if will create 3D password, so for generating 3D password, we have to go to our bank's website and then, click 3D secure service and then write our card number, CVV, pin no., and write our password and rewrite it and then click ok or submit." After this we get a 'thank you' message. Like PNB, SBI also started 3D secure services for verified by Visa. Verified by Visa is a new service that will let you use a personal password with your State Bank of India Visa card, giving you added assurance that only you can use your State Bank of India Visa card to make purchases over the Internet.

3. Nuclear and military Facilities: 4D password has a very large password space and since it combinesRECOGNITION+ RECALL+ TOKENS+ BIOMETRIC in one authentication system, it can be used for providing security to nuclear and military facilities.

4. Airplanes and Jet Fighters: Since airplanes and jetplanes can be misused for religion and political agendas, they should be protected by a powerful authentication scheme.

5. ATMs, Desktop and Laptop Logins, Web Authentication.

6. The Cloud: Cloud computing [9] is an internet-based model for enabling convenient, on-demand network access to a shared pool of configurable computing resources. It provides various services over internet such as software, hardware, data storage and infrastructure. Cloudcomputing providers deliver the applications via internet, which are accessed from web browsers, desktop and mobile apps. The 4D password scheme, if successfully implemented here can make the cloud much more safer and reliable.

6 FUTURE WORK AND ANALYSIS.

Cloud computing provides various internet-based, on demand services like software, hardware, server, infrastructure and data storage. To provide privacy services to the intended customer, it is a better option to use sophisticated and robust password generation and authentication technique. A state of the art technique would ensure that the strict authentication and authorization is possible. The security levels of cloud environment can be further improved by multi-level of authentication. This is the future work of our research. Our future work will be carried out in adding multidimensional password generation method to multi-level authentication tecnique.

This amalgamation of techniques can lead to another revolutionary concept of authentication,[10] that even surpasses the utility and robustness of the current authentication schemes, the best of which is the 3D password at present. Of course, the fourth dimension makes it totally unsurpassable.

REFERENCES

[1] A. Adams and M. A. Sasse, "Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures," *Communications of the ACM*, vol. 42, pp. 41-46, 1999.

[2] K. Gilhooly, "Biometrics: Getting Back to Business," in *Computerworld*, May 09, 2005.

[3] R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in *Proceedings of 9th USENIX Security Symposium*, 2000.

[4] M. Kotadia, "Microsoft: Write down your passwords," in *ZDNet Australia*, May 23, 2005.

[5] A. Gilbert, "Phishing attacks take a new twist," in *CNET News.com*, May 04, 2005.

[6] A. Jain, L. Hong, and S. Pankanti, "Biometric identification," *Communications of the ACM*, vol. 33, pp. 168-176, 2000.

[7] 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.

[8] Fawaz A. Alsulaiman and Abdulmotaleb El Saddik,"Three-Dimensional Password for More Secure Authentication," IEEE, *http://ieeexplore.ieee.org*., Last Updated – 6 Feb 2008J.

[9] Thorpe, P.C. van Oorschot. Graphical Dictionaries and the Memorable Space of Graphical Passwords. USENIX Security 2004, San Diego, August 9-13, 2004. J. Williams, "Narrow-Band Analyzer," *PhD dissertation, Dept. of Electrical Eng., Harvard Univ.*, Cambridge, Mass., 1993. (Thesis or dissertation)

[10] D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes," in *Proc. 13th USENIX* .