
International Journal of Computational and Electronics Aspects in Engineering
Vol. 1, Issue. 2, March 2015, Revised in June 2020, pp 70-74
https://doi.org/10.26706/ijceae.1.2.20150105

# 3D Password for More Secure Authentication for Smart Phone

**Snehal S. Pohane**
snehalspohane@gmail.com

**Sudhir W. Mohod**
sudhir_mohod@rediffmail.com

Department of Computer Science & Engineering
Bapurao Deshmukh College of Engineering Sewagram, Wardha, India.

***Abstract* - Authentication on mobile devices is not (and should not be) the same as on desktop and laptop computers. Since past few years there has been a remarkable rise in the popularity of touch screen mobile phone devices. With respect to the data and information that can be stored on the mobiles as well as mobiles are nowadays are also used for accessing mail and connecting to social media so it is necessary to ensure the security of the data and information that is stored on the mobiles. User authentication is an important security measure for protecting the information stored on the mobile phone devices. When user enters their password in public place then it can be capture by attacker by direct observation or by recording the user's authentication session. This attack is known as Shoulder surfing attack. In this paper, we present a 3-D password for more secure authentication for smart phone. The 3D Password is multi-factor and multi password authentication techniques that consist of 3D virtual environment containing real time object scenarios.**

***Index Terms***—Authentication, Graphical password, Multi-factor, Textual password, 3D Password, 3D Virtual environment.

## I. INTRODUCTION

The authentication system which we are using is mainly very light or very strict. Since many years it has become an interesting approach. With the development in means of technology, it has become very easy for 'others' to hack someone's password. We are provided with many password types such as textual passwords, biometric scanning, tokens or cards (such as an ATM) etc. But there are many weaknesses in current authentication systems. When a person uses textual passwords, he likely chooses meaningful words from dictionary or their nick names, etc which can be cracked easily. And if a password is hard to guess then it is hard to remember also. Users face difficulty in remembering a long and random appearing password and because of that they create small, simple, and insecure passwords that are easy to attack. Graphical passwords can also be used. Their strength comes from the fact that users can recall and recognize pictures more than words. Token based systems can also be used as way of authentication in banking systems and for entrance in laboratories. Smart cards or tokens prove your validity but are susceptible to loss or theft. Biometric scanning is your "natural" signature and 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. Many years back Klein performed tests and he could crack almost 15 passwords per day. As the technology has changed many fast processors and tools are available on internet it has become very easy. So, in this, we have introduced 3-d password scheme.

Technical Article
First Online on – 30 March 2015, Revised on – 30 June 2020



Cite this article – Snehal S. Pohane and Sudhir W. Mohod, "3D Password for More Secure Authentication for Smart Phone", *International Journal of Computational and Electronics Aspects in Engineering*, RAME Publishers, vol. 1, issue 2, pp. 70-74, 2015, Revised in 2020.
https://doi.org/10.26706/ijceae.1.2.20150105

*A. 3D password system*

3D password is combination of both recall-based (i.e. textual password, etc) & recognition based (i.e. graphical password, biometrics, etc). So that 3D password is multifactor & multi password authentication scheme.

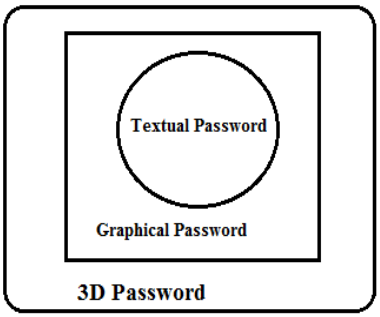


Fig. 1 Multifactor authentication scheme

The idea is simply outlined as follows. The user navigates through a three-dimensional virtual environment. The combination and the sequence of the user's actions and interactions towards the objects in the three-dimensional virtual environment constructs the user's 3D password. Therefore, the user can walk in the virtual environment and type something on a computer that exist in (x1, y1, z1) position, then walk into a room that has a white board that exist in a position (x2, y2, z2) and draw something on the white board. The combination and the sequence of the previous two actions towards the specific objects construct the user's 3D password. Users can navigate through a three-dimensional virtual environment that can contain any virtual object. Virtual objects can be of any type. We will list some possible objects to clarify the idea. An object can be:

1. A computer that the user can type in
2. A white board that a user can draw on
3. An ATM machine that requires a smart card and PIN
4. A light that can be switched on/off
5. Any biometric device
6. Any Graphical password scheme
7. Any real life object
8. Any upcoming authentication scheme

Moreover, in the virtual three-dimensional environment we can have two different computers in two different locations. Actions and interactions with the first computer is totally different than actions towards the second computer since each computer has a (x,y,z) position in the three-dimensional virtual environment. Each object in the virtual three-dimensional environment has its own (x,y,z) coordinates, speed, weight and responses toward actions[1].

## II. RELATED WORKS

Shubham Bhardwaj, Varun Gandhi, Varsha Yadav, Lalit Poddar have worked on the 3-D passwords and it is the combination of physical and biometric authentication. The sequence of actions and interfaces 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 conclude the 3-D password key space. In this paper authentication process is lengthy & that's why large memory space required [8]. K.Nivetha, M. Muthumeena, R. Srinivasan has proposed two authentication techniques based on text and colors are proposed for PDAs. These techniques generate session passwords and are resistant to dictionary attack, brute force attack. Both the techniques use grid for session passwords generation. Pair based technique requires no special type of registration; during login time based on the grid displayed a session password is generated. For hybrid textual scheme, ratings should be given to colors, based on these ratings and the grid displayed during login, session passwords are generated. However these schemes are completely new to the users and it is different to the existing authentication system but it is time consuming [9].

Vishal Kolhe, Vipul Gunjal, Sayali Kalasakar, Pranjal Rathod have worked on Secure Authentication with 3D

Password .In this paper they have introduced their contribution towards 3D Password to become more secure & more users friendly to users of all categories. This paper also explaining about what is 3D password. Working of 3D password scheme, some mathematical concept related to 3D password, applications of scheme etc. This paper combines all existing authentication techniques & use 3d Quick hull algorithm but drawback is Shoulder surfing attacks is possible [10].

Priti Jadhao, Lalit Dole has worked on a Survey on Authentication Password Techniques. They explained authentication is process of determining whether someone or something is, in fact who or what to be declared. For authentication mostly textual passwords are used. Passwords are the most commonly used method for identifying users in computer and communication systems. Typically, passwords are strings of letters and digits, i.e., they are alpha-numeric. Such passwords have the disadvantage of being hard to remember. Graphical passwords, which consist of some actions that the user performs on an image. Such passwords are easier to remember, but are vulnerable to shoulder surfing (which consists of simply watching a user login).This paper explains about textual, Graphical passwords but it is vulnerable to dictionary & Shoulder surfing attacks [11]. Banita Chadha, Dr. Puneet Goswami has worked on to calculate the probability of finding the password .Using 3D password make the hacker difficult to hack computer system. It includes various strategies in various fields.3D includes the values along x axis, y axis, and z axis. This paper presents the strategy based on 3D virtual environment.3d includes various services like biometrics, ATM, Smart cards etc [12].

## III. Implemented Work

### A. *3D virtual environment*

The 3-D password is a multifactor authentication scheme. In this multi-factor authentication scheme, the basic building block used is 3D virtual environment. 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. 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.

In 3D password user have to First Authenticate with simple textual password (I.e. user need to provide user name & password) Once authentication successful then user moves in 3D virtual environment where he/she has to select multiple point in that room or he can do some action in that environment like switching on/off of computer or AC. In this way the password is set for that particular user. The 3-D password is constructed by observing the actions and interactions of the user and by observing the sequences of such actions.

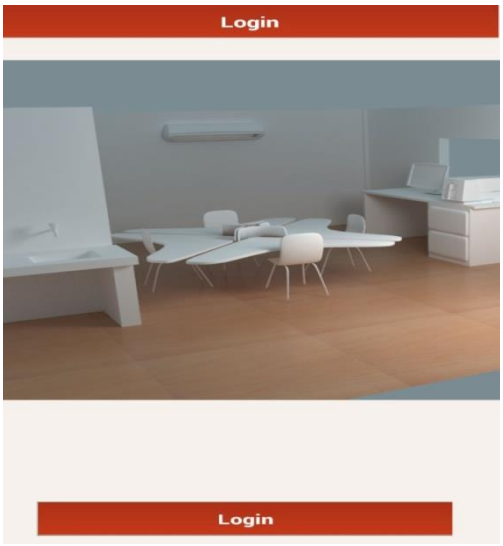


Figure 2. Shows a snapshot of a 3-D virtual environment on smart phone.

Following are the steps for authentication:

1. User will connect to the server for system login.
2. After successful client-server connection registration form will be filled up.
3. User will now enter into virtual 3-D environment.
4. Now the user will perform its authentication steps according to set design.


Figure 3. Shows a snapshot of an experimental 3-D virtual environment on smart phone.

*B. 3D Virtual Environment Design Guidelines*

Design of 3D virtual environment imitating the need and security requirements of the user is the first step in creating 3D Password that affects usability, acceptability and effectiveness of the3D Password system.

Following are the guidelines that need to be considered while designing 3D virtual environment.

*1) Real-life similarity*

The prospective 3D virtual environment should reflect what people are used to seeing in real life [1]. Virtual objects should be relatively similar in size to real objects and their responses should be realistic. Possible actions and interactions toward virtual objects should reflect real-life situations.

*2) Object uniqueness and distinction*

Every virtual object/item present inside the 3D virtual environment should be different from each other and their uniqueness must come from the fact that every virtual object has its own attribute for instance position. Thus, the prospective interaction with object 1 is not equal to the interaction with object 2. Therefore, 3D virtual environment design should consider the distinguishing factors of virtual objects that increase the user's recognition of objects thereby, improving system usability.

*3) Three-dimensional virtual environment size*

Size of 3D virtual environment do matters and should be studied carefully. 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 [1]. A large 3D virtual environment contains large number of virtual objects and hence, requires more time to create 3D password compared to small 3D virtual environment that contains few virtual objects.

*4) Number of objects (items) and their types*

Most important part to be consider while designing 3D virtual environment is to determine the type of object that reflect what kind of responses the object will have and number of objects to be placed in the virtual environment. Selection of the right type of object and number of object affects the probable 3D Password space.

*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.

## IV. Conclusion And Future Work

Currently available schemes include textual password and graphical password .But both 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 &

multi password authentication scheme. Moreover, these work shows that it requires less space as compare to the existing works because it uses xml animation technique for to design the 3D virtual environment. This virtual environment can contain any existing authentication scheme or even any upcoming authentication schemes.

The 3-D password is still in its early stages. Shoulder surfing attacks are still possible and effective against 3-D passwords. The future work is needed to be done on a simple and efficient scheme based on texts and colors, without using any physical keyboard or on-screen keyboard for to implement it in 3d password on Textual Password authentication to prevent the Shoulder Surfing attack.

## REFERENCES

[1] Sobrado, L and Birget, J. "Graphical Passwords", The Rutgers Scholar, An Electronic Bulletin of Undergraduate Research, Ruthgers University, New Jersey, Vol.4, 2004.

[2] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "Authentication Using Grap hical Passwords: Basic Results", In Human-Computer Interaction International (HCII 2005), Las Vegas, NV, 2005.

[3] H. Zhao and X. Li, "S3PAS: A Scalable Shoulder- Surfing Resistant Textual-Graphical Password Authentication Scheme," in 21stInternational Conference on Advanced Information Networking and Application Workshops (AINAW 07), Vol.2.Canada, 2007, pp.467-472.

[4] Fawaz A. Alsulaiman and Abdulmotaleb El Saddik "Three-Dimensional Password for More Secure Authentication", IEEE Transactions On Instrumentation And Measurement, Vol. 57, No. 9, September 2008.

[5] Ms. Vidya Mhaske-Dhamdhere, Prof. G. A. Patil "Three Dimensional Object Used for Data Security" International Conference on Computational Intelligence and Communication Networks 2010.

[6] M.ArunPrakash, T.R.Gokul "Network Security-Overcome Password Hacking Through Graphical Password Authentication", Proceedings of the National Conference on Innovations in Emerging Technology 17 & 18 February, 2011.pp.43-48.

[7] Tao Feng, Ziyi Liu, Kyeong-An Kwon, Weidong Shi, Bogdan Carbunar, Yifei Jiangz and Nhung Nguyen, "Continuous Mobile Authentication using Touchscreen Gestures" School of Computing and Information Sciences, Florida International University, 2011.

[8] Shubham Bhardwaj, Varun Gandhi, Varsha Yadav, Lalit Poddar "New Era of authentication: 3-D Password" International Journal of Science, Engineering and Technology Research (IJSETR) Volume 1, Issue 5, November 2012.

[9] K.Nivetha, M. Muthumeena, R. Srinivasan,"Authentication Mechanisim For Session Passwords By Imposing Color With Text", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com ,Vol. 2, Issue 5, September- October 2012, pp.1611-1615.

[10] Vishal Kolhe, Vipul Gunjal, Sayali Kalasakar, Pranjal Rathod "Secure Authentication with 3D Password" International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 2, March 2013

[11] Priti Jadhao, Lalit Dole," Survey on Authentication Password Techniques", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-2, May 2013.

[12] Banita Chadha , Dr. Puneet Goswami " 3d Password – A Secure Tool ", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 1, January 2014.