

Short communication

AN INTERACTIVE MAP FOR 3D-PASSWORD SECURITY AUTHENTICATION

Abstract

The drawbacks of all the existing security techniques have led to a newer technique called 3D Password. The 3D Password authentication technique can accommodate those previous authentication techniques (Textual password, graphical password, biometric password and so on) which make it difficult for hackers to crack because of the inclusion of a 3D virtual environment and its virtual objects. Mapping techniques have evolved over the years with the aid of the computer system, satellite and Global Positioning System (GPS) each location on a map is geo-referenced. This paper proposed a combination of 3D Password security authentication with 3D Interactive Maps for better and more enhanced security, hence allowing the user to select the area he is much familiar with and making it more difficult for hackers to break. Also, a 3D interactive map is an existing technology and a virtual environment, service, commonly used by end-users all around the world. With this, it will make 3D password security authentication more secured and better user-friendly as against developing a specific virtual environment for a user to select a virtual object which he might be seeing for the very first time. This can lead to a user forgetting an object that was chosen in the first place when he is to login at another time interval which could be days, weeks, months or years.

Keywords: 3D Password, 3D interactive map, security, virtual environment, user-friendly

1. INTRODUCTION

The issue of security has remained one of the major concerns (Kolhe et al., 2013) that have stayed very close with a man ever before the first computer was manufactured. Man has ever looked for ways of protecting himself from numerous attacks to be able to survive. And now that computer system has also come to stay with a man in almost every facet of life (for example medicine, engineering, education, military, communication, transportation and so on) the issue of security has also found a niche for itself. To be able to protect invaluable data and information stored in computer system or database, various authentication techniques such as textual password (Gokhale & Waghmare, 2016), graphical password, biometric password and so on were employed for genuine user-access control to the computer. These types of authentication techniques have been found to have a lot of loopholes for hackers to penetrate. For example, the textual password requires that the user select particular words from dictionaries which make this authentication technique prone to the same dictionary attack or brute force attack. The graphical password was assumed to be easier for the user to remember by identifying the pre-selected picture(s) among many others. Yet this faces a lot of challenges as it requires a longer time for the pictures to load, especially in a slow network, hence making it susceptible to shoulder surfing attacks. Biometric authentication has also been found with its drawback which is the none willingness of the users to subject themselves under such technology

3D authentication technique is a multifactor authentication scheme that combines the benefits of various authentication schemes. Users have the freedom to select whether the 3D authentication will be solely recalled, biometrics or token-based or a combination of two or more schemes. This freedom of selection is necessary because users are different and they have different requirements. Therefore, to ensure high user acceptability, the user's freedom of selection is important (Tejal et al, 2012). The principle behind 3D authentication is the combination of the sequence of action and interaction of the user with the objects in the virtual environment. Hence, to make a 3D password highly acceptable to the end-users it is better to combine this new authentication technique with the existing platform (3D map) that the user is already familiar with. It will be of great interest to the user when he is asked to select his favourite location and navigate to a particular spot of interest on a 3D interactive map. And because it is his own real-life world experience that is being transposed into the virtual environment, he will not only find the platform more user-friendly but will also not forget easily, if he is asked to navigate the same route over and over again.

2. EXISTING PROPOSED SYSTEMS

2.1. Geographic Coordinate System

A geographic coordinate system is a coordinate system that enables every location on the earth to be specified by a set of numbers or letters. The coordinates are often chosen such that one of the numbers represents a vertical position, and two or three of the numbers represent horizontal position. A common choice of coordinates is latitude, longitude and elevation (wikipedia.org), hence 3D mapping. General-purpose maps provide many types of information on one map. Most atlas maps, wall maps, and road maps fall into this category. The following are some features that might be shown on general-purpose maps: bodies of water, roads, railway lines, parks, elevations, towns and cities, political boundaries, latitude and longitude, national and provincial parks. These maps give a broad understanding of the location and features of an area. The user can gain an understanding of the type of landscape, the location of urban places, and the location of major transportation routes all at once (wikipedia.org).

2.2. Virtual Environment

Ramloll et al (2001) divided 3D virtual environment into small regions he collected noticeable images and assigned roles to each image, like the entrance to the area, exit from the area, and feature point of the area. With this, the user will be able to remember the environment structure in an organized way, and reuse was also proven to be easy. The research by Kim et al (2005) showed that the topic map can not only be utilized in the Web environment, but can also be applied as a navigation

aid in a 3D virtual environment and that semantic linkage of the topic map expresses the hierarchical structure in the spatial structure, and semantically links the subjects related to the environment. The paper further stated that spatial knowledge refers to the knowledge that organizes the virtual environment into a hierarchical structure so that the world could be well understood. The world is divided into several zones in the virtual environment, based on their regional features and classifications, and each zone is divided into sub-zones. Also, the navigation aid suggested in their paper will integrate subject knowledge, which can be handled in the world, and spatial knowledge, which can grasp the structure of the world. Using the topic map technology, the said navigation aid can help users navigate to their target/destination in the virtual environment as they follow the semantic linkage.

Vishal *et al* (2013) proposed in their paper that the 3D password authentication scheme is a combination of many other authentication schemes together. 3D password is a 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. And that for authentication with 3D password a new virtual environment is introduced called 3D virtual environment where the user navigates, moving in a 3D virtual environment to create a password which is based on the schemes. The paper cited an example that a user has to first authenticate with a simple textual password (i.e. user needs to provide user name & password) once authentication is successful then the user moves in a 3D virtual environment, thereafter a computer with keyboard will be seen on screen. On that screen, the user has to enter a password (textual) which is stored in a simple text file in the form of encrypted coordinates (x1, y1, z1). After successful completion of this authentication, then the user automatically enters into an art gallery, where he/she has to select multiple points in that gallery or he can do some action in that environment like switching button on/off or perform an action associated with any object like an opening door, etc. The sequence in which the user has clicked (i.e. selecting objects) that sequence of points is stored in a text file in the encrypted form. In this way, the password is set for that particular user.

2.3. Use of Game as Virtual Environment

Nidhi et al (2012) described using a chess game as a virtual environment for a 3D password that when a new user enters the environment, the user must initially enter all his details in the registration form. The user must then click on the environment button to select the chess environment. Figure 1 below shows an environment for a chess game, having a total of 32 objects, out of which 16 are red and 16 are white. It also encloses seven buttons together namely, New button, Record button, Stop button, Play button, Confirm button, Close button and Swap button, and one Checkbox option.



Figure 1: Chess game virtual environment

But it is not everybody that loves to play games especially when on the computer or in a very serious environment while others may not be familiar with certain game or may prefer one game over another (e.g. chess game to football game) and if the 3D password virtual environment has been designed for a particular game the user's interest might be weakened, thereby not making the platform user-friendly. In a 3D interactive map, for the user to select the map of the area of choice, the interest is already won and the process of capturing the 3D authentication begins, almost immediately.

3. DISCUSSION

According to Gadicha *et al* the 3D password, multifactor authentication scheme combines the benefits of various authentication schemes and it should satisfy the following requirements.

1. The new scheme should not be either recalled 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 recalled, 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.

This paper focuses on items 2, 3, 4 and 5 listed above by making the virtual environment more user-friendly based on what the user is already familiar with and also based on proven technology (3D interactive map).

Note: This work quite understands that any other type of technique could be integrated, but to make it more concise the paper focuses on the integration of 3D interactive map into the security authentication techniques.

3.1. 3D Interactive Map

Map websites such as Google Map, MapQuest, NASA World Wind, OpenStreetMap and so on, have developed their platforms from ordinary static maps to interactive maps to make it user-friendly. Some have even embedded real-time traffic scenarios into their interactive map platform coupled with modelling of real-world features into 3D virtual objects, making it more user-friendly and making the user assume the feel of real-environment. Figure 2 is an example of a 2D interactive map of MapQuest showing some parts of Lagos State, Nigeria.

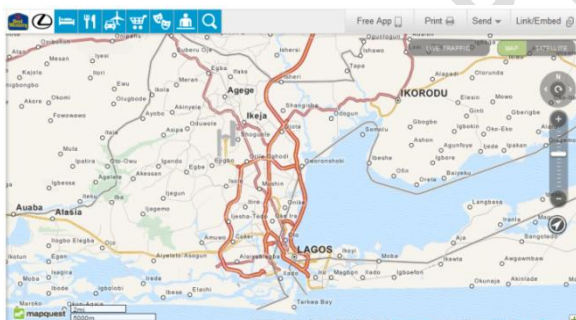


Figure 2: 2D interactive map (<http://www.mapquest.com/>)

To make the user have the feeling of reality and presence, instead of designing a new virtual environment for the user to begin to learn or familiarize himself with, which will take an appreciable amount of time to do and may eventually lead to making the 3D password susceptible to hacking. This also can lead to users not being able to remember actual virtual objects picked in the first place, if he is to login at another time interval which could be a day, a week, a month, a year or several years interval, depending on when the user wants to re-login into the same virtual environment. This paper looks at using (1) 3D interactive map is already known and widely used by many end-users, and (2) that the technology is already available as a virtual environment. These could be combined in accomplishing 3D security authentication technique. According to Tejal *et al* (2012), the prospective 3D virtual environment should reflect what people are used to seeing in real life.

3.2. 2D Geographical Coordinates

Each point on the earth is already geo-referenced by the use of Global Positioning Systems (GPS) and satellites into x and y coordinates and each point is unique. The Cartesian coordinate system uses two axes: one horizontal (x), representing east-west, and one vertical (y), representing north-south. The point at which the axes intersect is called the origin. Locations of geographic objects are defined relative to the origin, using the notation (x,y), where x refers to the distance along the horizontal axis and y refers to the distance along the vertical axis. The origin is defined as (0,0).

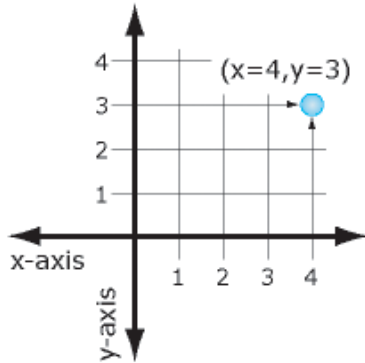


Figure 3: 2D coordinate (www.resources.arcgis.com)

3.3. 3D coordinate systems

Increasingly, projected coordinate systems also use a z-value to measure elevation above or below mean sea level. In the illustration below, the notation (2,3,4) records a point that is two units over in x and three units in y from the origin and whose elevation is four units above the earth's surface, such as 4 meters above mean sea level.

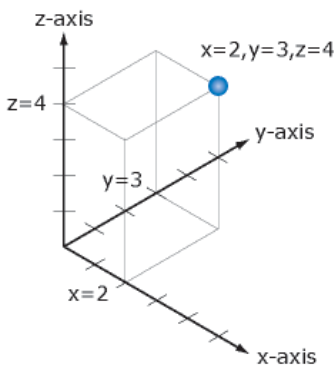


Figure 4: 3D coordinate (www.resources.arcgis.com)

3.4. 2D and 3D Coordinates combined.

As the user navigates through point A with coordinates (x1, y1) is not the same as navigating through point B with coordinates (x2, y2) which are both 2D coordinates.

That is; point A (x1, y1) \neq point B (x2, y2)

Also, for every object, Ni has its coordinate (Xi, Yi, Zi). (Where $i = 1, 2, 3, \dots n$)

Also, $x_i \neq X_i$, and $y_i \neq Y_i$

Therefore, coordinates (xi, yi) and (Xi, Yi) are uniquely distributed on the earth's surface.

3.5. Capturing Security Authentication from 3D Interactive Map

To be able to capture security authentication from a 3D interactive map, the user must first be asked to choose a location he/she is much familiar with. Then as the user passes through the virtual street or route he can interact with as many virtual objects as possible that are known to the user/her. The interaction with the virtual objects and the coordinates of these locations are captured into 3D security authentication. These objects could be a building, stadium, garage, park, shop, traffic light, human, animal, trees etc. that are unique in the real-world environment. The combination of the coordinates of the user's path along (x_i, y_i) and his interaction with the object (X_i, Y_i, Z_i) forms the 3D password. For example, a user's interest is in football and he remembers the day his club or country won a cup, he might choose the route to the stadium, starting from the bus stop and again, he can select objects that he can vividly remember which are uniquely distributed in the virtual environment, such as bus, the bus-stop, shop, buildings, trees, poles etc, which he interacted with when going to the stadium. And finally, he can select other objects within the stadium and the stadium itself.

For example figure 5 has white spots that shows important locations and junctions that the user can combine if he visited some of the white spots (locations) and if he did not, as he moves from point A to point B (the route he can vividly remember) all the coordinates along A and B and interaction with other virtual objects will all be part of the 3D password authentication, irrespective of the direction he chose. With this, the 3D password space is broadened and will make it harder for hackers to break, because each point is uniquely identified as part of the 3D password scheme.

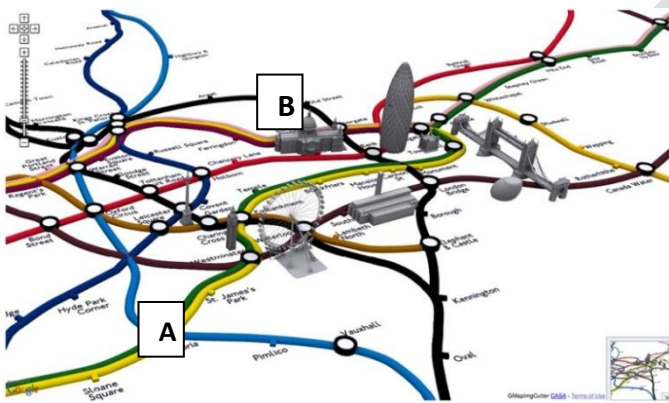


Figure 5: User's route from point A to B (www.designboom.com)

Figure 6 shows a clear picture of a 3D interactive map which allows the user to zoom-in/zoom-out. Some of the advantages of this are that the technology is already provided as an online service by companies such as Google Map, MapQuest, OpenStreetMap etc. It is also available as an offline service that can be implemented on any machine. The user can repeatedly perform this activity over and over again because he is used to the environment, the scenario, the device and maps. The same user can also decide to choose an entirely new location to perform the 3D security authentication.



Figure 6: Picture of a 3D Map w(ww.offbeatchina.com)

Gadicha et al stated that 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. Also, 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. Not that designing a new virtual environment is not good but because of reusability and performance of 3D password authentication, it will be much better to re-engineer the existing technology (3D interactive map) and integrate it with 3D password system for accessibility and acceptability of the end-users.

4. CURBING ATTACKS WITH 3D INTERACTIVE MAP

Various attacks on different types of password authentication techniques have been identified, such as:

4.1. Timing Attacks: this has to do with the time required for a user to complete a successful login into an account. The attacker can have enough time to study the password especially when the authentication scheme is not well designed. With a 3D interactive map, the time taken for loading is reasonable, especially for the offline 3D interactive map.

4.2. Well-Studied Attacks: This type of attack is based on a careful study of an authentication scheme by an attacker while trying various combinations of tricks on the scheme. This type of attack is not possible with 3D password authentication technique based on the 3D interactive map because the user's experience of his real-world environment is unique.

4.3. Shoulder Surfing Attacks: This is the only type of attack that seems to work against 3D password with the use of camera or gazing from behind the user. A transparent screen blocker is also designed along with the 3D interactive map to minimize the possibilities of this type of attack.

4.4. Key Logger: The attacker installs key logger software on a target device **intending to retrieve** the password to **perpetuate** his attack. This has been very successful with textual password technique, but with the recent technology, it has not been possible with 3D password technique. And because of the combination of several coordinate points on a 3D interactive map, it makes this even more difficult for hackers.

4.5. Brute Force Attacks: This is when an attacker tries all possible ways in guessing the 3D password which will be very difficult because of time taken to do so and the high number of coordinates in the 3D password space scheme, using the 3D interactive map.

4.6. ADVANTAGES OF USING 3D INTERACTIVE MAP

4.6.1. The technology is readily available

To design other types of the virtual environment for 3D authentication technique, there are lot of things to be considered such as the type of virtual environment to make available to the user, the virtual objects to be included in the environment, and so on. But in the 3D interactive map, the technology behind the virtual environment is already made available by a lot of providers (for example Map, MapQuest, NASA World Wind, OpenStreetMap and so on). Hence, the integration of the 3D interactive map into security authentication will be much easier in planning and implementation.

4.6.2. User familiarity

The mind behind security authentication is that every end-user will be able to use the technology with much ease in protecting his/her data or other valuables. The purpose of the technology will be defeated when the user takes some appreciable **period** in learning a new virtual environment, as in the case of other types of 3D virtual environments. For the

3D interactive map, the users are already familiar with the use of technology as a virtual environment and need not take much time in using the technique for authentication.

4.6.3. Large Space Scheme

In 3D interactive map security authentication technique, the security space scheme is much wider than any other types of security authentications (such as password, biometric, graphics and so on). This is because the combination of numbers of coordinates along the route and the interaction with other objects increases the 3D password space scheme, which is enough to make it wearisome for any hacker

4.6.4. The “forgot your password?” Phrase

One common feature that often comes along with security authentication techniques is the phrase "forgot your password?" which many users often make use of because they have forgotten the password. With 3D interactive map technique, clicking on this phrase will be much reduced because the environment the user chooses is a real-world environment he/she is familiar with and the experience within the environment that could easily be recalled as often as possible.

4.6.5. Easy Acceptability

A user will readily accept to continue to use the technology or the environment he/she is much familiar with than to begin to learn a new one. Hence, 3D interactive map technique will be easily acceptable by the end-users.

4.6.6. User-friendly

User-friendly is part of what most of the 3D interactive map providers **have** already provided along with their platforms, much reason, millions of users are making use of these interactive maps daily. More so, there is no virtual environment that could be designed and made friendlier than the user's real-world environment. The ability to choose a certain real-world virtual environment with its features will further increase user-friendly of the 3D interactive map for security authentication technique.

4.6.7. Freedom of Choice

Unlike other types of a 3D virtual environment where the user is restricted within the virtual environment, in 3D interactive map users can choose any location on the globe as long as it is captured in 3D. Also, users are not limited by the number of virtual objects they can interact with for security authentication unlike other types of 3D virtual environments.

5. CONCLUSION

Textual password, graphical password, biometric password and so on, were the various password techniques employed since the advent of the computer system with people from various backgrounds, such as the industry and the academia, having tried to proffer solution to this issue of security yet hackers consistently counter the solutions. The drawbacks of all these existing security techniques have led to a newer technique called 3D Password. The 3D Password authentication technique can accommodate those previous authentication techniques (Textual password, graphical password, biometric password and so on) which make it difficult for hackers to crack because of the inclusion of 3D virtual environment and its virtual objects. The virtual environment is very similar to the real-world environment and it is also more user-friendly.

Mapping techniques have evolved over the years and with the evolving technologies each location on a map is geo-referenced and the coordinates determined with the aid of satellite and GPS. Interactive maps have also come with 3D and many people all over the world are making use of this technology in locating their favourite stores, restaurants, streets, navigation, and so on. Combining 3D Password security authentication with 3D Interactive Maps will enhance better security authentication, allowing the user to select the area he is much familiar with (user-friendly), making it more difficult for hackers to break and also 3D interactive map is an existing technology and a virtual environment, service, commonly used by users all around the world. With this, it will make 3D password security authentication more secured and better user-friendly as against developing a specific virtual environment for a user to select virtual objects which he might be seeing for the very first time. This can lead to a user forgetting an object that was chosen in the first place when he is to login at another time interval which could be days, weeks, months or years.

6. REFERENCE

1. A.B. Gadicha and V.B. Gadicha "Virtual Realization Using 3D Password" International Journal of Electronics and Computer Science Engineering (IJECSSE). www.ijecse.org Accessed on 5th November, 2019.
2. Kim, H. K., Song, T. S., Choy, Y. C., & Lim, S. B. (2005). Guided navigation techniques for 3d virtual environment based on topic map. In *International Conference on Computational Science and Its Applications* (pp. 847-856). Springer, Berlin, Heidelberg.
3. Geographic Coordinate System http://en.wikipedia.org/wiki/Geographic_coordinate_system. Accessed on 16th November, 2019
4. <http://resources.arcgis.com/en/help/getting-started/articles/026n0000000s000000.htm> Accessed on 5th November, 2014
5. Map Quest <http://www.mapquest.com/> Accessed on 7th November, 2017
6. Nidhi M. P. and Monisha S (2012) "3d Password: Minimal Utilization Of Space And Vast Security Coupled With Biometrics For Secure Authentication" International Journal of Advanced Technology & Engineering Research (IJATER).
7. R. Ramloll and D. Mowat, (2001) "Wayfinding in virtual environments using an interactive spatial cognitive map, " Information Visualization, London.
8. Tejal K., Yugandhara T. and Snehal K. (2012) International Conference on Advances in Communication and Computing Technologies (ICACACT).
9. Vishal K., Vipul G., Sayali K. and Pranjali R. (2013) "Secure Authentication with 3D Password" International Journal of Engineering Science and Innovative Technology (IJESIT).
10. www.designboom.com Accessed on 8th October, 2017
11. www.offbeatchina.com Accessed on 8th October, 2018
12. Kolhe, V., Gunjal, V., Kalasakar, S., & Rathod, P. (2013). Secure authentication with 3D password. *International Journal of Engineering Science and Innovative Technology (IJESIT)*, 2(2), 99-105.
13. Gokhale, M. A. S., & Waghmare, V. S. (2016). The shoulder surfing resistant graphical password authentication technique. *Procedia Computer Science*, 79, 490-498.