Usable Authentication Mechanisms for Mobile Devices: An Exploration of 3D Graphical Passwords

Zhen Yu, Ilesanmi Olade
Dept. of Computer Science and Software Engineering
Xi'an Jiaotong-Liverpool University
Suzhou, China
Zhen.Yu12@student.xjtlu.edu.cn;
Ilesanmi.Olade@xjtlu.edu.cn

Hai-Ning Liang, Charles Fleming
Dept. of Computer Science and Software Engineering
Xi'an Jiaotong-Liverpool University
Suzhou, Jiangsu, China
{haining.liang; charles.fleming}@xjtlu.edu.cn

***Abstract*—Current authentication systems in mobile devices such as smart phones have many shortcomings. Users tend to use simple textual passwords such as PINs, which are easily cracked by intruders. Meanwhile, graphical passwords suffer from shoulder surfing attack. In this paper, a new authentication system using 3D graphical passwords, will be proposed and tested to offer more security for mobile devices. This authentication system allows users to interact with the 3D objects in a 3D virtual environment and these actions are tracked in the virtual environment and used to create unique passwords. Based on the previous studies of the 3D password scheme, this paper developed a simple testing program that enables users to create their own 3D password easily. At the end of the paper, some improvements of the program and this authentication system are discussed.**

Keywords—mobile devices; security mechanism; authentication; 3D graphical passwords; 3D virtual environment.

I. Introduction

Mobile devices such as smart phones and tablet PCs are widely used nowadays due to their portable and multifunctional characteristics. The dramatic growth of mobile device usage has brought about numerous security concerns because they are increasingly essential personal or organizational information storage devices. One main security mechanism of mobile devices is user authentication, which is a process of validating the user's claimed identity. Generally human identity validation techniques can be classified into three categories: knowledge-based, token-based and biometric-based authentication. Since external hardware tokens and biometrics scanners are challenging or expensive to implement and use for mobile devices, knowledge-based authentication involving textual and graphical password are universally acceptable. A four number PIN is a kind of textual password based on human recollection, and are commonly used in mobile devices today. The other prevalent knowledge-based authentication used in mobile devices also includes maze lock, which is a kind of graphical password [1, 2].

Although these widely-used password systems are straightforward to implement on the mobile devices and can be effective, they have a range of weaknesses that are easily utilized by intruders. According to an experiment conducted by Klein [2], 25% (total 15000 passwords) of the textual passwords consisting of letters and numbers could be guessed by using a small dictionary with 3*10^6 words. In addition to these dictionary attacks, users have a tendency to use passwords that are easily remembered such as character string 'password', and therefore their passwords can be simply guessed or cracked through personal relationship or social engineering by an intruder [3, 4]. As for graphical passwords, most of them are easily observed and recorded by shoulder surfing attack, while the graphical password is being entered by the legitimate user [2].

Since existing user authentication systems/solutions have various drawbacks, it is worthwhile to design a more reliable authentication system for mobile devices. Consequently, the objective of this paper is to propose a new set of security mechanisms that can overcome the limitations of the existing user authentication systems and provide more secure and user-friendly authentication for mobile devices.

II. Related Works

Alsulaiman and El Saddik [5] have proposed a new 3D graphical password scheme, which is a multifactor authentication system used in a 3D virtual environment. In the 3D virtual environment, each 3D virtual object has its own response to the actions performed by the user. The different actions and their combined sequences form the user's 3D password. The following scenario can be used to illustrate this concept. In a 3D virtual environment, a user might place virtual objects such as garden tools scattered in a virtual garage in a particular order so as to represent his/her password, or may engage in a form of role playing in the virtual world and thereby using such repeatable actions to represent the password actions that allows login into a mobile device.

The 3D password scheme has many advantages as summarized in [6]. A 3D password is easy to remember because the user can regard the password as a 'little' story. Additionally, the diverse 3D objects and the large number of possible interactions towards them can provide large theoretical password space, which increases the difficulty of cracking.

978-1-4673-8685-2/16/$31.00 ©2016 IEEE

III. Theories & Materials

Based on the rationale and merits of the 3D password scheme proposed by researchers, the basic idea of the new authentication system in this research is creating a 3D virtual environment in the mobile devices, which enables users to interact with various objects in the 3D virtual environment and map these actions to unique password sequences that are reproducible.

In this research, 3D software development is required and we chose the Unity3D package [7] which was utilized to create the 3D virtual environment due to its cross-platform features and powerful 3D modeling and scripting ability using C#. To facilitate the interaction between users and mobile devices, a device called Leap Motion [8], which is a commercial hand tracking hardware, a used to capture the movement of the users' fingers and hands inside a virtual space displayed in the mobile device.

We envisioned the 3D environment as a cubic matrix where "nodes" and "edges" provided the spatial data we needed to construct a unique password. (See Figure 1). Actions within the 3D environment are tracked as a sequence of nodes and edges. (See Figure 2).

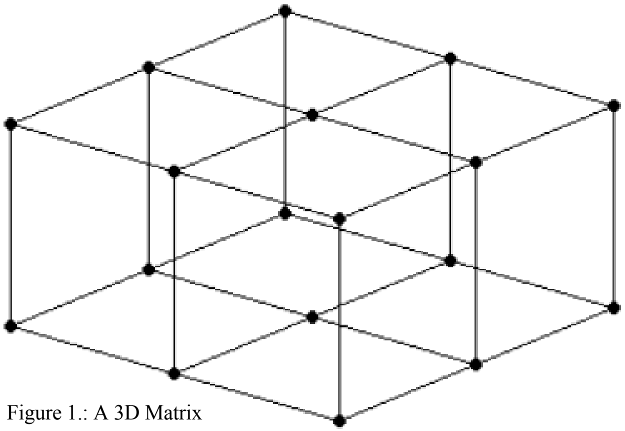

Figure 1.: A 3D Matrix

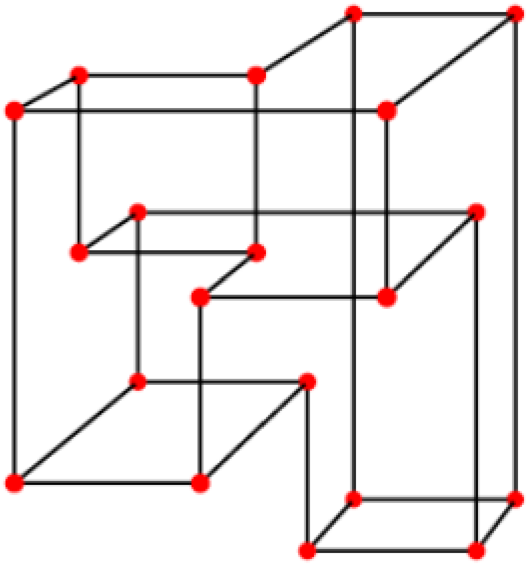

Figure 2.: Actions as a sequence of nodes and edges

IV. Preliminary Results

A testing program was developed to implement the 3D graphical passwords system by utilizing the Unity and leap motion.

A. *User interface*

Figure 3 shows the user interface of this testing program. The user interface is a 3D virtual environment with eight identical green cubes uniformly distributed in the 3D space. The user's hand and hand movement can be sensed by the Leap, and correspondingly the 3D virtual hand model can be displayed in the user interface as shown in Figure 3. With the movement of the hand inside the detection region, the 3D virtual hand model would mimic the user's hand movements, which enables the user to interact with the objects in the user interface.

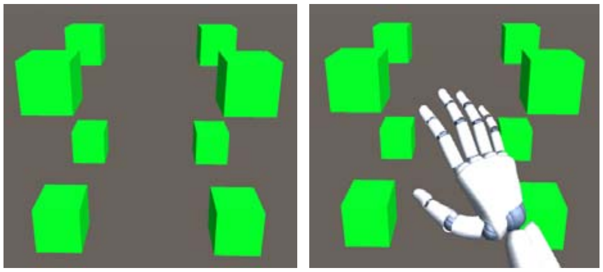

Fig. 3: A simple 3D virtual environment as the user interface. Left picture shows the 3D objects (eight green cubes) in the 3D virtual environment without interactions performed by the user. Right picture shows the user interface with the user's right hand detected by the leap motion hardware.

B. *3D Graphical Passwords*

In this test, the 3D graphical passwords are constructed by the following rules to enable the user to create a reasonable password:

- Every touched cube changes its state and display the state in a visual way.
- The sequence of the touched cubes is be recorded and be displayed in a visual way as a cue to the user.
- The stored sequence is passed to an algorithm that generates a unique password.

The position of the cubes in 3D space can be randomly set and chosen during initial password creation. According to the rules listed above, the process for creating and using the 3D graphical passwords can be achieved and an example of a created 3D graphical password is shown in Figure 4. Each indicated character represents factors in 3D space that are fed into the algorithm. The red line shown in Figure 4 represent additional discretization factors to generate unique passwords.

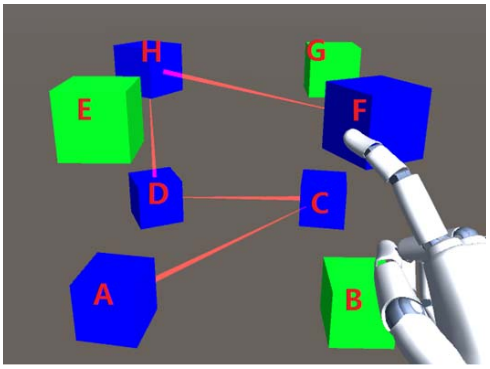

Fig. 4: An example of a 3D graphical password created by the user.

V. Future Work

The simple testing program validates the feasibility of creating 3D graphical passwords in a 3D virtual environment. The next step will be examining its usability in mobile devices. Because the leap motion can be used in android smart phones, as well as the Unity application, the examination will be easily accomplished. As mentioned by Alsulaiman and El Saddik [5], their 3D password scheme proposed can have different kinds of objects in the 3D virtual environment, which can increase the theoretical password space and therefore improve the security. Additionally, they used the coordinate (X, Y, Z) to label each 3D objects. However, only cubes are used as the 3D objects in this research and each of them are merely labeled with simple letter. Consequently, more elements can be added into the 3D virtual environment to enhance the interactivity and security in the future. We plan to eliminate the use of the external Leap Motion hardware and allow users to operate the 3D authentication system solely from the mobile device touch screen interface. Furthermore, it is also necessary to conduct a survey that collects usability opinions about 3D password authentication for mobile devices from the public, which may prove the effectiveness of the 3D password authentication system in practice.

References

[1] Jansen Wayne, Authenticating mobile device users through image selection, The Internet Society: Advances in Learning, Commerce and Security 1, pp. 183-194, 2004.

[2] Alsulaiman Fawaz A., and Abdulmotaleb El Saddik, Three-dimensional password for more secure authentication, IEEE Transactions on Instrumentation and Measurement, 1929-1938, vol. 57, no. 9, September 2008.

[3] Robert Morris, Ken Thompson, Password Security: A Case History, Communications of the ACM, 22(11), pp. 594-597, November 1979.

[4] Daniel Klein, Foiling the Cracker: A Survey of, and Improvements to, Password Security, Proceedings of the 2nd USENIX Unix Security Workshop, pp. 5-14, August 1990.

[5] Alsulaiman Fawaz, and Abdulmotaleb El Saddik, A novel 3D graphical password schema, Virtual Environments, Human-Computer Interfaces and Measurement Systems, Proceedings of 2006 IEEE International Conference on. IEEE, pp. 125-128, July 2006.

[6] Mcchester Odoh, and Ihedigbo Chinedum E., Implementing 3D Graphical Password Schemes, IOSR Journal of Electronics and Communication Engineering, vol. 9, Issue 6, pp. 09-17.

[7] "Unity - Game Engine." Accessed November 27, 2015. http://unity3d.com/.

[8] "Leap Motion." Accessed November 27, 2015. https://www.leapmotion.com/.