Implementation of a Graphical Password Authentication System 'PassPositions'

Gi-Chul Yang and Haengun Oh
Department of Multimedia Engineering, Mokpo National University, Mokpo, Korea
Email: gcyang-umkc@hanmail.net, huoh67@daum.net

***Abstract*—Passwords are often used to secure computers and information Passwords must be secure and easy to use. Traditionally used passwords are text-based passwords that use letters and numbers. However, text-based passwords are long and uncomfortable for users to use and are easy to steal from others. Today, passwords are required to meet the needs of many modern societies. Graphical passwords, which are recognized as an alternative to text-based passwords, have the potential to be superior to text-based passwords in terms of ease of use and security. Many researches have been carried out in various places to realize a useful graphical password authentication system using this potential. In this paper, we compare PassPositions and PassPositions-II, which are recently announced graphical password authentication systems, and show experimental results on usability and security of implemented systems. PassPositionsII is a successor to PassPositions, a graphical password authentication system with improved usability and security.**

***Index Terms*—security, graphical password, usability, authentication**

I. Introduction

The importance of security is increasing day by day in a complex society. Also, as society changes, security techniques are also changing. Passwords are often used to secure computers and information. A good password for security should be easy for the user to remember and difficult for others to steal. However, it is not easy to satisfy these conflicting conditions in a current password system. The same is true in traditional, widely used text-based passwords. Text-based passwords are difficult for users to remember if password lengths are long and complex. Therefore, people tend to prefer short passwords [1]. However, if the length of the password is short, then it is easy to be stolen by others.

Many people in this modern society who need passwords often use a single password in many places. In this case, however, if you lose your password you can lose a lot of information. Therefore, an authentication technique that can replace a text-based password is required. Various authentication methods such as biometric authentication methods have been developed in response to such needs. However, using these new authentication methods requires complex systems and separate hardware. Thus, graphical passwords can be an alternative to authentication methods that can provide better usability and security under similar conditions to text based passwords.

Graphical passwords are based on the fact that pictures are easier to remember than characters [2]. Instead of letters or numbers, pictures or patterns are used as passwords, which are easier to remember than text-based passwords. There have been various studies on the user authentication system using such a graphical password. In this paper, we implement PassPositions and PassPositions-II [3], [4] and show experimental results. In the next section, we explain the difference between PassPositions and PassPositions-II, along with a brief description of the types of graphical passwords. And we show the experimental results on the security and usability of the system implemented in Section 4. And conclusions are made in Section 5.

II. PassPositions and PassPositions-II

The graphical password scheme is an authentication scheme built on the fact that people easily remember pictures rather than letters or numbers. Currently, the graphical password schemes can be divided into four categories. These categories are recall-based scheme, recognition-based scheme, cued-recall scheme, and hybrid scheme. Fig. 1 shows the types of graphical password. (Hereinafter, a user authentication system using a graphical password is simply referred to as a graphical password system.)

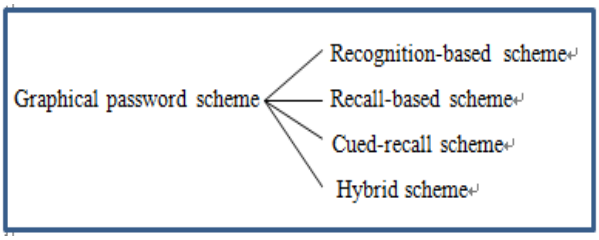

Figure 1. Types of graphical password schemes.

The recall-based graphical password system handles authentication by drawing a memorized pattern same as the password registered by the user or clicking the specific grid drawn in the input window in the predetermined order. They are also known as draw metric [5]. This process is like a text-based password system. At this time, the user has to remember the password without

Manuscript received July 2, 2018; revised December 6, 2018.

doi: 10.18178/joig.6.2.117-121

any help information. Therefore, users are not easy to use long passwords for the recall-based graphical password system. Hence the recall-based graphical password system is weak against dictionary attacks.

A recognition-based graphical password system is a system in which various pieces of information are listed and the user chooses the correct password information to obtain the authentication. For example, the recognition-based graphical password system acquire authentication by displaying a screen having a plurality of faces and selecting a face designated as a password [6]. This method takes a long time to input a password and there may be various problems such as communication cost for collecting, storing and transmitting photograph data necessary for system construction and operation.

The cued-recall type graphical password system inputs the password pattern with the help of the background image and other helpful information. Therefore, it can be seen that the burden on the memorization of the user is less than that of the simple recall-based password system. For example, there is a system that obtains authentication by clicking on predetermined points on a given image in order [7]. Such a system has advantages such as quick input of password and less burden of user's memory. But there are disadvantages of having the hot spot problem through frequent use of specific locations as clicking points and requirement of clicking accurate point.

A hybrid graphical password system is a system that uses several kinds of graphical password techniques together. When building a hybrid graphical password system, it is important to think about interaction and maximize the efficiency of the final system.

PassPositions and PassPositions-II are basically belong to a recall-based graphical password system, but it can considered as a cued-recall type system in that they use the background image in the input window to help remember passwords. To understand the difference between PassPositions and PassPositions-II, first explain PassPositions.

A. PassPositions

PassPositions System [3] is similar to PassPoints system [7], [8] in terms of entering the password by clicking anywhere in the input window in order. However, PassPoints use the absolute position information of the clicked points as passwords, while PassPositions use the relative position information of clicked points as passwords. That is, in PassPoints, authentication is performed by clicking exactly the same position as specified when setting the password, whereas PassPosition uses the relative position information of the clicked points for authentication. Therefore, Even if you click different location, the authentication is done if the positions entered in order are relatively same to the point you clicked immediately before. Therefore, the people who have difficulties to pointing precise locations can use PassPositions easily. And the people who use PassPositions can enter passwords faster than the people using PassPoints. PassPositions security against shoulder-surfing attack is stronger than PassPoints, because you don't need to click exactly the same location each time you enter the password. However, the password space of PassPositions is smaller than the password space of PassPoints.

For example, Fig. 2 (a) and (b) are different passwords in PassPoints, but they are recognized as the same password in PassPositions.

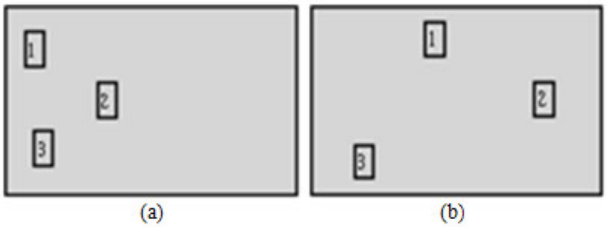

Figure 2. Password difference.

Therefore, PassPositions are easy to use for people who have difficulties to locating precisely, and people can enter passwords faster than PassPoints. PassPositions is also robust than PassPoints because it does not have to pointing exactly the same location each time you enter the password. However, the password space of PassPositions is smaller than the password space of PassPoints.

B. PassPositions-II

The PassPositions-II system has two-part improvement to the PassPositions system. One is that password space is wider than PassPositions, and the other is less likely to make a mistake when constructing a password. PassPositions-II has enhanced password security and improved usability compared to PassPositions.

In terms of security, PassPositions-II differs from PassPositions. In PassPositions, the newly clicked point is compared to just one previous clicked point. In PassPositions-II, however, the relative positions of the current input point against all previously entered points are calculated. Therefore, the password space is greatly increased as shown in the example of Fig. 3.

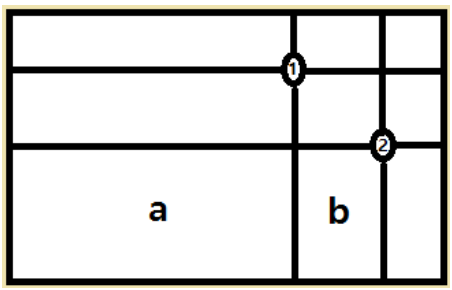

Figure 3. Password space difference.

Fig. 3 explains how password space is different. When the third input point is clicked in Fig. 3, PassPositions generates the same password information irrespective of whether it is located in area a or area b. In PassPositions-II, however, different password information is generated depending on whether the third input point is located in area a or area b. This is because of the relative positions of the third input point to the second input point are the same, but the relative positions of the third input point to the first input point are different.

PassPositions cause an error when a new click occurs on a straight line extending from the previously inputted points to up, down, left, and right directions. And it is difficult for the user to accurately recognize the position of the input point if a new point is inputted at a position close to the straight line. That is, it is not easy to distinguish whether the position of the new input point is above or below the left or right, based on the extending straight line. To improve these drawbacks, PassPositions-II extends the width of lines that extend vertically and horizontally as shown in Fig. 4. Thus, the usability of PassPositions-II is enhanced.

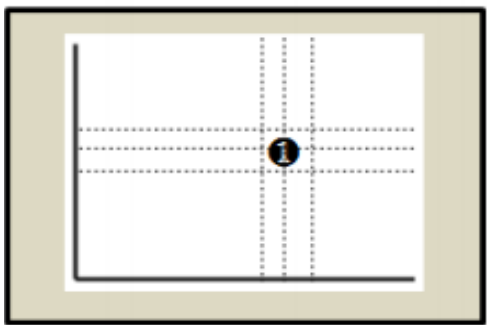

Figure 4. Line thickness expansion.

III. Implementation

The system was implemented in the Galaxy Tab using Java under the Android environment. Hence, currently it works on Android mobile devices.

A. System Comfiguration Diagram

Following Fig. 5 is the system configuration diagram.

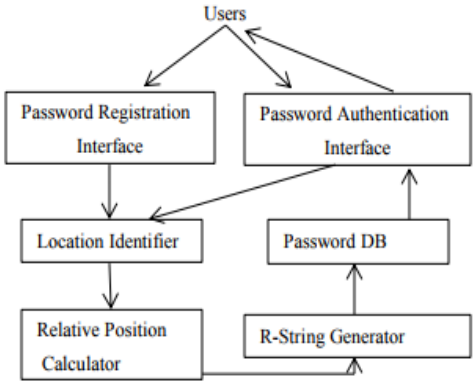

Figure 5. System configuration diagram.

There are two interfaces, one for password registration and the other for password authentication. Both interfaces accept users clicked inputs and pass them to the 'Location Identifier' to get the exact absolute location of a input point. From the second input point corresponding absolute location value passed to 'Relative Position Calculator' to determine the relative position against the previous input point. Next, 'R-String Generator' generates RString as a password and stores it password DB to compare for authentication.

B. Implementation Screen

Following Fig. 6 is the implementation screen of the system.

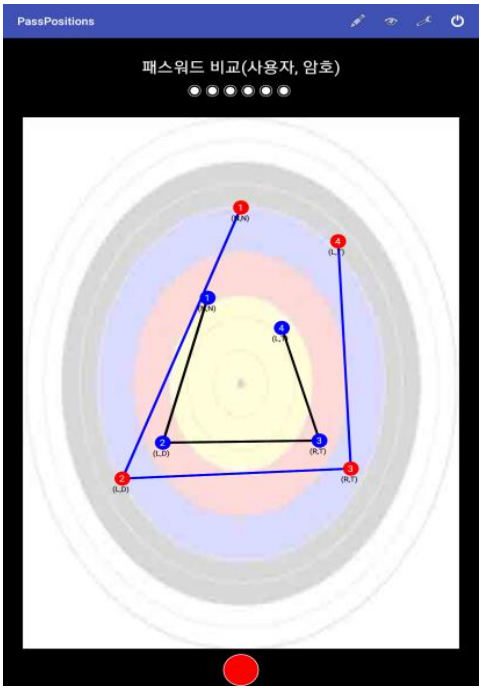

Figure 6. Implementation screen.

C. Way of Use

In order to register a password, the user clicks more than two selection points on the input screen, and the system generates the relative position information and stores it as a user's password in the system.

To register a password, press the button ( ) on the top right of the screen, then the password management screen appears. From here, you can register the password by clicking several points on the screed. To finish the registration, click the button ( ) on the upper right corner and save the password for authentication information.

To authenticate the password, click the multiple selection points in the input screen as you do for registration, and enter the password by pressing the input button ( ) at the bottom center. The system computes the relative position information between the selected points from the input screen and compares it with the registered authentication information to process the authentication.

IV. Analysis of the System

We tried a simple survey on the usability and security of the system. For usability we asked two questions. One is "How long dost it take to login?" The other question is "How many times you may fail to login?". The result of the first question is shown in Fig. 7. Here, 0 indicates the shortest time and 10 indicates the longest time.

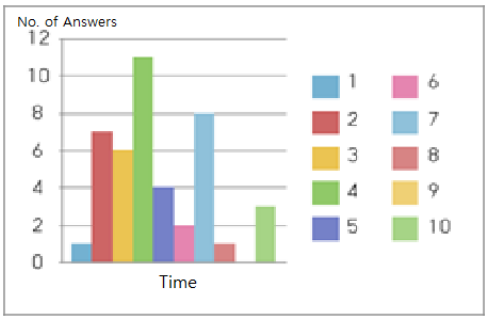

Figure 7. Result of the first question.

The result of the second question is shown in Fig. 8.

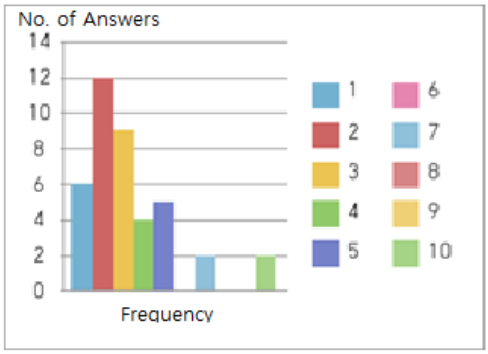

Figure 8. Result of the second question.

For security, we asked a question "How easy do you think it is easy to find someone else's password?" The result is shown in Fig. 9. Here, 1 indicates the easiest and 10 indicates the hardest.

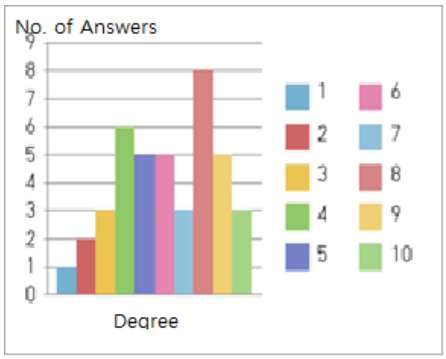

Figure 9. Result of the third question.

More comprehensive analysis may need but we can find overall easiness of the system and strong security power from the survey.

V. Conclusions

Graphical password authentication technique is one of major authentication scheme actively researched around world and getting big attentions from various business organizations these days. Graphical passwords are not easily stolen than text-based passwords and are easy for users to remember.

An efficient graphical password system called 'PassPositions' and its improved version 'PassPositions-II' are explained in this paper. The PassPositions system has been implemented to work in the Android environment with Galaxy Tab. Hence, currently it works on various Android mobile devices.

The PassPositions system is designed based on universal design, so it is easy to use especially for handicapped people. We perform a simple survey to analyze the usability and security of the system. The result of the survey shows that the system is easy to use and has relatively strong security power. It is easy to implement and it is a light system. Therefore, it can be used for various mobile applications by replacing the text-based password schemes.

Acknowledgment

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2017R1D1A1B04032968).

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] R. N. Shepard, "Recognition memory for words, sentences and pictures," *Journal of Verbal Learning and Verbal Behavior*, vol. 6, pp. 156–163, 1967.

[3] G. C. Yang and H. Kim, "A new graphical password scheme based on universal design," *Journal of Digital Convergence*, vol. 12, no. 5, 2014.

[4] G. C. Yang, "PassPositions: A secure and user-friendly graphical password scheme," in *Proc. 4th International Conference on Computer Applications and Information Processing Technology*, Bali, 2017.

[5] D. Angeli, "Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems," *International Journal of Human-Computer Studies*, vol. 63, no. 1-2, pp. 128-152, 2005.

[6] D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes," in *Proc. 13th USENIX Security Symposium*, 2004.

[7] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system," *International Journal of Human Computer Studies*, vol. 63, pp. 102-127, 2005.

[8] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Basic results," in *Proc. Human-Computer Interaction International*, Las Vegas, NV, 2005.

Gi-Chul Yang was born in Gwangju Korea. He received M.S. degree in Department of Computer Science from the University of Iowa in 1986 and Ph.D. degree in Computer Science and Telecommunications Program from the University of Missouri in 1993. Since September 1993, he is with the Department of Multimedia Engineering at Mokpo National University as a Professor. He is interested to research in Artificial Intelligence and HCI. He was a visiting scholar at Heriot-Watt University and University of Hamburg in 2002 and 2015 respectively. He had also collaborated with professors at Linkoping University, University of Zurich, University of Missouri and Drexel University.

Haengun Oh was born in Korea. He received M.S. degree in Department of Computer and Statistics from Mokpo National University in 1998. He finished his course works for Ph.D. in2004. He is currently working as an instructor at Mokpo National University. His research interest includes Graphical Passwords, Conceptual Graphs and RDF.