PassPositions: A Secure and User-Friendly Graphical Password Scheme

Gi-Chul Yang
Department of Multimedia Engineering
Mokpo National University
Mokpo, Korea

Abstract—To solve the problem of text-based password authentication, graphical passwords using images have evolved. Graphical passwords process authentication by selecting the exact positions on the image shown on the screen. These conventional graphical password schemes cannot be used for recognition if the correct points on the screen cannot be selected in the same order. To solve this problem, a new graphical password scheme called PassPositions was introduced. PassPositions were designed based on universal design, so it is user-friendly for everyone, regardless of their physical abilities. However, in certain cases, PassPositions does have some weak points. In this paper will identify a problem of PassPositions, and improve the PassPositions.

Keywords—graphical passwords, authentication, information security

I. Introduction

In today's information society, the importance of information protection is increased day by day. One of the things you need to protect your information is the security of information devices. The most commonly used scheme for the security of information devices, is the password. Password use numbers only, or use combinations of numbers and letters also. This authentication technique is called text-based authentication. There is a problem with text-based authentication that is the numbers should be easy to remember, but others should be impossible to predict. However, In order to remember the password, the password should be short and meaningful. But short and meaningful password can be easily stolen. Moreover, users want to enter a password quickly and long passwords are hard to remember, so they often use the same password for different accounts [1,2]. Therefore, when a password for one account is revealed, it becomes difficult to keep the security of other accounts.

To solve the problem of this text-based authentication, various methods have been developed. Among them, there are fingerprints or iris recognition biometrics passwords [3], graphical passwords using images in place of text, and so on. Biometric techniques can be used with special devices and the system construction cost is high and inconvenient. Also, there is a problem such as personal information leakage. On the other hand, graphical passwords [4] have no problems in biometrics and use images that the users can easily remember rather than text.

Currently, graphic passwords are also developed in various ways. This paper descrives 'PassPositions' a novel graphical password scheme [5] and improve the PassPositions. In the next chapter, shows reviews on some important graphical password systems, and in Chapter 3 explains PassPositions in detail. PassPositions is a kind of graphical password system use Relative Positions. Chapter 4 shows a way of improve the usability on PassPositions. Chapter 5 discusses the direction of future development and concludes the paper.

II. Study on Graphical Passwords

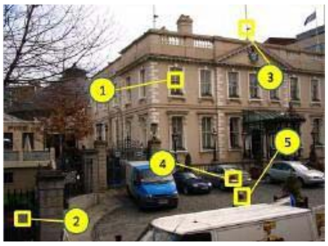
This chapter describes the researches on graphical passwords and what kind of graphical password systems have been developed since the ideas of graphical passwords coming to the present. Knowing the existing systems will help you to understand what is different between PassPositions that has a new concept of authentication and existing systems.

Graphical passwords are easy for users to remember, and difficult for others to predict. Graphical password is a user friendly authentication method compared to text-based authentication techniques [7]. The graphical passwords are rapidly developed as a fast-paced alternative to the text-based authentication since Blonder's idea [4] came out. Graphical passwords are largely can be classified into recognition-based graphical passwords and recall-based graphical passwords. The recognition-based graphical passwords will be described first.

Recognition-based graphic passwords developed from the Blonder-style graphical password [4]. The Blonder-style graphical password system, the developer will define the image to be used and divide into specific zones. The regions of the image divided by different shapes depending on the image can be used as selection points. When you create a password, you select the zones in order, and you can select the same area in the same order for authentication.

This Blonder-style graphical password [4] is necessary to use only predetermined regions within the image as selection points. There are inconveniences that the selection points cannot be arbitrarily determined and users cannot use their personal images. In order to improve the disadvantages of the initial Blonder type graphical password, Wiedenbeck and her colleagues developed a password system which you can use any image or photo with no predefined regions [7, 8]. Therefore, users who use PassPoints can create passwords by select any pixel and scale around selected pixels as selection points regardless of the picture on the screen. The neighboring pixels in the image are all recognized as the same selection point. For example, around a selected pixel, a radius of 2 mm or all the pixels within 3 mm are regarded as selection points.

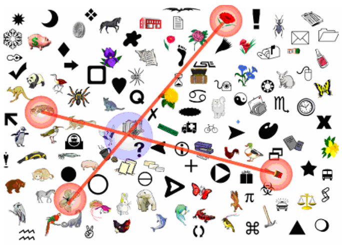
At this time, if the radius is increased, the password can be easily stolen and inconvenient to use if it is small. Also, on-screen image helps only to remember selected points because pixels are used as selection points rather than areas within on-screen. So you don't need to use predefined images and you can use your favorite pictures or photos on the screen. In addition, different pictures on different systems can help to prevent password stealing. Nevertheless, graphical passwords do have certain parts of the picture that are often used as passwords. There are one image and selection points used by the PassPoints system [Fig. 1].



[Fig. 1] An Image and Chosen Points in PassPoints [10]

Dirik and his colleagues studied the possibility of theft in the PassPoints system [9]. That is a study of how to predict in advance what might be a point to be, when a background image is used.

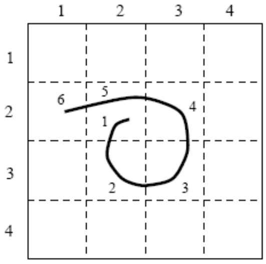
There have, also, been efforts to make difficult to steal your graphical passwords [11,12]. [Fig. 2] is an example of using many objects to make it difficul,t even if you steal passwords from behind your back [12].



[Fig. 2] A Shoulder-Surfing Resistant Graphical Password Scheme [11]

Thorpe and Oorschot have studied a method, how to find a password, called 'Graphical Dictionaries' [15]. Next, examine about recall-based Graphical Passwords.

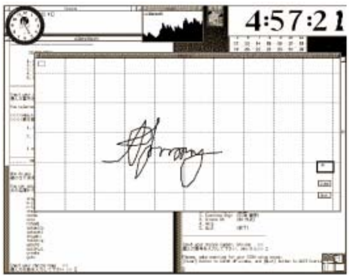
Jermyn and his colleagues introduce a system known as DAS (Draw-A-Secret) as recall-based Graphical Passwords. This system is a system that can draw a pattern as in [Fig. 3].



[Fig. 3] DAS(Draw-A-Secret) Scheme[13]

In the DAS system, there are divided areas on the screen, and a pattern is drawn as they pass through the areas. As the pattern is drawn the order of the passing area is remembered, and the passing order of the areas should be the same for authentication. Therefore, the user should memorize the pattern and reproduce it at the time of authentication.

Then, [Fig. 4] is a system proposed by Syukri and colleagues, the authentication is done by drawing a signature with the mouse in this system [15]. Online signature recognition is another topic and it will not be discussed more in this paper.



[Fig. 4] A Signature Recognition System [15]

By using Syukri and his colleagues system, it is easy to remember the passwords and difficult to use by others because it allows users to use their own signature as a password. However, it has the disadvantages of being difficult to use and the procedure of recognition is complicated. In recent years, the techniques that use graphical passwords and text-based passwords together also had been introduced [16]. Chapter 3, a new concept graphical password system called PassPositions.

III. Pass Positions

Unlike most existing graphical password schemes, ‘PassPositions’ is a graphical password scheme, which uses relative positions of the click points. If the user uses a thick pointer or a finger, and presses a region instead of a point (at a pixel level), then PassPositions will find the center point of the region automatically, and use the center point as the click point. Earlier graphical password schemes than PassPositions (e.g. PassPoints) used absolute coordinates of the click points. For example, a user chose three points, and their (x, y) coordinates values were (100, 650), (430, 330), and (170, 70). These absolute values of coordinates were used as a password for graphical password systems earlier then PassPositions. It is difficult, however, in the recognition phase, to choose those exact points again. This leads to discretizing the image into squares that are large enough to allow the user to easily hit the same square. So, the system allows certain areas around the chosen points. But the size of the allowed pointing area affects the reliability of the password system [8]. The click points can possibly be expanded to the click regions, within some tolerance distance (e.g. within 0.25 cm) in the PassPoints system. However, allowing arbitrary click regions leads to the edge problem of discretization, and it can be solved by simultaneously using three discretization grids, as described by Birget et al. in [17].

However, PassPositions remembers the relative positions of the chosen points. The relative position indicates the direction of the current chosen point, according to the chosen point just one step prior to the current chosen point. In the registration phase of PassPositions, a user chooses several points on the screen in order, and the relative positions of all the chosen points are remembered by the system, except the first chosen point,. For example, if the PassPositions is applied with an image size of 1024 x 752 (roughly the full screen), and three points are chosen (i.e. (150, 650), (530, 330), (370, 70)), as shown in Fig. 1, then PassPositions generates R-String (RD, LD) in the registration phase.

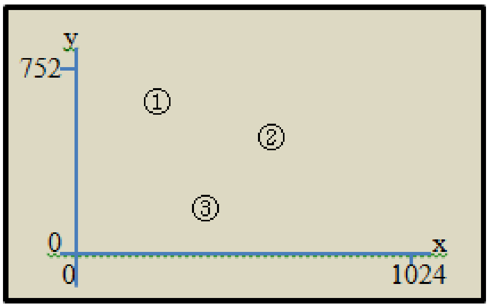


Fig. 1: Three Chosen Points in PassPositions

R-String is a variable to hold the relative positions of the chosen points. RD means Right-Down, which indicates that the second chosen point’s location is relatively to the right hand side of the first chosen point (the point just before the current chosen point), and down below the first chosen point. The meaning of the symbols used for R-String is explained in Table 1.

Table 1: The meaning of the symbols used for R-String

Symbol	Meaning
L	Current point’s x-coordinate value is less than the x-coordinate value of the previous point. (Current point’s position is to the left of the previous point)
R	Current point’s x-coordinate value is greater than the x-coordinate value of the previous point. (Current point’s position is to the right of the previous point)
U	Current point’s y-coordinate value is greater than the y-coordinate value of the previous point. (Current point’s position is above the previous point)
D	Current point’s y-coordinate value is less than the y-coordinate value of the previous point. (Current point’s position is below the previous point)

If a user choose the points (550, 650), (950, 330), and (100, 70) at the registration phase, then PassPositions will generate the same R-String (RD, LD). This case is displayed in Fig. 2.

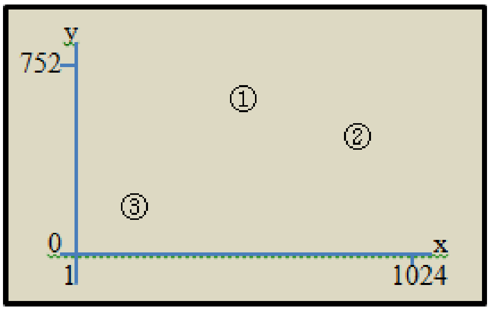


Fig. 2: Another Three Chosen Points in PassPositions

So the passwords will be matched, even though the points are not in the same absolute location. Some may think this freedom creates a security problem that makes the password easily breakable. The entropy problem can occur in most graphical password schemes. Hollingsworth et al. confirms that many users may be attracted to incongruous or unexpected elements, which can be ‘hot spots’ in an image [18]. In PassPoints, only a half of the area of the image is used, and the other half of the area has no memorable features to click on [9]. Basically, in most graphical password schemes, including PassPositions, this kind of password space problem can be solved by increasing the number of click points in the password registration phase. Also, in the case of PassPositions, an image appearing on the screen would not have much effect on the click point distributions and hot spots problem, since PassPositions can work without any image on the screen. A secure method that can solve the password space problem for PassPositions is introduced in the next section, for those people who want a more secure system.

IV. Improvement on Pass positions

Previously, researchers focused mainly on technical problems to solve the security problem, until there were efforts to see the security problem as a Human-Computer Interaction (HCI) problem, to make the security mechanism effective [19, 20]. PassPositions is a user-friendly system that enables the user to easily learn to input graphical passwords without error, and create passwords quickly and easily. However, there is still room to improve PassPositions, from the viewpoints of usability and security. For example, if a user selects two points (15, 35) and (15, 25), then the R-String generated by PassPositions would be (D), which means the second point is right below the first point (i.e. Down), and it is not to the left or right of the first point. If this case happens, it is difficult to once again choose the points that can generate the same R-String (D) (i.e. the points that have the same value of x-coordinates, and a lesser value of y-coordinates). PassPositions needs a little modification, to provide a more error-free and user-friendly password scheme. The idea for improvement of PassPositions is described in the next section.

From the usability viewpoint, PassPositions can be improved, by removing the possible occurrence of errors as much as possible, and reducing the password input time. If an R-string is (R, D), this means the y-coordinate values of the first chosen point and the second chosen point are the same, and the x-coordinate values of the second chosen point and the third chosen point are the same. That means the first chosen point and the second chosen point are on the same horizontal line, and the second chosen point and the third chosen point are on the same vertical line.

In this case, it is difficult to click the point on the same line (at the pixel level) again, in the recognition phase. Hashing does not allow approximation, but the hashing problem can be solved by discretizing the image, and the edge problem with the discretization square can be solved, by simultaneously using three discretization grids [17]. Improved PassPositions allows a tolerance area of 2 pixels by default (or the user can adjust the range) in four directions around the chosen points. Hence, choosing a point on the same vertical or horizontal line becomes easier for the user, and the possibility of error occurring is reduced.

As we know, higher tolerances may lead to many false positives, while lower tolerances may lead to many false negatives. Possible problems that are raised by the error tolerance can be compensated for with other well-known methods, such as increasing the number of click points, magnification of an area of the image, and so on. The tolerance area allows a user more freedom to select a point on the same line. With the tolerance area, it is more user-friendly, and allows a user to quickly and easily input a password, without extra concerns of choosing a point on the same pixel line. This may lead to more secure password behavior.

V. Conclusion

This paper studied about graphical password among authentication methods that can replace text based authentication method, and desribes PassPositions which is a new concept of graphical password system implementation technique. PassPositions generate the authentication code by taking advantage of the relative positions of the selection points, making it easy for people who cannot select the correct absolute position [5].

PassPositions can be made even more practical when used in mobile devices that operate directly using the touch pad with hands. When using a tool such as a mouse or electronic fan, it is relatively easy to select the narrow area more accurately than when using the hand. PassPositions also allows you to freely select images for your backdrop as you would in the PassPoints system. In other words, the user can use the desired image or photo as the background image, which makes it possible to build a system that meets the user's individuality. It can be used even without any background picture. This feature prevents the password space problem caused by the hot spot which is a problem in the conventional graphical password systems.

And PassPositions can help you solve the problem of password stealing by selecting different locations each time for the same password. In addition, PassPositions uses a relative position string (RP-String) unlike the existing graphical password scheme, so it can easily tell a password to another person through a simple character string as in text-based authentication [5]. However, in certain cases, PassPositions does have some weak points. In this paper identified a problem of PassPositions, and improve the PassPositions.

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

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

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

[4] Blonder, G., "Graphical passwords," in Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent, Ed. United States, 1996.

[5] G-C Yang and H. Kim, “A New Graphical Password Scheme based on Universal Design” The Journal of Digital Convergence, Vo.15, No. 5, 2014.

[6] Ronald L. Mace, Graeme J. Hardie, Jaine P. Place, Accessible Environments: Toward Universal Design, a chapter in Design Intervention: Toward a More Humane Architecture, W.E. Preiser, JC. Vischer, E.T. White (Eds.). Van Nostrand Reinhold, New York, 1991.

[7] Xiaoyuan Suo Ying Zhu G. Scott., Graphical Passwords: A Survey, In 21st Annual Computer Security Applications Conference(ACSAC), 2005.12.

[8] 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, 63, pp. 102-127, 2005

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

[10] A. E. Dirik, N. Memon, J.C. Birget, ``Modeling user choice in the PassPoints graphical password scheme'', Symposium on Usable Privacy and Security(SOUPS), at Carnegie-Mellon Univ., Pittsburgh, July 2007

[11] D. Hong, S. Man, B. Hawes, and M. Mathews, "A password scheme strongly resistant to spyware," in Proceedings of International conference on security and management. Las Vegas, NV, 2004.

[12] S. Man, D. Hong, and M. Mathews, "A shoulder surfing resistant graphical password scheme," in Proceedings of International conference on security and management. Las Vegas, NV, 2003.

[13] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The Design and Analysis of Graphical Passwords," in Proceedings of the 8th USENIX Security Symposium, 1999.

[14] J. Thorpe and P. C. v. Oorschot, "Graphical Dictionaries and the Memorable Space of Graphical Passwords," in Proceedings of the 13th USENIX Security Symposium. San Deigo, USA: USENIX, 2004.

[15] A. F. Syukri, E. Okamoto, and M. Mambo, "A User Identification System Using Signature Written with Mouse," in Third Australasian Conference on Information Security and Privacy (ACISP): SpringerVerlag Lecture Notes in Computer Science (1438), 1998, pp. 403-441

[16] Ahmad Almulhem, “A Graphical Password Authentication System”, World Congress on Internet Security (WorldCIS-2011), London, UK, February 21-23, 2011.

[17] J.C. Birget, Hong, D., Memon, N., 2003. Robust discretization, with an application to graphical passwords. Cryptology ePrint Archive http://eprint.iacr.org/2003/168. Accessed January 17, 2005.

[18] Hollingsworth, A., Williams, C.W., Henderson, J.M., 2001. To see and remember: visually specific information is retained in memory from previously attended objects in natural scenes. Psychometric Bulletin and Review 8 (4), 761.768.

[19] Patrick, A.S., Long, A.C., Flinn, S., 2003. HCI and security systems. In: Proceedings of the CHI 2004. ACM Press, New York, pp. 1056–1057.

[20] Dourish, P., 2004. Security as experience and practice: supporting everyday security. Talk given at the DIMACS Workshop on Usable Privacy and Security Software, July 7, 2004.