Graphical Password Based On Standard Shapes

Mohammad A. Alia,
dr.m.alia@zuj.edu.jo

Adnan A. Hnaif
dr.adnan_hnaif @zuj.edu.jo

Hayam K. Al-Anie
drhayam@zuj.edu.jo

Abdelfatah Aref Tamimi
Science@zuj.edu.jo

Department of Computer Information Systems, Faculty of Science and Information Technology –
Al Zaytoonah University of Jordan, P.O.Box: 130 Amman (11733) Jordan.
Tel: +962 6 4291511

Abstract

In this paper, we propose a new graphical password scheme to be an alternative to alphanumeric passwords in which users draw their passwords by selecting shapes to authenticate themselves rather than type alphanumeric sequences. This scheme was developed in two processes: identification and authentication processes that are based on system access control approach. In fact, this graphical password is more efficient than others graphical password schemes; since the proposed scheme is based on three simple factors; 1) shape abbreviation, 2) order of drawing shapes, and 3) size of the drawn shapes. However, this study is presented to provide the identity of an entity with very simple authentication protocol that based graphical password. Whereby, the graphical password is considered easier to be remembered than other password techniques for most computer users.

Keywords: graphical password, identification authentication, password, and access control.

1. Introduction

A large number of internet users and the power have reacted in contrasting to the researchers in developing protection algorithms of authentication protocols. That is to ensure the highest degree of protection to users against the brute force attacks with lowest cost. Therefore, the major motivation of this study is to reduce the computation cost and increase the security for the authentication based access control protocols. This motivation leads us to propose new authentication protocol based on graphical password. Since, there are many previous works in password based authentication. Most of these protocols were design in the textual approaches.

1.1 System Access Control (Logging)

System access control (SAC) (Lehtinen, 2006; Stallings, 2011) is the first defense layer in computer security system where computer system can provide security by controlling users to access systems. SAC process determines who is allowed to log into system, decides whether a user is authorized, and keeps track of user processing in the system. On other hand, this process is used to ensure that the system it is

accessible only to a legitimate user. Therefore, SAC includes two steps: identification (the user should tell the system who is who) and authentication (the user should prove his/her identity to the system).

Identification and Authentication: As discussed earlier, Identification and authentication (I&A) (Lehtinen, 2006; Stallings, 2011) are processes which can be used to identify and authenticate the users on the system. However, in most currently used systems, the user must identify (him/her)self, then the system will authenticate the identity before accessing the system resource. Therefore, the identification and authentication processes can be done successfully through the following three general methods (refer to Figure 1):

- Something you know: The most common way is a password.
- Something you have: Examples are smart cards and tokens.
- Something you are: Examples are handprint, fingerprint, voice, retina, and iris pattern.

1.2 Password Authentication Protocol

Password (Stallings, 2011) is the most common used method in authentication protocols. Whereby, the user should prove his/her username and password by comparing it with the system stored value. This authentication method is important for users since it is easy to be memorized. However, password is classified into two main types; textual password and graphical password.

Graphical password: A graphical password is one of the most important fields of authentication in system access control techniques. It allows users to draw or select their passwords from images bar, in a specific order. Then the password will be presented in a graphical user interface (GUI). On other hand, the graphical password is also defined as graphical user authentication (GUA). Therefore, graphical password is considered easier than other password techniques base text, since it is easy to be remembered for most computer users.

In term of security, graphical password offers better security than other textual passwords because the graphical password is created by selectable images as a series. These series is normally combined in specific order of images. Therefore, the graphical passwords are recently designed to be resisted to many kinds of attacks such as; shoulder-surfing. Whereas, it will be difficult to recognize the exact images series order (graphical password) by attackers.

However, this paper presents a new authentication protocol based on graphical password in which users draw their passwords from shapes tool bars to authenticate themselves rather than type alphanumeric texts.

2. Literature Review

There are many graphical password schemes have been done successfully. Among them are Jansen schemes (Jansen, 2004; Jansen, 2003), authentication schemes for session passwords using color and images (Sreelatha et al., 2011) a new graphical password scheme resistant to shoulder-surfing (Gao et al., 2010), a hybrid password authentication scheme based on shape and text (Zheng et al., 2010) and etc.

In (Jansen, 2004; Jansen, 2003), Jansen proposed his authentication schemes based graphical password for mobile devices. In general, these schemes are consist two major phases: registration phase and authentication phase. In registration phase, the users are required to create their password object by choosing set of images in thumbnail size. Whereas, the authentication stage, the users must input the password object correctly as it is in registration phase. However, each chosen image is represented by a numerical value, and the sequence of the chosen images will generate a numerical password as well.

In (Sreelatha et al., 2011), the authors proposed their scheme by using two authentication techniques that is based on text and colors for personal digital assistant (PDAs): pair based technique and hybrid textual technique. Whereby, these two techniques use grid for session passwords generation. This password authentication scheme is secure since the password is used once for one login process.

In 2010 (Gao et al., 2010) have proposed their graphical password Scheme CDS to be Resistant to shoulder-surfing by using N × N grid image (refer to Figure 2). In CDS scheme, the authors improve the user authenticity by combining DAS (Jermyn et al., 1999) and Story (Davis et al., 2004) schemes. Orderly, the users are required to draw a curve over their password images (pass-images) instead of clicking on them. However, the curve must be drawn randomly by selecting begin and end images. CDS scheme displays ambiguous passwords which are difficult to be distinguished attackers.

A Hybrid password authentication scheme (Zheng et al., 2010) proposed a scheme to make a bridge between the graphic and textual password. This scheme is designed to be used in computer system and mobile devices. Basically, the idea of this scheme is to make a graphical password map from shape to text whereby this map can be done with strokes of the shape and a grid with text. Actually, the design of the scheme focuses on following four factors:

1. Shapes and password as strokes on the grid, since the designed shape (shape of stroke) can be easier to remember than text by authorized users.
2. Large password space.
3. Resistant to shoulder-surfing.
4. Keyboard login process which can be supported by text.

Figure 3 shows the process of the creating graphical password based hybrid scheme by mapping from shape into a grid. Then the designed shape is symbolized by a number of the used blocks on the grid. However, this scheme still has some weaknesses, since 1) it is relativity unfamiliar to the public, 2) password creating process is vulnerable, and 3) in term of logging process time, it is very long comparing to other graphical schemes.

3. The Proposed Graphical Password Scheme

As mentioned earlier, many previous studies on graphical password have been done and focused on resistant to Shoulder-Surfing. In the proposed scheme, access control ensuring that authorized users access only resources and services that they are entitled to access. As well, system access control process is used to authenticate the user. The objectives of an access control system are often described in terms of protecting system resources against inappropriate or undesired user access. The proposed system access control is actually based on graphical password authentication process that involves two phases: registration and authentication.

3.1 Registration Phase

In this phase (refer to Figure 4), the users should identify themselves to the system by creating and confirming their graphical password. The users have to select a password based on the graphical interface that is displayed on the screen. Whereby, this password can be composed from series of standard shapes as shown in the standard shape bar in Figure 4. However, this bar consists ten standard shapes to be used in forming a particular object (refer to Figure 4). Typically, the user must draw his/her graphical password in the specified navigation area with at least five shapes as a minimum number to create the object.

Basically, this phase focuses on three main factors:

- Shape abbreviation.
- Order of drawing shapes.
- Size of the drawing shapes.

As shown in Figure 5, the three mentioned factors are considered during drawing process since the textual password will be created. Each shape is presented by two letters (refer to Table 1). Sequentially, the order

of the drawn shapes is stored and numbered according to the order of drawing process. Finally, the size of the drawing shapes is calculated during the drawing process.

Continuously, the users have to confirm their passwords registration by redrawing the password in the right shapes sizes and order as shown in Figure 6. Similar to the registration phase, the confirmation phase gives the user chance to familiarize the authentication process as shown in Figure 6.

As discussed earlier, the system will produce the textual password along with the graphical password. The textual password consists of letters and numbers that map the three mentioned factors. Particularly, each shape (refer to Table 1) is abbreviated to text from two letters. The order of the drawing shape assigns numbers. Respectively, the size of shape is also considered by assigning relative number according to other drown shapes. Finally, the drawn graphical password is stored as a text in the intended system.

3.2 Authentication Phase

In this phase, the user can access the intended system by logging into the system using his/her correct username and graphical password.

4. Discussion

We implemented our proposed graphical password scheme to show the performance of the proposed system comparing with other systems. As discussed in Section 3, the user should use some of the shapes to draw an object which will be considered the password. Figure 7 shows that the user has drawn his/her object as a simple computer sketch by selecting set of shapes: two rectangles, rounded rectangle, line, and circle.

The shapes were drawn in the following order:

1- Rectangle (Figure 7, Step 1).
2- Rectangle (Figure 7, Step 2).
3- Rounded Rectangle (Figure 7, Step 3).
4- Line(Figure 7, Step 4).
5- Circle (Figure 7, Step 5).

In Figure 7, the size sequence of each shape is relatively listed from biggest to smallest as follows:

1- Rectangle (Figure 7, Step 2)
2- Rectangle (Figure 7, Step 1).
3- Rounded Rectangle (Figure 7, Step 3).
4- Line (Figure 7, Step 4).
5- Circle (Figure 7, Step 5).

When the drawing process was completed, the textual password is created according to the drawn shapes, and then the password will be displayed in the textual password field as illustrated in Figure 7.

However, the generated password in Figure 7 is composed of letters and numbers. The letters represents shape abbreviation for the drawn shapes and the numbers represents the sizes of the drawn shapes. Moreover, the abbreviation of each shape is represented as (refer to Table 1): "rc" for rectangle, "rr" for rounded rectangle, "ln" for line, and "cl" for circle.

In this example, the numbers represent the sizes of the drawn shapes such that the biggest shape assigned number 1 and the numbers will be increased for the other shapes. Similarly, the order of the drawn shapes is according to the order that followed during the drawing done by the user. So the password will be as follows:

rc2rc1rr3ln5cl4

In term of security, this Subsection presents the security analysis for the proposed graphical password scheme. We suggest that the minimum number of shapes is five for a password object. This should give 5! (Factorial of 5) possibilities for every password that is being attacked with brute force. However, the security protection of the proposed scheme depends the drawing factors and the randomness of the output generated.

5. Conclusion

This paper has presented a new authentication scheme based graphical password . This scheme has been proposed to be an alternative to textual password schemes whereas the users can draw their passwords by selecting shapes sequences. Mainly, the proposed scheme includes identification and authentication processes that are based on system access control approach. As the result, the proposed graphical password is more efficient than others graphical password schemes since the proposed scheme is based on three simple factors; the shape, the drawing order, and the shape size. As well as, this scheme is considered easier to be remembered than other password techniques for most users.

Acknowledgment

The authors would like to thank Al Zaytoonah University of Jordan for supporting this study.

References

Davis, D. F. Monrose, & Reiter, M. K., (2004). On user choice in graphical password schemes. *In Proceedings of the 13th Usenix Security Symposium. San Diego, CA*.

Gao, H. Zhongjie, R. Chang, X. Liu, X. & Aickelin, U. (2010). A New Graphical Password Scheme Resistant to Shoulder-Surfing. *International Conference on CyberWorlds.*

Jansen, W. (2003). Authenticating Users on Handheld Devices. *In Proceedings of Canadian Information Technology Security Symposium*.

Jansen, W. (2004). Authenticating Mobile Device User Through Image Selection. *In Data Security.*

Jermyn, I., Mayer, A. Monrose, F. Reiter, M. & Rubin, A. (1999). The design and analysis of graphical passwords. *In Proceedings of the 8th USENIX Security Symposium*.

Jansen, W. Gavrila, S., & Korolev, V. (2003). A Visual Login Technique for Mobile Devices. *National Institute of Standards and Technology Interagency Report NISTIR 7030*.

Lehtinen, R. (2006). *Computer Security Basics*. (2nd ed.), O'Reilly. ISBN-10: 0-596-00669-1.

Sreelatha, M. Shashi,, M. Anirudh, M. Sultan Ahamer, Md. & Manoj Kumar, V. (2011). Authentication Schemes for Session Passwords using Color and Images. *International Journal of Network Security & Its Applications (IJNSA)*, Vol.3, No.3.

Stallings, W. (2011). *Cryptography and Network Security.* (5th ed.). Pearson Education.

Zheng, Z, Liu, X. Yin, L. & Liu, Z. (2010). A Hybrid Password Authentication Scheme Based on Shape and Text. *Journal Of Computers*, Vol. 5, No. 5.

Table 1. Proposed Graphical Password Standard Shapes

Shape	Shape Name	Shape Abbreviation
	Rectangle	rc
	Hexagon	hx
	Line	ln
	Triangle	tn
	Circle	cl
	Star	st
	Parallelogram	pl
	Arrow	ar
	Diamond	dm
	Rounded rectangle	rr

Figure 1. Authentication Schemes

Figure 2. CDS Scheme (Gao, et. al., 2010)

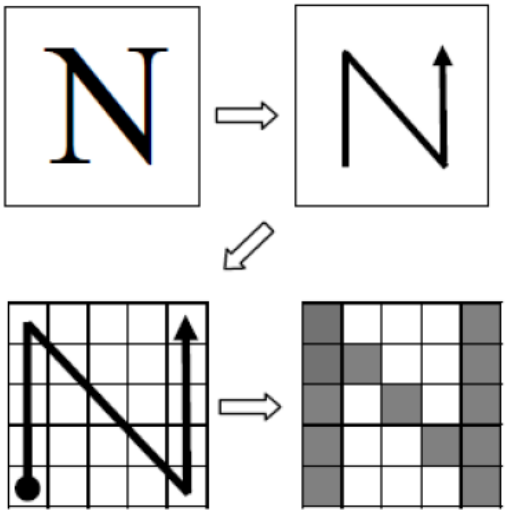

Figure 3. Hybrid Scheme (Zheng, et al., 2010)

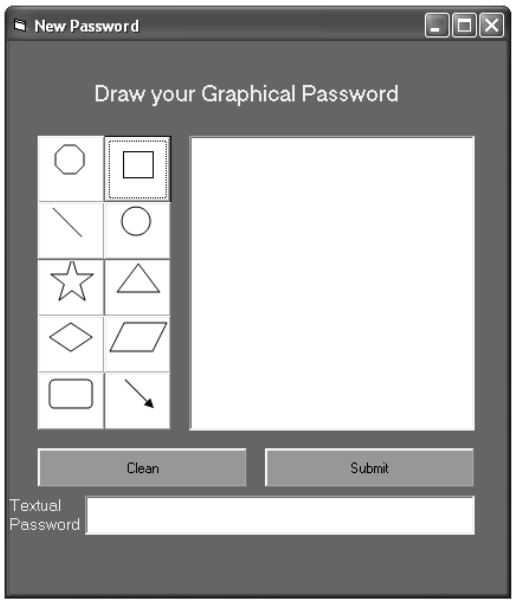

Figure 4. Form for New Password

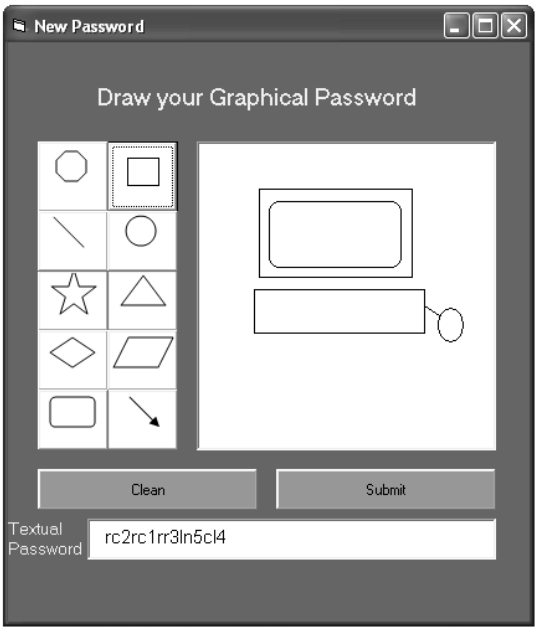

Figure 5. Form for Creating New Password

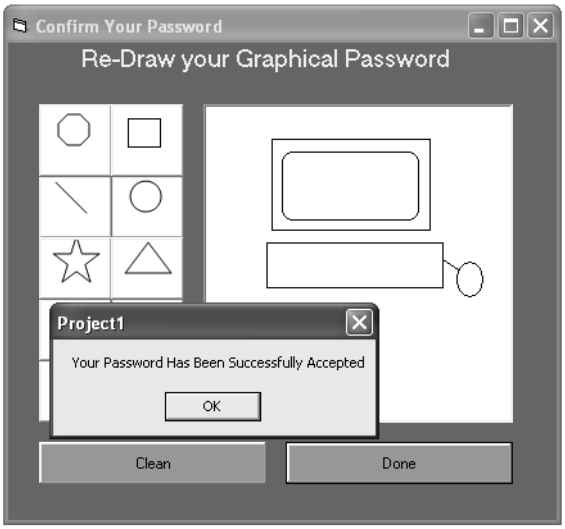

Figure 6. Form for Password Confirmation

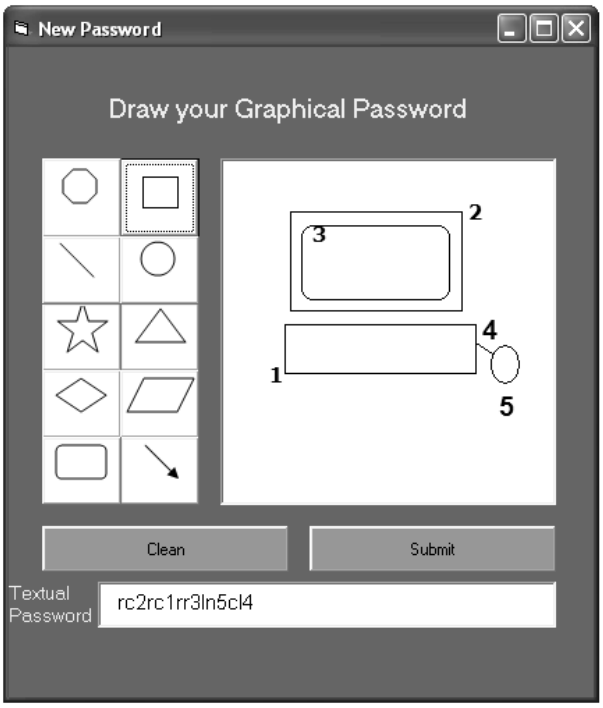

Figure7. A Working Example for the Proposed Graphical Password