GRID-IMAGE PASSWORD BASED SCHEME: ENHANCING MEMORABILITY FEATURES OF PASSWORDS

1Obasan Adebola, 2Norafida Ithnin and 3Mohd Zalisham Jali
1,2Information Assurance and Security Research Group, Department of Computer System and Communication, Faculty of Computing, Universiti Teknologi Malaysia, Malaysia, Skudai, 81310 Johor, Malaysia
3Faculty of Science and Technology, Universiti Sains Islam Malaysia, 71800 Bandar Baru Nilai, Negeri Sembilan, Malaysia

Received 2012-10-30; Revised 2013-03-04; Accepted 2014-07-28

ABSTRACT

Password authentication has become a widely recognized element of computer security practices where human users are proven or confirmed as legitimate users for access to secure systems. Using this system, every user needs to recall its password correctly before access can be granted to an intended service or applications. Remembering the secure passwords is an everyday problem for users because of individual memory limitation. In an effort to solve this problem, graphical password was presented as one promising authentication alternative taking advantage of picture superiority over texts. The main objective of this study is to provide a comprehensive survey of array of graphical password schemes in different categories based on their common features with the primary aim of identifying the memorability features and propose a new graphical authentication system with enhanced memorability features.

Keywords: Graphical Passwords, Password Space, Authentication

1. INTRODUCTION

Computer security is a critical issue with modern information systems because its valuable contents and diverse day-to-day applications, namely banking, accounting and others. Consequently, they require some measures of control and protection to ensure reliability, integrity and other security goals. In order to achieve reasonable level of protection, username-password methods have been widely used as method of choice for identifying, authenticating and authorizing users by many banks, government and corporate bodies and even all websites on the internet. The user identification is employed to identify a user to the system while the authentication proves user’s claimed identity as being right or wrong depending on username and corresponding password. In order to complete used authentication process, authorization deals with the users’ right to access resources ones they are authenticated. Text-based password method was introduced in the 1960s as a security measure to restrict access of useful information to authorized users within a computer system setup or worldwide networked computers (Nielsen and Vedel, 2009).

Conversely, it is popularly known that text passwords are vulnerable and insecure for a number of problems (Biddle et al., 2012; Lashkari et al., 2009). For this reason, other factors are used to complement and improve the security of text password mechanisms (Karnan et al., 2011; Tiwari et al., 2011; Vu et al., 2007). The main problems of text-based passwords is that users find it difficult to remember secure passwords which are expected to be meaningless strings choosen from lower and upper case letters, digits and special symbols (Zhang et al., 2009). Intensive studies in this area have revealed that users tend to pick short passwords or passwords that are meaningful in favour of memorability (Biddle et al., 2012; Vu et al., 2007). Unfortunately, such meaningful strings are weak text passwords which can be easily guessed or broken, by an attacker who strives maliciously to obtain the legitimate user passwords through dictionary, keystroke logging.

Corresponding Author: Obasan Adebola, Information Assurance and Security Research Group, Department of Computer System and Communication, Faculty of Computing, Universiti Teknologi Malaysia, Malaysia, Skudai, 81310 Johor, Malaysia

Science Publications

1065
phishing, eavesdropping, shoulder surfing and other threats (Bonneau, 2012; Forget et al., 2010; Hafiz et al., 2008; Owens and Matthews, 2008).

Moreover, another easy method that can be used to restrict access of information to the legitimate users through knowledge-based authentication mechanism which does not require additional hardware is graphical passwords where pictures are drawn via mouse or stylus to register passwords instead of texts to lessen the passwords being forgotten. This advantage is caused by the capability of humans memory which retains graphical representations longer than texts. In 1996, the idea of Graphical passwords was conceived by Blonder as an alternative to text-based password for user identification (Almuairfi et al., 2011; Chiasson et al., 2007; Zhang et al., 2009). In this system, an image appears on the screen, then user clicks with the help of mouse or stylus on one or more chosen regions of the displayed image to create a password. A user can only be authenticated if correct regions are clicked at later stage.

1.1. Graphical Password Authentication Systems

Today, many graphical password systems which require use of visual information to identify users are available in many forms and to some extent, they provide features required to overcome passwords memorability problem for users in user-friendly environments provided by the same graphical systems (Almuairfi et al., 2011). This is possible due to psychological theories that humans have a momentous competence to recall and to recognize visual information or images. In addition to making passwords easy to remember, graphical password methods must provide desirable level of security to resist some basic attacks such as dictionary and brute attacks, an attacker must construct a bigger dictionary than conventional textual passwords before these attacks can be successful (Zhao and Li, 2007).

Over the last decade, several graphical password systems have been proposed with intensive studies on them. The available graphical password schemes are categorized in diverse forms. Table 1 below discusses a number of schemes that are relevant to our study in two categorizations. In a grid-based graphical system, user typically draws and reproduces their password on a drawing grid to verify its identity (Nali and Thorpe, 2004; Tyagi et al., 2011). This approach is alphabet independent and as such making it equally accessible for users of any language (Jermyn et al., 1999). These systems exist in different forms as illustrated in Table 1 below. The Figure 1 shows Drawing-A-Secret (DAS) scheme. Other implementation alternatives of DAS scheme (Chalkias et al., 2006; Lin et al., 2007; Tao and Adams, 2008; Thorpe and Van Oorschot, 2004) are also represented in Fig. 1. While in an image-based graphical system, users typically draw and reproduce their passwords over some portion or the entire picture/image for the purpose of authentication. These systems are in different forms (Wiedenbeck et al., 2005) as illustrated in Table 1. PassPoints system is the image-based scheme adapted in our scheme and illustrated in Fig. 2. Where it was shown that a PassPoints password is a number of points, selected by a user in an image that is displayed on the screen.

1.2. Merits and Demerits of Grid-Based Graphical Passwords:

- Grid of size NxN is a simple and ordered structure consisting of equal cells and each cell is denoted by two-dimensional discrete coordinates (x,y) which is a member of [1,N]x[1,N]
- Grid-based systems are recall-based algorithms, as such they rely on users’ memory to provide the passwords correctly, without any cue from any image if background image is not provided
- A user study conducted by revealed that it is difficult for users to draw their passwords with mouse or stylus in 2D grid coordinates and maintaining the sequence at the same time
- Perfect drawings with mouse or stylus without committing fuzzy boundary problem is difficult
- Identifying the starting point for some drawing may be hard

Figure 1. DAS Graphical scheme

Figure 2. Every pixel on an image used in the PassPoints system can be used for the password
Table. Illustrating summary of existing schemes

<table>
<thead>
<tr>
<th>Grid-based schemes</th>
<th>Image-based schemes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drawing-A-Secret (DAS), is the first of its kinds. It was developed by Jermyn in the year,1999 as a graphical passwords on grid background. In this system, passwords are pictures drawn on cell of a 5x5 grid and identified by their coordinates of the cells. Passdoodle algorithm was proposed by Christopher et al. (2004). The scheme was based on the idea of hand written designs or words, drawn with a pen onto a sensitive screen. Users are validated by tracing a doodle over a touch screen, which is then accepted or rejected by the system.</td>
<td>In 1996, Blonder pioneered the idea of graphical passwords scheme. In this scheme, the user clicks with a mouse or other device like stylus on a few chosen regions in a single image-based background that appears on the screen and a password is a number of clicks on these locations in a particular order. The scheme was limited to one pre-processed image. Dhamija and Perrig (2000) proposed Déjà Vu system for the purpose of user authentication based on Hash Visualization technique. Its design involved the use of random or non-describable abstract images, rather than photographs. In this scheme, the user selects a specific number of images from a larger set of images presented by a server. The user has to identify the pre-selected images for him or her to be authenticated. Passpoint is scheme that uses any kind of image provided by the user to use password from greater password space (256 bits for four faces in four different rounds. The use of dynamic grid transformations that distinguish it offered better security because users select random images that not related to them unlike human faces.</td>
</tr>
<tr>
<td>Pass-Go was motivated by an old Chinese game, Go. The scheme was proposed by Tao in 2006 as an improvement of the DAS. User selects intersections instead of cells on a 9x9 grid as in the case of DAS. The use of intersections as against cells allows the user to use password from greater password space (256 bits for the most basic scheme) and provides better usability than DAS.</td>
<td>“Passfaces” is a graphical password technique developed by Real User Corporation. In the scheme, the users are expected to choose just any four images of human faces from a face database as their future password. The user is authenticated if he/she correctly identifies the four faces in four different rounds.</td>
</tr>
<tr>
<td>Qualitative Draw-A-Secret (QDAS) was made by Lin et al. (2007) as an improvement of DAS to solve shoulder surfing (Tyagi et al., 2011). QDAS introduces qualitative spatial descriptions of strokes and the use of dynamic grid transformations that distinguish it from its DAS counterpart. With these features, users could set strong secrets that do not impose load on long-term memory and to be resistant to shoulder surfing.</td>
<td>Passlogix V-GO system is one of password schemes based on the Blonder’s technique developed by Passlogix and Microsoft in large scale. To create a password with V-GO, a user can click on a number of items in a single image in a particular sequence. Story scheme was proposed by (Davis et al., 2004) is an improvement over passfaces. In Story’s scheme, a user’s password is a sequence of k images selected by the user to make a story. The scheme offered better security because user select random images that not related to them unlike human faces.</td>
</tr>
</tbody>
</table>

1.3. Merits and Dismerits of Image-Based Graphical Passwords

- They are vulnerable to shoulder surfing attack when used in an open place
- The password space is almost infinity in DAS. The total number of possible passwords is larger than that of image-based systems

1.4. Proposed Scheme

To enhance graphical passwords, we have developed a system grid-image-based graphical password system. The system involves two 5x5 matrices which adapted from image and grid-based methods and the technique is aiming at enhancing the graphical authentication in terms of memorability and better security by reducing the possibility of occurrence of shoulder surfing problem. Our adaptation is influenced by taking the merits of both methods and larger password space and make a chosen password difficult to guess and observe
- Image-based graphical passwords require techniques for controlling the tolerance error in order to avoid mis-selected click points or passwords and to have an efficient system
- Every image has some regions that are more attractive than the others and user tend to click on such regions to form their passwords. Any image with too many attractive locations may cause hotspot, dictionary and targeted attacks

To enhance graphical passwords, we have developed a system grid-image-based graphical password system. The system involves two 5x5 matrices which adapted from image and grid-based methods and the technique is aiming at enhancing the graphical authentication in terms of memorability and better security by reducing the possibility of occurrence of shoulder surfing problem. Our adaptation is influenced by taking the merits of both methods and larger password space and make a chosen password difficult to guess and observe
- Image-based graphical passwords require techniques for controlling the tolerance error in order to avoid mis-selected click points or passwords and to have an efficient system
- Every image has some regions that are more attractive than the others and user tend to click on such regions to form their passwords. Any image with too many attractive locations may cause hotspot, dictionary and targeted attacks
possibility of enhancement. This new system involves two main steps, namely registration and authentication phases and each phase has activities that should be performed. In the first step, users are required to select one event from a list of ten everyday events which then appears over the grid. The event provides autobiographical memory (Adebola et al., 2013) which serves as a cue to see whether users can set more complicated passwords and to know whether the event helps user to remember them during authentication phase (Dunphy and Yan, 2007). The grid divides the image into $5 \times 5$, which is 25 parts where passwords are drawn. In the second step of this phase, users enter their username and click their passwords on the grid, then save the passwords to a MySQL database over an extended period of time. Figure 3 illustrates the activities during registration phase.

During the login process, the user will be presented with Fig. 4 from the database after entering the username correctly. The user enters any five cells corresponding to his/her passwords via on-screen pad without touching the screen to avoid shoulder surfing because the image in the grid and passwords are directly seen by anxious and malicious observers when they are being used. Figure 4 illustrates a user entering “24533163613” from the randomly generated digits as his password. The passwords selected must correspond to the selected cells highlighted in Fig. 4. Once that happens the login is successful otherwise the login is unsuccessful.

2. CONCLUSION

Today, good number of graphical password schemes are available but they have their advantages and limitations. In this study, we have conducted a comprehensive survey of existing password techniques in two main classifications to identify their strengths and weaknesses. From the study, we have proposed a graphical authentication system which is based on users day-to-day events to improve memorability of any chosen passwords on this system and reduce the users’ memory load. The present study is limited to system implementation while our future action plan is to conduct the system comparative evaluation and users satisfaction survey.

7. ACKNOWLEDGMENT

The researchers would like to express their appreciation to Universiti Teknologi Malaysia, (UTM) for providing enabling environment for research.

8. REFERENCES


