A New Hybrid Password Authentication System

Muhammad Irzan Nazri
Faculty of Information Science and Technology
Multimedia University
Melaka, Malaysia
muhammad.irzan.naz05@student.mmu.edu.my

Afizan Azman
Faculty of Information Science and Technology
Multimedia University
Melaka, Malaysia
afizan.azman@mmu.edu.my

Yean Li Ho
Faculty of Information Science and Technology
Multimedia University
Melaka, Malaysia
ylho@mmu.edu.my

Siong Hoe Lau
Faculty of Information Science and Technology
Multimedia University
Melaka, Malaysia
lau.siong.hoe@mmu.edu.my

Abstract—Most graphical password system only has one technique – they may be either recall-based or recognition-based graphical password systems. This password system offers the use of both techniques at once. By using a drag-and-drop picture password system that has been configured to record the order of the password, it combines both recall- and recognition-based password systems. A successful combination will enable users to register and authenticate themselves with this system.

Keywords-component; graphical password; recall-based password; recognition-based password

I. INTRODUCTION

Graphical password systems are systems where the password is presented in a graphical manner, be it pictures, graphs, figures or drawings. The systems can be largely split in two different techniques: recall-based and recognition-based passwords. Most of these systems use only one technique, therefore reducing the security of the graphical password system.

A. Problem Statement

Some people may have problems remembering normal text-based password; they may be forced to write it down just to remember it. Others may have trouble figuring out a good password, so they use a phrase they know and am familiar with. However, this can be circumvented with social engineering. Some systems have password policies in which passwords are required to meet a set of criteria such as a minimum number of passwords, use of capital letters, numbers and symbols, password expiry date and password history. This may lead to complex and hard to remember passwords.

This system is designed so that users do not need to remember texts and strings of characters. Instead, this system uses pictures as an authentication method. The human mind can remember pictures, patterns and graphics better than texts, a phenomenon known as the 'picture superiority effect' [1]. This system leverages that ability to make an authentication system that is safe and easy to use for the end user.

B. Project Objectives

There are two project objectives for this project: designing a new graphical password system which is a combination of recognition and recall password techniques and to code a working prototype of the authentication system. This serves to test the implementation and viability of this system in the real world as well as creating the ‘proof-of-concept’ for this project.

C. Project Scope

The scope of this project is to create an authentication system that is secure while being easy to use. The system is a webpage and has two parts: registration and authentication. Once the user is registered, he or she should be able to log into the system with ease.

II. LITERATURE REVIEW

In a paper by Suo, Zhu, & Owen [2], it summarized the difference between recall-based and recognition-based techniques as well as an analysis of the usability of graphical password system in general. Recognition-based technique relies on users to recognise a pattern displayed on the screen; this pattern can be user-defined or generated by the system as part of the authentication process. The implementation may vary between systems. Recall-based technique is another method of picture-based authentication method in which users must recall a series of actions that the user has configured into the system as part of the registration process.
A. Recognition-based Techniques

Dhamija & Perrig [3] proposed a system called Déjà vu where the user is asked to pick images from a larger set of pictures in order to authenticate the user. This system has a 90 percent success rate compared to 70 percent for normal text-based passwords and PINs. Weaknesses in the system include longer login times, the action of selecting pictures may take a longer time compared to normal text-based passwords and the reference that points to the images is saved in plain text. Akula & Devisetty [4] improved on the last point by using SHA-1 hash function instead of plain text. This has the advantage of being more secure and it is less resource-intensive.

Fraser [5] describes the most secure configuration of Tricerion’s SafeLogin system. Once the user has entered his or her username, the picture keypad will show up, displaying a series of pictures in the grid. The pictures are randomly generated but are tied to the username’s data such that the same set of pictures will be shown everytime the user logs into the system. The positions of the pictures in the grid are scrambled with each login. The pictures themselves have multiple variations of a core picture so that an attacker may not know the actual picture that the user is referring to.

Dunphy & Yan [6] wrote an analysis about the FacePIN, a system where the numbers on a grid is replaced with faces of various people. When the mask is applied on the top of the mock credit cards, the visible PINs are revealed to the user.

Wiedenback et al. [7] proposed a system called the Convex Hull Click Scheme (CHC). The order of the password is related to the shape of the area of the password, also known as the convex hull. When the user attempts to authenticate, the system will display a window filled with a large number of randomly generated and arranged icons. The user then needs to locate his or her passicons, mentally picture a convex hull and click on the area inside the convex hull which serves as the password. This process will be repeated with a new set of icons. The passicons (and the icons) may move in or out of the rotation so that it is harder for the attacker to guess what the passicons may be.

Davis, Monrose, & Reiter [8] wrote about the Story system, a system developed based on a variant of the Face system that is similar to the Passface scheme. By having a number of different themes for images, a user is expected to construct a “story” of the passwords, hence the name. For example, there may be multiple themes such as vehicles, faces and plants. When a user wants to be authenticated, he or she must pick the correct set of images from the themes provided.

B. Recall-based Techniques

Draw a Secret (DAS), a technique proposed by Jermyn et al. [9] is a system where the user draws a picture on a series of grids. The stroke sequence of the drawing is also recorded. If the system matches the drawing of the user to a recorded drawing in the database and the user draws it in the correct order, the user is then authenticated.

The article written by Lim, Ithnin, & Mammi [10] begins with a description of the Painting Album Mechanism, a mechanism that attempts to thwart shoulder surfing attacks by carrying out a series of actions on a picture or colour pattern that, when done correctly, authenticates the user. This involves three different input schemes: swipe (swipe on the picture), colour (touch or tap on coloured boxes displayed on the screen) and scot schemes (a combination of swipe and colour schemes in which users need to swipe on the picture and tap on coloured boxes). A user is expected to use multiple schemes and at least eight different pictures or coloured boxes or in combination of both.

The article written by Kimwlele, Mwangi, & Kimani [11] describes a method of authenticating a user by means of clicking or tapping multiple points on a picture displayed on the screen in sequential order. This concept is augmented by the design of the picture in which it should contain as many different colours as possible. Having different colours may lead to easier recollection of the click points by the end user. The end user can specify his or her own pictures, specify the tolerance of the click points and be able to specify the number of hit points needed to authenticate the user. Once all the points are entered in the correct position and order, the user is authenticated. Tolerance of the click points is important as it affects the security of the authentication process and it is proposed that the tolerance should have a diameter of two to five millimetres within the chosen click point. This provides a balance between accessibility and security.

Lin, Weng, & Huang [12] wrote about the Random Geometric Graphical Password (RGGPW), a recall based graphical password system that attempts to solve the problem of other recall based graphical password systems: guessing attack vulnerability due to the image used having too few distinguishing features and the inability of users to remember the password if the image used have too many features. By generating the image used in the system with custom parameters from the server and the user, the resulting images may have the property of having the right amount of features. Some of the parameters that can be changed are the colours and the shapes of the objects in the image. It should be noted that the images generated by the system is not used as a password by itself; rather, the images are used to help the users remember the password.

Lin et al. [13] proposed a variant of the Draw-a-Secret system called Qualitative Draw-a-Secret (QDAS). It uses a different way to encode the strokes. It takes into account the change of direction in the grid; a change of direction is defined when a stroke enters a grid is a different direction to the exit of the previous grid. QDAS employs a technique called dynamic grids instead of a fixed grid to perform the encoding process. When a user draws the password, the encoding process takes into account the starting grid and the
sequence of the change of direction. One of the benefits of this system is the large password space.

Chalkias, Alexiadis, & Stephanides [14] wrote about a variant of the Draw-a-Secret called Multi-Grid DAS. A research done by Nali & Thorpe [15] reveals that DAS is vulnerable to attacks if users use the DAS with passwords that are predominantly centred in the grid. In order to mitigate this attack, the authors of this paper made modifications to the DAS where the grids are not identical in size. Some grids may be larger or smaller than the ones in the series of grids.

Stubblefield & Simon [16] uses the Rorschach inkblot test to generate inkblots that can be used to create passwords. Instead of using pre-determined set of inkblots, this system uses an inkblot generator that can create inkblots based on various parameters. During the authentication process, the user is shown an inkblot. The user types the first and the last letter that he or she associates the inkblot with (e.g. if the user thinks the inkblot looks like a cat, the user types in C and T as in ‘cat’) and the system will render another inkblot in which the user is asked to type in the first and last word that they associate it with, again. This process is repeated until the end of the authentication process. If the user types the wrong character (therefore wrongly associating the inkblot) the authentication process is failed.

v-Go SSO is an enterprise single sign on system developed by Passlogix, now owned by Oracle. According to a product report by Allan [17] of Gartner and an article by Berry [18], it involves a series of pictures that can be grouped up under a common theme such as various types of beverages or card symbols that can be dragged and dropped into a field. The password is generated by the actions that were taken during the authentication process. Once the images have been filled correctly by the user, the password window will generate a key which is then used to decrypt the secure system.

C. Comparison of the Systems

This section has three tables that compare the systems discussed above on various metrics. Tables 1 and 2 compare the systems on their usability and security, respectively. Table 3 shows the systems being compared on their advantages and disadvantages.

<table>
<thead>
<tr>
<th>Systems</th>
<th>Authentication</th>
<th>Memorability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deja vu</td>
<td>Users pick and choose the correct series of pictures</td>
<td>Easy to remember if there are not too many pictures to be remembered</td>
</tr>
<tr>
<td>Draw-a-Secret</td>
<td>Users draw on a series of grids</td>
<td>Easy to remember if the pattern is simple, though that may not be secure</td>
</tr>
<tr>
<td>SafeLogin</td>
<td>Pictures on grid are shown, users will need to pick and choose the correct</td>
<td>High, though it may be confusing if a picture has multiple variants</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Systems</th>
<th>Password space</th>
<th>Possible attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deja vu</td>
<td>Brute force, social engineering</td>
<td></td>
</tr>
<tr>
<td>Draw-a-Secret</td>
<td>Brute force</td>
<td></td>
</tr>
<tr>
<td>SafeLogin</td>
<td>Brute force, shoulder surfing, spyware, social engineering</td>
<td></td>
</tr>
</tbody>
</table>
TABLE III. ADVANTAGES AND DISADVANTAGES COMPARISON TABLE

<table>
<thead>
<tr>
<th>Systems</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Déjà vu</td>
<td>Simple to use</td>
<td>May be susceptible to brute force attacks if the number of pictures are low</td>
</tr>
<tr>
<td>Draw-a-Secret</td>
<td>Uses the device’s peripheral to authenticate users</td>
<td>Users need to be precise with their drawings and strokes</td>
</tr>
<tr>
<td>SafeLogin</td>
<td>Users need to remember pictures, not numbers or alphabets</td>
<td>Users may have trouble differentiating the icons if it has many variants or subtle details</td>
</tr>
<tr>
<td>FacePIN</td>
<td>Similar to SafeLogin but with</td>
<td>Some people may have trouble remembering people’s faces</td>
</tr>
</tbody>
</table>

Convex Hull Click
- Depending on the number of iterations, the area of the convex hull and the randomisation of the icons
- Brute force, spyware

Story
- Brute force, social engineering, shoulder surfing

Painting Album Mechanism
- Has a bigger password space if more actions (swipe or touch) are performed
- Shoulder surfing, spyware

Kimwele, Mwangi, & Kimani [11]
- Bigger password space if there are many click points
- Brute force, shoulder surfing, spyware

Random Geometric Graphical Password
- Bigger password space if there are many click points
- Brute force, shoulder surfing, spyware

Qualitative Draw-a-Secret
- Large if there are a large amount of strokes
- Brute force

Multi-Grid DAS
- Large if there are a large amount of strokes and the pattern is drawn away from the centre
- Brute force

Stubblefield & Simon [16]
- More secure than normal text-based password since the system adds in an order of randomisation to the password creation
- Spyware, social engineering

v-Go password window
- Shoulder-surfing, social engineering

III. METHODOLOGY

The proposed system is derived from a combination of features from the works of Dhamija & Perrig [3] called Déjà vu, a recognition-based graphical password system that lets the users pick their picture passwords from a series of pictures and the works of Passlogix’s v-Go password window [17, 18]. The proposed system is a recall-based graphical password system that allows users to drag-and-drop pictures into the password field to create a password. Therefore, it combines the characteristics of both Déjà vu and v-Go password window.
Users are shown a grid in which users are allowed to put in pictures into the grid as the password. The pictures provided may have multiple themes like animals, automotive and plants and there will be multiple pictures associated with each theme. The pictures themselves are split in multiple parts. In order to authenticate themselves, users will need to put in parts of the pictures in the correct grid spot. For example, assuming that a particular authentication set-up has set a picture split in two parts and users are required to pick two pictures from two different themes, users need to put in four parts of the picture in the grid. This is shown in Fig. 1.

During the registration process, users are required to enter a unique username. After that, the user is asked to choose the pictures that they will use as the password. The user is then asked to drag and drop the pictures into the grid according to their preference. The order of the picture matter as it would be saved as well. A user does not need to fill up the entire grid with pictures.

When a user wants to be authenticated, a grid and a series of pictures sorted according to themes will be shown to the user. The user is required to drag and drop the multiple parts of the pictures that they have selected during the registration process into the correct spot of the grid. If the pictures are in the correct place on the grid and in the correct order, the user is successfully authenticated.

The split pictures offers yet another way for users to remember the picture passwords. By splitting the pictures in parts, one part of the picture may have more interesting features than the other part. The pictures may have something dominant in one part; therefore a user’s mind may be able to remember it more clearly. It is also a way to easily populate the available selection of the pictures for use as a picture password.

The system therefore offers both recognition-based and recall-based graphical password system. By picking pictures to be used as a graphical password, it satisfies the requirements for a recognition-based password while the drag-and-drop action required to authenticate the user (as the order of the picture password matter) can be considered as a form of recall-based password system.

IV. THE IMPLEMENTATION RESULTS

Fig. 2 shows the registration page. There’s a username field, a 6x5 grid destination grid where users can drag-and-drop pictures from the source grid, a pictures grid spread over two rows, a Register button and a message field. The picture grid has a horizontal scrolling bar which the user can select more pictures by scrolling the grid to the right. The pictures’ themes are sorted by row – row one contains pictures of living things such as animals and plants while the second row contains machines and mechanical cars such as aircrafts and cars. The pictures are split in two and can be moved independently of each other. The message field will notify users whether the registration is successful or not, when the username field is left blank and when a username has already been taken.

The login page is identical to the registration page. The only visible changes are the login button and the message field. The message field will notify the user if he or she is successfully authenticated.

For the calculation of the password space, assume the available pictures to be used as a password, the grid size and the password length. The formula is:

\[ a^{P(g, l)} \]

Assuming the system has minimal security requirement by the form of six pictures for use with a password length requirement of three pictures and a grid of three pictures by three pictures (3x3), the password space is \(1.54 \times 10^{392}\). On the other hand, if we go by the example system given in Fig. 2 with \(a = 24\), \(g = 30\) and \(l = 6\), the password space is \(10^{10^9}\).
V. CONCLUSION

The authors believe that the researches done for this report has proven that there are possibilities for another type of graphical password system using a combination of both recognition-based and recall-based graphical password methods. The system is hoped to be both easy to use and secure at the same time. The authors also hope that the project will be beneficial to the wider graphical password field.

REFERENCES