ENHANCING USABILITY AND SECURITY IN CLICK-BASED VISUAL PASSWORD SYSTEMS

Haider al-Khateeb, Carsten Maple and Marc Conrad

Institute for Research in Applicable Computing,
University of Bedfordshire, Luton, Bedfordshire, LU1 3JU, United Kingdom.

ABSTRACT

Security and usability are key elements in system design. A bad design might result in unnecessary inverse proportion between the two, while a good design must find a balance to achieve usable security. In this paper we present and discuss the results of a user study to show how good application of click-based systems can produce a system people can easily use while maintaining security.

In this study, participants were asked to do trials using 5 different prototypes of the system. A comparison between them helped to find the best criteria where there is an acceptable balance between security and usability. For instance, using a relatively small tolerance distance enhances security by increasing the password space, the comparison helps to find how small the distance can be while maintaining usability.

Another objective of this study was to distinguish between two types of images; the results revealed that using cartoon images have positive impact on usability. Nevertheless, hotspots occurred and that makes particular images more vulnerable to dictionary attacks. Experiments also show that, if they can chose, users select images more vulnerable to hotspots.

KEYWORDS

Click-based systems, HybridPass, visual passwords, cued recall, usable security, authentication.

1. INTRODUCTION

Due to their usability, text passwords are used for authentication on the vast majority of systems [1]. They consist of letters, digits and sometimes symbols to authenticate people and control access to resources. Despite having many advantages, previous studies revealed that text passwords have many drawbacks and limitations [2] [3] [4]. The main problem is that people often find it difficult to recall them, this lead users to create weak passwords which are the most common cause for system break-ins [5].

Visual solutions such as [6], [7] and [8]. have been suggested to replace the traditional text passwords. The advantage is that human can remember pictures better than words [9] [10], however, visual passwords implementations have been proven to be problematic. For instance, because users enter this kind of passwords visually on a screen, users might find it difficult to protect from shoulder surfing attacks, while with text password, they can use their hands to hide key strokes.

To combine the best of both solutions: text and visual passwords, HybridPass [11] was proposed to eliminate their drawbacks while used together and provide an additional level of security. In this paper we examine the usability and security of HybridPass approach based on a controlled user study.

The rest of the paper is organised as follows: Section 2 provides background information and more details about HybridPass. Section 3, introduce the methodology used in the user study. Section 4 presents the results of the experiment and Section 5 discuss these results in details. Finally, conclusions and future work are presented in Section 6.
2. BACKGROUND AND RELATED WORK

HybridPass [11] is a click-based cued recall system. In these systems users perform a sequence of clicks on a particular image whilst their mouse coordinates are captured.

The first application of a click-based systems was proposed by Blonder [12]. In Blonder’s scheme, users click on a predefined regions, this idea developed in PassPoints [7] to capture the click-points on a pixel level to increase the password space. Several lab studies were conducted afterwards such as [7], [13] and [14]. Recent example is Cued Click Points (CCP) [15]. To Sign in using this method, users make a single click on an image, the next image is uniquely based on the previous click-point. The authors suggested this technique to increase the number of used images to increase the workload for attackers in return.

In HybridPass approach, user authentication starts with entering a username and traditional text-based password, its text password needn’t be long or complicated. In fact any short memorable string would do. The text password is only an initial part of the final password. In addition, it protects the images. If the text password and username were valid, the correct set of images appears as small buttons beside a clickable area. When any button-image is clicked, the linked picture is loaded into the clickable area. Users may navigate through the set of images linked to their account to recall the click-points and make their visual password.

The hybrid nature of the system provides a solid built-in anti phishing technique. If a user was misguided by a phishing link to enter his credentials, after entering the initial password, the fake site will fail to provide the correct set of images linked to the user account. The user is then warned that the site is not legitimate.

3. EXPERIMENT METHODOLOGY

The user study had 40 participants who completed the experiment individually. To imitate the environment of a substantial internet application, it was implemented using PHP, JavaScript and SQL, and hosted online on a dedicated server. Participants to a great extent were university students and all were familiar with computers.

The screen resolution was predetermined to 1280 x 800 and HybridPass clickable area was 230 x 100 pixels. Passwords and click-points were not hashed in the database, so no discretization methods [16] [17] were used. This was necessary to keep clear record of all click-points.

Trials that every participant was asked to do consisted of profile creation, password confirmation and finally a sign in attempt. Users were first asked to enter a User ID, Text Password, Full Name and then still on the same page create their Visual Password. To create a visual password, there are four images randomly selected by the system to choose from. The system forced visual passwords of four clicks and didn’t allow continuous clicking on the same click-point.

After that users are asked to re-enter both text and visual passwords one more time. Registration is successful if the passwords matches, and consequently, the system forward users to Sign in. If any of the passwords did not match, users are asked to try registering one last time.

Sign in: to calculate the time required to input visual passwords, the sign in process has been divided into two phases. Users were first asked to enter their ID and Text Password (Figure 1), and then proceed to enter the corresponded visual password (Figure 2). If the passwords match the database records for that user ID, user is authenticated. After a successful registration, Users are asked to sign in, one time only.

Five system prototypes were used, identical code, but with different parameters. For example, two types of images were tested. First type was cartoon (drawing images) and the second type was photograph images (real life snapshots taken by camera). In addition, 4 and 6 pixels distance from the actual click-point were used. This implies that, if 4 pixels are permitted, and the original click-point is \((x, y)\) then \((x', y')\) is accepted if \(x' \geq x + 1\) and \(y' \geq y + 1\). And \(x' \geq x + 4\) and \(y' \geq y - 4\). Check Table 1 to see which parameters were used in which prototype.
Prototype 1 was used as a training stage and to study how users deal with the system for the first time, after that, prototypes 2, 3, 4 and 5 are accessed randomly to make the result comparison fair.

Table 1. Description of prototypes parameters (\( \delta \) is the tolerance distance from the actual click-point)

<table>
<thead>
<tr>
<th>Image type</th>
<th>Prototype 1</th>
<th>Prototype 2</th>
<th>Prototype 3</th>
<th>Prototype 4</th>
<th>Prototype 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mixed (cartoon + photographs)</td>
<td>4 pixels</td>
<td>4 pixels</td>
<td>4 pixels</td>
<td>6 pixels</td>
<td>6 pixels</td>
</tr>
<tr>
<td>Cartoon</td>
<td>4 pixels</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Photographs</td>
<td></td>
<td></td>
<td>4 pixels</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cartoons</td>
<td></td>
<td></td>
<td></td>
<td>6 pixels</td>
<td></td>
</tr>
<tr>
<td>Photographs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>6 pixels</td>
</tr>
</tbody>
</table>

4. RESULTS

Participants generated 2166 click-points on 15 background images. The number of successful trials was 165, which is the number of times participants were able to register and then try to sign in to the system.

4.1 Prototype 1 (First Time Users)

Registration time was reduced to less than the half with those who had to try for the second time. For more details refer to Table 2. The minimum time recorded decreased as well, moreover the number of users who finished their registration in less than one minute raised from 10% on the first trial to 65% on the second one.

Table 2. Prototype 1 registration time

<table>
<thead>
<tr>
<th></th>
<th>Registration (first trial)</th>
<th>Registration (second trial)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Create</td>
<td>Confirm</td>
</tr>
<tr>
<td>Mean time</td>
<td>00:02:34</td>
<td>00:00:30</td>
</tr>
<tr>
<td>Median time</td>
<td>00:02:14</td>
<td>00:00:28</td>
</tr>
<tr>
<td>Minimum time</td>
<td>00:00:50</td>
<td>00:00:11</td>
</tr>
</tbody>
</table>

42.2% only were able to register successfully, 15% on the first trial and 27.5% on the second trial. This does not reflect a problem with HybridPass usability, because users were left alone and asked to create accounts without any help other than the system interface simple guidelines. Sign in times were counted for those who successfully signed in only. Check Table 3 for the results.

Table 3. Text and visual passwords entry time while signing in to the system using Prototype 1

<table>
<thead>
<tr>
<th></th>
<th>Text password + Username</th>
<th>Visual password</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mean time</td>
<td>00:00:15</td>
<td>00:00:19</td>
</tr>
</tbody>
</table>
4.2 Image Type

Both cartoon and photographs were chosen carefully to be used in HybridPass, but because the colours in cartoon images are more contrasted and clean in the sense the details are clear, a question to answer was if they are a better choice for click-based systems. The result in this study approved this assumption as showed in Table 4 and Table 5.

Prototype 2 and 3 are identical except for the type of images used, however prototype 2 shows better success rates. The same result repeated itself again with prototype 4 and 5 for the benefit of prototype 4 where cartoon images were used. Time record comparison showed an average of 5 seconds change in the creation stage for the benefit of cartoon images between prototype 1 and 2 where the click square is small (9x9) but the change was not effective with the bigger click-square (13x13) between prototypes 4 and 5.

<table>
<thead>
<tr>
<th></th>
<th>Create</th>
<th>Confirm</th>
<th>Create</th>
<th>Confirm</th>
<th>Create</th>
<th>Confirm</th>
<th>Create</th>
<th>Confirm</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mean time</strong></td>
<td>00:00:55</td>
<td>00:00:25</td>
<td>00:00:50</td>
<td>00:00:24</td>
<td>00:00:48</td>
<td>00:00:24</td>
<td>00:00:47</td>
<td>00:00:24</td>
</tr>
<tr>
<td><strong>Median time</strong></td>
<td>00:00:46</td>
<td>00:00:23</td>
<td>00:00:47</td>
<td>00:00:23</td>
<td>00:00:43</td>
<td>00:00:21</td>
<td>00:00:40</td>
<td>00:00:22</td>
</tr>
<tr>
<td><strong>Minimum time</strong></td>
<td>00:00:21</td>
<td>00:00:13</td>
<td>00:00:24</td>
<td>00:00:11</td>
<td>00:00:19</td>
<td>00:00:11</td>
<td>00:00:21</td>
<td>00:00:11</td>
</tr>
</tbody>
</table>

Success rates

<table>
<thead>
<tr>
<th></th>
<th>Prototype 2</th>
<th>Prototype 3</th>
<th>Prototype 4</th>
<th>Prototype 5</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mean time</strong></td>
<td>00:00:19</td>
<td>00:00:19</td>
<td>00:00:19</td>
<td>00:00:18</td>
</tr>
<tr>
<td><strong>Median time</strong></td>
<td>00:00:19</td>
<td>00:00:17</td>
<td>00:00:16</td>
<td>00:00:17</td>
</tr>
<tr>
<td><strong>Minimum time</strong></td>
<td>00:00:08</td>
<td>00:00:09</td>
<td>00:00:08</td>
<td>00:00:09</td>
</tr>
<tr>
<td><strong>Success rates</strong></td>
<td>81%</td>
<td>80%</td>
<td>94.8%</td>
<td>86.4%</td>
</tr>
</tbody>
</table>

In Table 4, Success rates are for those who successfully registered weather that happened on the first or second trail. Timing in Table 5 was calculated for users who successfully signed in only.

4.3 Tolerance Distance

Using six pixels tolerance distance (13x13 click-square) had an obvious positive impact on the usability of the system. Success rates increased 5% between prototypes 2 and 4 and between 3 and 5. In the sign in process, success rates elevated from 81% in prototype 2 to 94.8% in prototype 4. Something similar happened between prototypes 3 and 5.

Time record comparison in the creation stage pointed to a prominent change for the benefit of the bigger tolerance distance in prototypes 4 and 5.

In conclusion, the results indicate that a 6 pixels tolerance distance is fairly usable in practise.

4.4 Success Rates and Time

Success rates with the best criteria that is prototype 4 are 97.5% for registration and 94.8% for sign in. These are good rates considering other click-based systems, for instance, in CCP user study [15] only 83% of their users were able to create and confirm their accounts and then 96% signed in successfully.

Users spent 43 to 48 seconds to create an account and 21 to 24 seconds to confirm their passwords, thus full registration would take between 64 and 72 seconds. Considering the minimum recorded values, full registration is possible within 30 second. To sign in, users spent 16 to 19 seconds to enter the visual password.
as most of them were pausing to comment and ask questions while entering their passwords, however some users needed 8 seconds only, this results is very close to the sign in time in CCP user study.

4.5 Hotspots

In click-based systems, hotspots are areas that comprise most user clicks. If users were not interrupted by the system to select a good password, then, there is a high probability that most users unconsciously select them. This particularly implies that attackers can do image analyses to locate hotspots and run effective dictionary attacks on click-based systems. Previous researches like [18] [15] [19] addressed this problem.

Similarly, this study approves that most clicks are contained within hotspots, every image has a unique hotspots map. Figure 3 illustrates clicks on the most employed cartoon image in prototypes 2 and 4. It shows clusters of clicks in some areas, less clicks in other areas and absolutely no click on the rest.

Figure 3. Scatter chart illustrating 83 clicks on the most employed cartoon image in prototypes 2 and 4.

Furthermore, an interesting result was that users tended to unconsciously favour images which are more vulnerable to hotspot analyse. Previous implementations forced images, but since our approach gave users a choice, this behaviour was observed. People chose what is clear and easy to remember, since they didn’t have experience on click-based systems security, they created weak visual passwords.

This study collected the necessary data to focus on hotspots, other security concerns like shoulder surfing, and other attacks were covered in [11] and are considered out of scope.

5. DISCUSSION

As expected, new users took more time to register, prototype 1 showed how time was diminished on the second trial and then with the consequent prototypes.

The best recorded time for entering a visual password in HybridPass was 8 seconds, which is 1 second more than the best recorded time for entering a text password and username using the same environment. Considering the difference between the Mean values that is 1 second again, while the Median is 4, the required time to enter a visual password in the system is nearly the same as entering a traditional text password and username under the same circumstances. However, while text password can be entered directly into one filed on any internet page, HybridPass interface for visual passwords is more interactive because users may navigate to display images in the clickable area, hence if an image failed to load properly due to a connection problem, users should reload the image and some might reload the whole page. This possible scenario could waste time in online visual solutions.

Registration and sign in success rates revealed positive impact while using cartoon images and increased usability. But, this did not have significant impact on the registration and sign in times.

Users located their entered visual passwords easier when the tolerance distance was big, but increasing tolerance decrease the number of possible clicks in the system. The objective behind testing relatively small tolerance in the experiment was to identify a usable yet security convenient distance. Good pass rates were achieved with 6 pixels, which approves similar result reported in [13].

Figure 4. Scatter chart illustrating 87 clicks on the most employed photograph image in prototypes 3 and 5.
6. CONCLUSION AND FUTURE WORK

Visual passwords usability problems can be eliminated without affecting the security by way of better applications. This paper showed how the time required to enter visual passwords was minimized to be nearly the same as the time needed in text password systems, while previous studies like [20] found visual passwords to be time consuming. Nevertheless, PassPoints used 20x20 tolerance square (9.5 pixels of tolerance), but we showed how tolerance of 6 pixels achieved a convenient registration success rate of 97%.

Considering the hotspots problem as a serious vulnerability in click-based systems, future work of this ongoing research will focus on developing methods to eliminate hotspots effect. It is a main problem for click-based systems and more research should be done in this area.

REFERENCES