Accessibility and Graphical Passwords [*]

Sonia Chiasson[1,2], Alain Forget[1,2], Robert Biddle[2]
[1]School of Computer Science & [2]Human Oriented Technology Lab
Carleton University, Ottawa, Canada
{chiasson, aforget}@scs.carleton.ca, robert_biddle@carleton.ca

ABSTRACT

In this brief paper, we explore the issue of accessible authentication with respect to click-based graphical passwords. These schemes normally rely on complex visual presentation and fine motor control for pointing. We take the approach of identifying the semantic structure, and show how the same kind of scheme could work with alternative interaction modalities. In particular, we explore the use of audio passwords that work similarly to click-based graphical passwords, and report on a simple informal study of their characteristics. We conclude that modality independent authentication is a reasonable concept, but that great care is needed because the modalities employed in implementation will affect both usability and security.

Categories and Subject Descriptors

K.6.5 [**Management of computing and information systems**]: Security and protection: Authentication; K.4.2 [**Computers and society**]: Social issues: Assistive technologies for persons with disabilities

General Terms

Security, Human Factors, Experimentation

Keywords

Accessibility, authentication, usable security

1. INTRODUCTION

Much work has been focused on usable authentication in recent years since traditional text passwords have both usability and security issues. One general approach is the use of graphical passwords [5, 6]. By relying on the human ability to remember and recognize images, more usable and secure password schemes may be possible.

Click-based graphical passwords rely on vision in order to recognize and pinpoint the exact location of click-points. They also rely on fine motor control to target the click-points within the acceptable margin of error. These characteristics render click-based graphical passwords inaccessible or difficult for some user populations.

In previous work on accessible authentication, a key idea has been to examine the structure of an established authentication method, and to design a new method with a similar structure, but without dependencies on particular modalities of communication [8]. This approach can be seen as following a basic principle of accessibility in user interface design: separating semantic content from the modality of presentation, and then allowing different modalities to be linked with the same semantics. For example, using the CSS (cascading style sheets) in web site design.

In this brief paper, we explore whether the structure of click-based graphical passwords suggests opportunities for improving accessibility.

2. SEMANTIC STRUCTURE

Our recent work has focused on click-based graphical passwords, where a password consists of a sequence of user-chosen click-points on one image or on a sequence of images. With PassPoints [9], users select five click-points on a given image and must re-enter these points in the same order and with acceptable accuracy to successfully log in. Cued Click-Points (CCP) [2] operates in the same way except each click-point is on a different image and the next image displayed is based on the current click-point. A third system, Persuasive Cued Click-Points (PCCP) [3] helps users during password selection so that they select more random passwords.

During usability testing, we found that subtle interface modifications, such as those differentiating these three click-based graphical password schemes, could have significant usability and security consequences. For example, when required to select five click-points on one image, users tend to choose similar click-points, forming hotspots across users, but when offered some guidance during password selection, as in PCCP, such hotspots were much less likely to occur.

All these variants relied on the same modalities: visual pre-

This work was presented at the Symposium On Accessible Privacy and Security (SOAPS), July 2008

sentation as output and fine motor control of a pointing device as input. They all offer a cued-recall scenario. Users are presented with an image which should help trigger the memory of where their click-point is located. In response, users select their click-points by accurately targeting them with a mouse-click.

This articulation suggests that the structure may also be seen at a more abstract level. In every case, the visual presentation is a cue that is rich in semantic detail and allows identification of small elements. Similarly, the fine motor control input is used to select those small elements. So this is the essential structure of click-based graphical password systems: presentation of a cue rich in identifiable details, and user selection of some of those details.

3. ALTERNATIVE MODALITIES

Having determined the essential structure of click-based graphical password systems, we now consider the use of alternative modalities within the same structure. There are two sides to consider, the presentation, and the selection. We propose that for presentation, we consider a modality different to visual display, and for selection, we consider a modality different to pointing.

For the presentation modality, what we need is something with rich complexity that permits identification of details. In the graphical scheme, we present a picture. As an alternative, the system might for example play an audio sequence, such as piece of music. Like a picture, the music would be rich in semantic detail, which would be a strong source of cues to the user. Moreover, audio also comprises many small detail features that can be identified by a user. For example, an audio sequence is presented over a duration of time, and particular points in time associated with audio elements could be identified by the user.

For the selection modality, what we need is the ability to specify detail elements of the presentation. In the graphical scheme, the user uses a pointing device, such as a mouse, to click on parts of the picture. As an alternative, if we have chosen audio as the presentation modality, and wish to distinguish points in the time-line of the audio, the user could listen to the audio, and select time-points using a simple keystroke or mouse-click.

Together, these two alternative modalities replicate the structure of a click-based graphical password system, but without the need to use either visual display or fine motor control for pointing. In the graphical scheme, the authentication system consists of the user inspecting a picture, choosing points, and then later logging in by clicking those points. In the audio alternative, the system consists of the user listening to an audio sequence, choosing times, and then later logging in by clicking at those times.

3.1 Security and Usability

In assessing this alternative, we should consider both security and usability. In this brief exploration, we will discuss only some immediate issues. The security of the system will involve the size of the possible password space. In a graphical system such as PassPoints, this is determined by the image size, the size of a tolerance region for selecting points, and the number of points. For example, PassPoints has an image size of 451x331 pixels, a tolerance region of 19x19, and 5 click points. This suggests a password space of 1.2×10^{13} or 43 bits.

To consider the security of our audio alternative, we need to suggest the duration of the audio sequence, the time tolerance for selection, and the number of time points. To explore this, we built a crude prototype system, and ran a number of tests with ourselves as users. We do not argue this is a reliable range, but it gave us a place to start. After exploring a number of shorter and longer duration clips, we decided that a duration of about 30 seconds was tolerable. We then tried to determine how accurate we could be in selecting time points. Human ability to repeat actions in time synchrony is very good. For example, musicians can perform in synchronous collaboration with either recorded music or other musicians. For example, in performance, synchronization can be done to the Quaver (Eighth note), which at 120 BPM (beats per minute) is 250 milliseconds. If we took this as a tolerance, 30 seconds as a duration, and 5 time points, this would suggest a password space of 1.9×10^8, or 28 bits. This is not great, but our experiments showed a tolerance of 250 milliseconds was far too small for us. In fact, we had difficultly with tolerances of anything below 1 second, suggesting a password space of 1.4×10^5 or only 17 bits. Of course we could increase the number of points required, but this would have little effect, especially with the audio duration so short.

3.2 Hotspots

With click-based graphical passwords such as PassPoints, although the theoretical password space is large, studies by us and our colleagues have shown that the effective password space is much smaller because of “hotspots”, places is the pictures that are selected by many people [2, 7]. Our simple experiment with our audio approach suggested that similar problems would be likely to occur. In particular, we ourselves found that in order to select memorable time points in the audio sequence, we followed common patterns. In particular, where the audio sequence was music, we would choose time points related to lyrics, typically on a downbeat. This suggests that the system would be even less secure than we discuss above, because this would significantly reduce the size of the effective password space. In our work on improving click-based graphical passwords, we found we could diminish hotspots by using a different picture for each click, and making suggestions as to where to click. We could explore whether these approaches might also apply to our audio scheme.

This all suggests that although there was an identifiable structure to the click-based graphical password approach, and although we could identify alternative modalities, the security and usability of the system combine to suggest the alternative scheme we propose would need considerable refinement. In particular, we might consider different ways of identifying detail in the audio sequence, as the linearity of the time together with selection simply by time points is the main source of restriction. Alternatively, we might consider alternatives to audio, such as haptics, although the hardware support will be far less common.

4. CONCLUSION AND FUTURE WORK

In this brief paper, we have considered the nature of click-based graphical passwords, and how they might be adapted for greater accessibility. We took the approach of separating content from form, common in designing for accessibility in user interfaces. We first identified the essential semantic of graphical passwords as consisting of a presentation step, followed by a selection step. We then showed how alternative modalities could be used for each of these, and explored the consequences for security and usability. Our findings suggest that the general approach does show promise, in that authentication methods might be designed and analysed independently from any particular modalities used in implementation. This further suggests that we might be able to design an authentication framework where users may select modalities suitable to their particular circumstances. As our simple study showed, however, there are security and usability implications that vary with the modalities, and these will also have to be developed and studied with care.

5. REFERENCES

[1] Chiasson, S., Biddle, R., and van Oorschot, P.C. A Second Look at the Usability of Click-Based Graphical Passwords. ACM SOUPS 2007, 1-12.

[2] Chiasson, S., van Oorschot, P.C., and Biddle, R. Graphical Password Authentication Using Cued Click-points. ESORICS 2007.

[3] Chiasson, S., Forget, A., Biddle, R., and van Oorschot, P.C. Influencing Users Towards Better Passwords: Persuasive Cued Click-Points. ACM British HCI 2008.

[4] Cranor, L.F. and Garfinkel, S. (eds.) Security and Usability: Designing Secure Systems that People Can Use. O'Reilley Media Inc. Sebastopol, CA. 2005.

[5] Monrose, F. and Reiter, M. Graphical Passwords. Chapter 9 in [4].

[6] Suo, X., Zhu, Y., and Owen, G.S. Graphical Passwords: A Survey. ACSAC 2005.

[7] Thorpe, J. and van Oorschot, P.C. Human-Seeded Attacks and Exploiting Hot-Spots in Graphical Passwords. USENIX Security Symposium 2007.

[8] Topkara, U., Topkara, M., Atallah, M. K. Passwords for Everyone: Secure Mnemonic-based Accessible Authentication. USENIX Annual Technical Conference 2007.

[9] Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A., and Memon, N. PassPoints: Design and longitudinal evaluation of a graphical password system. International Journal of Human-Computer Studies 63, 102-127, 2005.