Opening the Web for all

Enhancing digital inclusion through authentication system design

Marcia Gibson
Institute for Research in Applicable Computing
University of Bedfordshire, Park Square, Luton, UK
marcia.gibson@beds.ac.uk

1. MY RESEARCH

During a MRes degree in computer security (completed in 2007), I became very interested and passionate about usable authentication. This led me to write a successful application to fund my current PhD. The principal aim of my project is to enhance the prospect of online inclusion for members of society who find authentication using established techniques difficult. This may be due to economic, physical, cognitive or skills related impairments. A review of the literature instructs that the development of an authentication technique that is accessible, usable, secure and low-cost would make a positive difference to the prospect of inclusion for these groups [4]. My research is focused on the development and evaluation of a system to fulfill these aims.

1.1 Background

The most widely deployed method of establishing the validity of an individual’s claim of eligibility to access a file, site or service online is to test their knowledge of a secret key - the familiar alphanumeric password.

The inherent problems of the password have led to a concerted effort to develop better alternatives. One approach involves the use of images to generate password keys. Depending upon implementation, when forming an image based password the user will select a number of images from a larger challenge set; select a number of coordinates within an image or sequence of images; or draw a picture or otherwise create a ‘path’ of actions through a visual interface. With the exception of path-based schemes wherein the user creates an image to authenticate him or herself, the images presented to the user at authentication provide additional and memorable cues to trigger recognition or cued-recall of the key - reducing the burden placed on the user. An added bonus is that these systems can usually be operated using the keyboard or via the point and click of a mouse.

In their many guises, image based passwords might offer a feasible solution to increased usability and security, but what of their accessibility? They certainly cannot be used by those who are blind and are likely to pose difficulties for the partially sighted user. They also cannot be used in situations where a GUI is not available, such as when accessibility is sought over the telephone (an important technology in reducing the divide [2]).

In terms of accessibility, I have been led to conclude that it is necessary to provide, alongside any image based scheme, a number of equivalent systems each offering a different al-


words. Such limitations include: dyslexia, which can result in unpredictable spelling; dyspraxia, which can lead to difficulties sequencing numbers and letters; and developmental or other language difficulties (especially in younger users). In addition to this, older users often find it difficult to retain newly learned information and users who are illiterate or who normally use a different alphabet can find password entry challenging [5]. To ensure that these users are not excluded from the benefits that the Web has to offer, we must absolutely ensure that they too are supported to log in.

1.2 Password alternatives

The inherent problems of the password have led to a concerted effort to develop better alternatives. One approach involves the use of images to generate password keys. Depending upon implementation, when forming an image based password the user will select a number of images from a larger challenge set; select a number of coordinates within an image or sequence of images; or draw a picture or otherwise create a ‘path’ of actions through a visual interface. With the exception of path-based schemes wherein the user creates an image to authenticate him or herself, the images presented to the user at authentication provide additional and memorable cues to trigger recognition or cued-recall of the key - reducing the burden placed on the user. An added bonus is that these systems can usually be operated using the keyboard or via the point and click of a mouse.

Due to the very large password space that can be achieved using soft, as opposed to hard-ware alphabets, these systems can be shown (in theory) to offer enhanced security compared to an equivalent alphanumeric password against a number of well-known attacks including, phishing, pharming, replay, dictionary and offline brute force - an optimized authentication system design co-developed by myself to achieve this is presented in [3].

1.3 Accessibility and Inclusion

In their many guises, image based passwords might offer a feasible solution to increased usability and security, but what of their accessibility? They certainly cannot be used by those who are blind and are likely to pose difficulties for the partially sighted user. They also cannot be used in situations where a GUI is not available, such as when authentication is sought over the telephone (an important technology in reducing the divide [2]).
Finally, a EuroSOUPS (or even worldwide SOUPS) wiki could act as a useful focal point for conference organisation. I am of the opinion that it might help to keep people interested in the conference if they can easily see and become involved with its development. The wiki could also contain other areas for members to share resources and experiences or to promote local events of interest. It might also be used to advertise employment and funding opportunities and as a forum to discuss usable privacy and security topics.

3. REFERENCES


