

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 level of security a password string offers against statistical and brute-force attacks depends upon the degree of entropy [10] (i.e. randomness, lack of predictability) it contains. However, it is widely acknowledged that passwords constructed of random letters, digits, and special characters can be difficult to recall [13]. For this reason, naïvely selected passwords are often based on meaningful objects or concepts [1], or contain otherwise predictable patterns. This assists imprinting [7] of the password, as well as its subsequent recall from memory.

In an attempt to ensure a minimum level of entropy is achieved, security professionals often advocate password construction policies that revert them back to their prior arbitrary and difficult to recall formats. This leads the user to behave insecurely, writing passwords down or sharing them over a number of accounts. On the Web, these issues become exacerbated due to the large number of sites requiring account registration, and because the neural pathways through which memories are accessed deteriorate without frequent use [9] and many Web sites are accessed *in*-frequently.

It is also difficult to design authentication systems that help the user avoid errors, or support them to recover when they do. This is because any error might indicate an attempt to break in to the system.

These problems are serious indeed, but users experiencing cognitive or physical impairments tend to experience usability issues on the Web more severely than others [8] and there are a range of disabilities that impact the use of pass-

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]).

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-

phabet modality for the user to choose from. Alternatives proposed in the literature include: haptic [6], thought [11] and rhythm based [12] authentication. As well as the author's own prototype system, "Musipass" which utilizes our abilities of music clip recognition [5].

Although it is possible to provide "practically" accessible authentication in this manner, it is currently not possible to provide a system which can be "certified" accessible via this strategy in terms of the current W3C accessibility guidelines. These were not written with alternative authentication in mind. The result is that they require significant "tweaking" if this solution is to be made viable, as they focus on the terminology of "text equivalency" which I find undermines the security of alternate modality schemes. Further, text-equivalency in this manner should be unnecessary, as long as a comprehensive combination of modalities is provided [4]. It is my opinion that in the future, this fundamental incompatibility (which is reminiscent of the tension between usability and security aspects), will contribute to a reduction in take up of these potentially enabling technologies, in particular from the very organisations that would show their dedication to online inclusion by following the W3C recommendations.

2. EUROSOUPS

Although I adore reading the proceedings of SOUPS each year, I always feel a little sour that budget restrictions make it unlikely I would be able to attend. When I initially heard a EuroSOUPS conference was being planned I was (and still am) very enthused. Although I am early on in my research career and have limited experience of what conference organisation involves, I do have some ideas about what I would like to see and I'd be very happy to roll up my sleeves and learn!

In terms of suggestions, I think in order to provide a mutually beneficial period of time for the findings from the two conferences to filter through into one-another, a ~6 month time interval should go between the two. As SOUPS happens in July, EuroSOUPS should therefore take place in December or January. How practical (or popular) this idea will be, might depend upon the timetables of other conferences and the academic obligations of participants. Another option might be to hold both conferences in conjunction, however it is my feeling that at least initially, it would be best to avoid this. Some researchers might like to attend both conferences and going "head to head" with the older, more renowned SOUPS conference might result in a lower quality of submission to EuroSOUPS.

Secondly, it might be useful (and enjoyable) to alternate the conference venues between different geographical regions. Perhaps a pattern such as, Western Europe, followed by Central and then Eastern areas might be good. This should help to ensure researchers in the various geographical locations have the same opportunities to participate, helping to foster a sense of ownership and community. It should also stop the conference becoming too stagnated and insular. A further point relating to the European focus of the conference might be to include in the paper call, the option to submit discursive articles on the many cultural, legislative and historical differences in privacy and security policy, technologies and attitudes between the various countries of Europe and the rest of the world.

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

- [1] S. Brostoff and M. A. Sasse. Are passfaces more usable than passwords? a field trial investigation. In S. McDonald, editor, *People and Computers XIV - Usability or Else! Proceedings of HCI 2000*, pages 405–424. Springer, 2000.
- [2] N. Geach. The digital divide, financial exclusion and mobile phone technology: Two problems, one solution? *Journal of International Trade Law and Policy*, 6(1):21–29, 2007.
- [3] M. Gibson, M. Conrad, and C. Maple. Infinite alphabet passwords: A unified model for a class of authentication systems. In *SECRYPT10: International Conference on Security and Cryptography*, Athens, Greece, 26–28 July 2010.
- [4] M. Gibson, M. Conrad, C. Maple, and K. Renaud. Accessible and secure? design constraints on image and sound based passwords. In *International Conference on Information Society (I-Society)*, London, United Kingdom, June 28–30 2010. (in press).
- [5] M. Gibson, K. Renaud, M. Conrad, and C. Maple. Musipass: authenticating me softly with "my" song. In *NSPW '09: Proceedings of the 2009 workshop on New security paradigms*, pages 85–100, 2009.
- [6] R. Kuber and W. Yu. Authentication using tactile feedback. In *HCI Engage 2006, Interactive experiences*, 2006.
- [7] A. Paivio. *The Empirical Case for Dual Coding. In Imagery, Memory and Cognition: Essays in Honour of Allan Paivio*. 307–322. Erlbaum, Hillsdale, NJ, 1983.
- [8] H. Petrie and O. Kheir. The relationship between accessibility and usability of websites. In *CHI '07: Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 397–406, New York, NY, USA, 2007. ACM.
- [9] R. Sapolsky. Stressed out memories. *Scientific American Mind*, 14(5):28, 2005.
- [10] C. Shannon. A mathematical theory of communication. *The Bell System Technical Journal*, 27:379–423, July and October 1948.
- [11] J. Thorpe, P. Van Oorschott, and A. Somayaji. Pass-thoughts: Authenticating with our minds. In *NSPW '05: Proceedings of the 2005 workshop on New security paradigms*, pages 45–46. ACM, 2005.
- [12] J. O. Wobbrock. Tapsongs: tapping rhythm-based passwords on a single binary sensor. In *UIST '09: Proceedings of the 22nd annual ACM symposium on User interface software and technology*, pages 93–96, 2009.
- [13] J. Yan, A. Blackwell, R. Anderson, and A. Grant. Password memorability and security: Empirical results. *IEEE Security and Privacy*, 2(5):25–31, 2004.