Challenges in Universally Usable Privacy and Security

Harry Hochheiser, Jinjuan Feng, and Jonathan Lazar
Department of Computer and Information Sciences, Towson University
8000 York Road
Towson, MD 21252
{hhochheiser,jfeng,jlazar}@towson.edu

ABSTRACT
Accessibility concerns compound the already-considerable difficulties of building systems that provide usable privacy and security. In addition to facing common concerns regarding the semantics of privacy and security tools, people with disabilities face accessibility obstacles, such as the inaccessibility of CAPTCHAs, phishing toolbars, verification images, and other displays that rely upon visual presentation of security and privacy-related information. An analysis of the security and privacy challenges facing users with disabilities can serve as the basis for a research agenda.

Categories and Subject Descriptors
K.4.2 [**Computers and Society**]: Social issues - *Assistive technologies for persons with disabilities* H.5.2 [**Information Interfaces and Presentation**]: User Interfaces - *Auditory (non-speech) feedback, Graphical user interfaces (GUI), Theory and methods, User-centered design*

General Terms
Design, Security, Human Factors, Standardization

Keywords
Universal Usability, Accessibility, CAPTCHAs

1. INTRODUCTION
Much of the difficulty in usable privacy and security can be attributed to the unusual characteristics of the perceptual, cognitive, and mechanical challenges involved in using these interfaces. Where most interfaces are ideally designed to support completion of a task, privacy and security tools are often one-step away from, if not directly in opposition to, immediate user goals. Interfaces that provide information in support of a task ("https" and security indicators), increase security without otherwise adding to the completion of the main goal (email encryption), and/or simply make tasks harder to complete (authentication systems including passwords and CAPTCHAs) all demand that see more, learn more, and do more. These challenges are magnified for individuals with perceptual, cognitive, or physical disabilities that may interfere with their ability to perceive subtle changes in state, interpret feedback, and execute appropriate input sequences in response.

Recent work in usable privacy and security presents a conundrum that illustrates the need for privacy and security tools that are both accessible and usable. Recent proposals for new password mechanisms [29] [21] [12] [18] [11], anti-phishing indicators [9], and security-related dialogs [1] rely heavily on visual displays, continuous control input (mouse or eye-gaze), cognitively-challenging text, and other elements that raise substantial accessibility barriers. These efforts stand in sharp contrast with evaluations that have questioned the efficacy of visual indicators, graphical passwords and complex interfaces [10] [5] [24] [31].

The usable privacy and security community is aware of these difficulties. Accommodations such as audio CAPTCHAs provide encouraging initial support for accessibility. However, the establishment of essentially parallel, but separate, mechanisms is costly. Universally usable [26] security and privacy systems present the potential for combining accessibility and usability, to the benefit of all users.

2. Accessible Privacy and Security Concerns
2.1 Anti-Phishing Tools
Phishing attacks attempt to convince users that a fake, malicious site is in fact a legitimate site. Identifying a phishing site often requires careful examination of both site content and various cues that may be available in the browser, including the address bar, protocol indicators ("https"), status bar security lock icons, and information about site certificates. Some of these elements are completely inaccessible: the popular JAWS screen reader [14], will read the protocol indicator from a URL, but it does not provide any audio feedback regarding the state of the padlock icon. Evaluation of this information presents significant challenges even to those who are not hindered by accessibility roadblocks: many users may not be aware of phishing concerns, while others may be challenged by difficulties in interpreting padlock icons, secure protocol indicators, and site certificates[10].

Numerous anti-phishing tools have been proposed and deployed in the hopes of helping users distinguish between legitimate and spoofed sites. Many banking websites have deployed verification images, which ask users to verify that an image presented on a login screen is the same image that they selected during earlier registration with a site [24]. Anti-phishing tools

Symposium On Usable Privacy and Security (SOUPS) 2008, July 23-25, 2008, Pittsburgh, PA, USA.

at the browser level include both built-in features and add-on toolbars or other extensions [9] [32] [31].

Many of these approaches present accessibility concerns. Although verification images might be accompanied by ALT tags describing the content of the image, this information might be susceptible to exploitation by sophisticated phishing attacks. Browser-based anti-phishing tools often involve text that may not be presented by screen reader software. The use of color-coding is widespread , raising concerns for users with color-blindness [32]. Other tools have used alternative, but still inaccessible visual techniques, such as changing page backgrounds [32] [9].

Current anti-phishing tools have not fared well in empirical studies. Studies have shown that anti-phishing tools often fail to influence user behavior, largely because users don't pay attention to them [31] [10] [24]. One study found popup dialog boxes to be more effective than warnings displayed in toolbars, but this approach is not without its limitations, as users may pay less attention to dialogs after repeated presentation [31] [1]. Many users, especially blind users, have their browser set to block pop-up windows, as they can cause frustration by disrupting the flow of information [20]. Enhanced dialog boxes aimed at providing context sensitive guidance and re-ordered content may help minimize this loss of impact [1], but at the potential cost of increased cognitive demands that may lead to other accessibility problems.

2.2 Passwords

Known usability problems with passwords – including weak passwords and password reuse – may be compounded for users with disabilities. Cognitive disabilities may limit a user's ability to remember multiple passwords, leading to greater reuse. Users with motor impairments who use pointers to press keys may find that long characters strings containing capitalized letters or symbols are too time-consuming to enter accurately. These difficulties might encourage these users to select weaker, but easier-to use passwords. Users who rely on speech recognition systems must speak their password aloud – an obvious security problem [6].

Usability concerns have led researchers to explore alternate authentication mechanisms that go beyond typing alphanumeric strings at a keyboard. Many of the recently-proposed alternative password schemes are graphical, relying on the user's memory of either specific pictures chosen from larger sets, or sequences of points drawn as a sketch or chosen from a picture

Systems involving recall of specific pictures require identification of selected images from a larger set including irrelevant decoys. Déjà Vu used randomly generated art and a single grid containing all of a user's chosen images, which must all be selected [8]. Passfaces used photographs of human faces, placing one of the user's images in a 3x3 grid with eight decoys, and requiring successful selection of four images in four sequentially-presented grids for successful authentication [8].

The selection of images from a grid can be contrasted with tools that use sketches or points selected on a 2D plane. Draw-A-Secret [16] and related tools use freehand sketches on a 2D grid to act as a password. Qualitative-Draw-A-Sketch [21] transforms the grid to use smaller cells of varying shapes, thus increasing the search space.

Passpoints asked users to click a selection of points in a photograph[30]. Evaluations of Passpoints have identified a variety of concerns, including the size of the tolerance window allowed when judging the correctness of a selection and the impact of the choice of image [29] [5]. Interference between multiple passwords may also be problematic [5]. A very different vision of a graphical password system is presented by EyePassword [18], which uses an eye-tracking system for gaze-based selection of password characters from an on-screen keyboard. Non-graphical password schemes have been proposed as well. Keystroke biometrics – the identification of individuals through timing patterns in keystrokes [23] has been the subject of many studies. One possible variation this idea includes measurement of keystroke force as an additional parameter [17].

Many of these alternative password schemes present significant accessibility challenges. Graphical passwords (and eye-tracking systems) are clearly inaccessible to individuals who are blind or who have substantial vision loss. People with poor motor control may find keystroke-based systems may be difficult, it not impossible to use.

2.3 CAPTCHAs

CAPTCHAs are tools for proving that a human – as opposed to a software program - is providing input to a software application [28]. The most widely used CAPTCHAs challenge users to type in a string of distorted letters found in an image. As long as extracting the characters via computer vision techniques is sufficiently difficult, one can reasonably sure that any correct answers were provided by human users. Alternatives to textual tests include image-based CAPTCHAs, which involve identification of image contents, selection of anomalous images from a set, or similar tasks [3, 4, 7]. These techniques have not been used as widely as the ubiquitous text in image CAPTCHAs.

The accessibility concerns with text-based CAPTCHAs have led to the introduction of audio alternatives. Audio CAPTCHAs typically ask users to type in a series of digits as spoken in the audio stream. As spoken digits can be recognized by speech-recognition software, these systems typically use added noise and a variety of voices to defeat potential attacks. [22] [25]. The resulting audio streams may be hard to interpret, making the system accessible but perhaps less than usable. An alternative design based on the transcription of spoken words eliminates the difficulties associated with remembering strings of random numbers [25]. Logic puzzles have also been proposed as accessible CAPTCHAs, but these might pose difficulties for users with cognitive difficulties [22].

3. USER CONCERNS

Users with disabilities are potentially more vulnerable to security and privacy threats. In a recent survey on computer usage by children and young adults with Down Syndrome (DS), security and privacy related concerns were frequently raised by the responding parents. According to the survey, individuals with Down Syndrome start using computers at early age (some as early as 3 years old) and spend considerable amount of time

online for both educational and entertainment purposes. However, their awareness and understanding towards the potential security and privacy threats are minimal [13]. Since those young individuals with DS tend to be more trusting towards others, parents have great concerns that their child will fall victim to online predators. As a result, some parents do not allow their child to participate in online chat rooms or to use instant messaging. Individuals with DS also have great difficulty dealing with various security mechanisms including passwords, CAPTCHAs, security questions, etc.

A recent investigation of the security concerns of blind users led to the identification of several pressing problems, including inaccessible CAPTCHAs and other software (including anti-virus tools; login timeouts; insufficient feedback during software installation; and spyware, including keystroke loggers [15]. Some of these concerns (inaccessible anti-virus software, updates that interfere with accessibility) may involve relatively tractable questions of design, development, and testing. Many of the other concerns of blind users, including insufficient details of software installation process and spyware are directly applicable to all computer users. Software installation tools are largely inscrutable: with even modestly complex tools requiring the installation of dozens of files, only the most expert users will be able to understand the files involved and their potential impact. Similarly, keystroke loggers or other malware are virtually impossible to detect manually. Usable and accessible tools that provide greater feedback in these areas would give users the information necessary to understand what their computer is doing and to apply that understanding towards greater privacy and security.

4. UNIVERSALLY USABLE PRIVACY AND SECURITY

Universal usability refers to the challenge of building tools that can be used by the widest possible range of users in the widest possible range of circumstances. Working towards this ideal requires attention to three critical areas: user diversity, technological diversity, and gaps in user knowledge [26, 27]. Consideration of each of these perspectives can lead to privacy and security tools that will better meet the needs of a broader range of users.

User diversity: Accommodation of users with differing abilities often means provision of alternative forms of content. Just as audio presentation has the potential to make CAPTCHAs accessible to blind people, tools such as graphical passwords or color-coded anti-phishing toolbars can be combined with alternatives that are accessible to users that cannot perceive visually-encoded information.

These alternatives can often increase usability for people who might not otherwise be traditionally considered to have an impairment. Audio-enabled anti-phishing tools might emit a warning tone when a user loads a web site that has been flagged as being a phishing page. In addition to making an otherwise inaccessible display available to blind users, this feedback will provide a redundant cue that might help sighted users avoid phishing attacks. Similarly, users with some age-related vision loss might find audio CAPTCHAs easier to use, as compared to their graphical counterparts.

Technological Diversity: Many widely-used tools and research prototypes implicitly assume the use of a traditional computer display. As users increasingly engage in mobile activity, and as mobile devices are increasingly used as accessibility aids [19], privacy and security tools that work on devices with small displays and keyboards will be necessary.

Small displays may present particular problems for graphical passwords. Although the presentation of an alternative mode may help in this regard, there may be unintended consequences. If a traditional textual password is provided as an accommodation to make graphical passwords both accessible and suitable for small displays, users may come to rely solely on the textual version, making the graphical display irrelevant.

Gaps in User Knowledge: Fighting phishing, preventing SPAM, avoiding malware, and cultivation of awareness regarding security and privacy all require appropriate user knowledge. The development of shared and comprehensible vocabularies and iconography to convey security concerns would benefit all users. Explanations of system actions and the ramifications of user choice that allow users to make informed, constructive decisions are also critically important.

Ideally, universal usability implies the use of a single system to meet all needs. Although “separate but equal” parallel tracks may be unavoidable in some circumstances, they should be used only as a last resort. The evolution of the web is instructive in this regard. Parallel accessible sites (“click here for the text only version of this site”) were expensive to maintain, as each change in content or design had to be made twice. Modern sites make appropriate use of style sheets, good design, and guidelines [2] to achieve high degrees of accessibility without the expense of a parallel structure. However, current guidelines and tools still focus primarily on perceptual and motor impairments, with relatively little attention paid to cognitive difficulties. Improvement in the accessibility of security and privacy systems for individuals with motor and perceptual impairments is a necessary first step towards the long-term goal of universally usable privacy and security.

Application of these principles to privacy and security may require reconsideration of some designs. Most current audio CAPTCHA alternatives are “separate but equal” designs. CAPTCHA systems that ask a user to answer a question independent of the output mode, might be easier to build and maintain. If such systems can be built without sacrificing efficacy in distinguishing between humans and computers, they present an attractive alternative.

5. CONCLUSION

Solutions that resolve outstanding usable privacy and security concerns without addressing accessibility leave a substantial need unresolved. Appropriate application of universal usability principles can motivate research and development of systems that provide usable privacy and security for a broad range of users.

6. REFERENCES

[1] Brustoloni, J.C. and R. Villaramarín-Salomón, *Improving security decisions with polymorphic and audited dialogs*, in *Proceedings of the 3rd symposium*

on Usable privacy and security. 2007, ACM: Pittsburgh, Pennsylvania.

[2] Caldwell, B., et al., *Web Content Accessibility Guidelines 2.0*. 2007.

[3] Chellapilla, K., et al., *Designing human friendly human interaction proofs (HIPs)*, in *Proceedings of the SIGCHI conference on Human factors in computing systems*. 2005, ACM: Portland, Oregon, USA.

[4] Chew, M. and J.D. Tygar. *Image Recognition CAPTCHAs*. in *7th International Information Security Conference (ISC 2004)*. 2004: Springer.

[5] Chiasson, S., R. Biddle, and P.C. van OOrschot, *A second look at the usability of click-based graphical passwords*, in *Proceedings of the 3rd symposium on Usable privacy and security*. 2007, ACM: Pittsburgh, Pennsylvania.

[6] D'Arcy, J. and J. Feng. *Investigating Security-Related Behaviors Among Computer Users With Motor Impairments*. in *SOAPS 2006 Symposium on Usable privacy and security*. 2006. Pittsburgh, PA.

[7] Datta, R., J. Li, and J. Wang, Z., *IMAGINATION: a robust image-based CAPTCHA generation system*, in *Proceedings of the 13th annual ACM international conference on Multimedia*. 2005, ACM: Hilton, Singapore.

[8] Dhamija, R. and A. Perrig, *Déjà Vu: User study using images for authentication*, in *Ninth Usenix Security Symposium*. 2000.

[9] Dhamija, R. and J.D. Tygar, *The battle against phishing: Dynamic Security Skins*, in *Proceedings of the 2005 symposium on Usable privacy and security*. 2005, ACM: Pittsburgh, Pennsylvania.

[10] Dhamija, R., J.D. Tygar, and M. Hearst, *Why phishing works*, in *SIGCHI conference on Human Factors in computing systems*. 2006, ACM.

[11] Dirik, A.E., N. Memon, and J.-C. Birget, *Modeling user choice in the PassPoints graphical password scheme*, in *Proceedings of the 3rd symposium on Usable privacy and security*. 2007, ACM: Pittsburgh, Pennsylvania.

[12] Dunphy, P. and J. Yan, *Is FacePIN secure and usable?*, in *Proceedings of the 3rd symposium on Usable privacy and security*. 2007, ACM: Pittsburgh, Pennsylvania.

[13] Feng, J., et al., *Computer Usage by Young Individuals with Down Syndrome*, in *Submitted to ASSETS '08*. 2008.

[14] Freedom Scientific. *Freedom Scientific - JAWS for Windows Screen Reading Software*. 2008 [cited April 16, 2008]; Available from: http://www.freedomscientific.com/products/fs/jaws-product-page.asp.

[15] Holman, J., J. Lazar, and J. Feng, *Investigating the Security-Related Challenges of Blind Users on the Web*, in *Designing Inclusive Futures*, P. Langdon, J. Clarkson, and P. Robinson, Editors. 2008, Spring-Verlag: London. p. 129-138.

[16] Jermyn, I., et al., *The design and analysis of graphical passwords*, in *Eighth USENIX Security Symposium*. 1999.

[17] Kotani, K. and K. Horii, *Evaluation on a keystroke authentication system by keying force incorporated with temporal characteristics of keystroke dynamics.* Behaviour & Information Technology, 2005. **24**(4): p. 289 - 302.

[18] Kumar, M., et al., *Reducing shoulder-surfing by using gaze-based password entry*, in *Proceedings of the 3rd symposium on Usable privacy and security*. 2007, ACM: Pittsburgh, Pennsylvania.

[19] Lanigan, P.E., et al., *Trinetra: Assistive Technologies for the Blind*. 2006.

[20] Lazar, J., et al., *What Frustrates Screen Reader Users on the Web: A Study of 100 Blind Users.* International Journal of Human-Computer Interaction, 2007. **22**(3): p. 247 - 269.

[21] Lin, D., et al., *Graphical passwords & qualitative spatial relations*, in *Proceedings of the 3rd symposium on Usable privacy and security*. 2007, ACM: Pittsburgh, Pennsylvania.

[22] May, M., *Inaccessibility of CAPTCHA: Alternatives to Visual Turing Tests on the Web*. 2005.

[23] Peacock, A., *Typing Patterns: A Key to User Identification.* IEEE Security and Privacy, 2004. **2**(5): p. 40-47.

[24] Schechter, S., E. , et al., *The Emperor's New Security Indicators*, in *Proceedings of the 2007 IEEE Symposium on Security and Privacy*. 2007, IEEE Computer Society.

[25] Schlaikjer, A., *A Dual-Use Speech CAPTCHA: Aiding Visually Impaired Web Users while Providing Transcriptions of Audio Streams*. 2007.

[26] Shneiderman, B., *Universal usability.* Commun. ACM, 2000. **43**(5): p. 84-91.

[27] Shneiderman, B. and H. Hochheiser, *Universal usability as a stimulus to advanced interface design.* Behaviour & Information Technology, 2001. **20**(5): p. 367-376.

[28] von Ahn, L.v., M. Blum, and J. Langford, *Telling humans and computers apart automatically.* Commun. ACM, 2004. **47**(2): p. 56-60.

[29] Wiedenbeck, S., et al., *Authentication using graphical passwords: effects of tolerance and image choice*, in *Proceedings of the 2005 symposium on Usable privacy and security*. 2005, ACM: Pittsburgh, Pennsylvania.

[30] Wiedenbeck, S., et al., *PassPoints: Design and longitudinal evaluation of a graphical password system.* International Journal of Human-Computer Studies, 2005. **63**(1-2): p. 102-127.

[31] Wu, M., R. Miller, C., and S. Garfinkel, L., *Do security toolbars actually prevent phishing attacks?*, in *SIGCHI conference on Human Factors in computing systems*. 2006, ACM.

[32] Zhang, Y., et al., *Phinding Phish: Evaluating Anti-Phishing Tools*, in *Proceedings of the 14th Annual Network & Distributed System Security Symposium (NDSS 2007)*. 2007: San Diego, CA.