Standards, Usable Security, and Accessibility: Can we constrain the problem any further?

Mary Ellen Zurko
IBM
5 Technology Park Drive
Westford, MA, USA
mzurko@us.ibm.com

Kenny Johar
Vision Australia
454 Glenferrie Road
Kooyong, VIC 3144
kenny.johar@visionaustralia.org

ABSTRACT

This position paper discusses the accessibility issues and lessons learned thus far in addressing accessibility in the standards work of the W3C Web Security Context working group.

Categories and Subject Descriptors

D.4.6 **Security and Protection,** H.1.2 **User/Machine Systems.**

General Terms

Security, Human Factors, Standardization.

Keywords

Usable security, accessibility.

1.INTRODUCTION

W3C's Web Security Context working group (WSC) is the first standards effort in the area of usable security [1, 2]. The current draft recommendation includes best practices in displaying security context information, user identification of authenticated servers, security error handling, TLS user trust, assurance, authoring and deploying usably secured sites and pages, and browser/user agent techniques to provide a robust channel for security context information (wsc-xit) [3]. W3C has had a long commitment to all its standard addressing relevant accessibility issues and concerns. W3C's commitment to accessibility in web specifications was formalized in 1996 with the formation of W3C's Web Accessibility Initiative (WAI) [4]. Its mission includes development of guidelines, technical support resources, and educational materials as well as the charge to work with other W3C working groups to more fully incorporate accessibility across all W3C technical efforts. Recognizing that commitment, the objectives for WSC specifically call out accessibility as a concern [5].

Many of the known best practices in presenting usable security context information presume visual display. Some are taken care of by software assistive technologies used in conjunction with browsers, such as screen readers, screen magnifiers, and voice recognition software. Some are not. While producing the current draft of wsc-xit, the working group has consulted with accessibility experts on language or recommendations that were only phrased for visual interfaces. This position paper discusses the accessibility issues that have been raised, discussed, and formed the basis of specific proposes in the current wsc-xit draft, along with additional issues and lessons learned, and future looking thoughts on those topics.

2.Accessibility in wsc-xit

Any time multiple disciplines need to work together, some basis for synthesis or collaboration needs to be set. In initial discussions, we discovered a basic architectural split between where the usable security and the accessibility experts were concentrating. The majority of the WSC work has been targeted at information communicated by code that the user (presumably) trusts, the browser (or user agent) chrome itself. On the other hand, the majority of current challenges in accessibility on the web are around usable presentation of web site content. Because of that emphasis, software assistive technologies used in conjunction with browsers do not make the browser chrome clues about security state available to the user. While a padlock icon to indicate TLS protection is widely recognized by sighted users [6], this indicator has been unavailable through assistive technologies for people with complete vision loss. Recognition of "https" in the URL has been the only clue, in those cases, to some security state or context being in play or available. Some user agents do not even present the https: in URLs, or make URL presentation optional [7].

One of the topics covered in wsc-xit is the display of logotypes in X.509 certificates ("Logotype Certificates"). Logotypes provide visual and/or audio branding information to aid in human recognition and trust decisions. RFC 3709 [8] which defines logotypes does not address any accessibility issues specifically. wsc-xit specifically addresses the accessibility issues around using audio logotypes for trust information ("Good Practices for the Creation of Audio Logotypes"). The accessibility issues identified around rendering audio logotypes were user confusion and time.

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

Short musical phrases are a well known way to render audio clues while not slowing down rendering. However, any well known sound can be spoofed by content in a different context. The authors suggest that screen readers should be given the task to speak text associated with the logo aloud, and that the text be retrieved on demand, not spoken automatically. While studies show that users do not generally search security information out, none have included users of assistive technology, who are thought to be more likely to proactively issue commands requesting information. The accessibility experts helping with this position paper come down quite strongly on this point – the use of a keystroke to retrieve information is second nature to the visually impaired. Studies are needed to determine if that change in interaction pattern leads to an increase of requests for security context information over the sighted population (since that information is not necessary for most primary tasks).

The wsc-xit recommendations currently encourage the use of personalization of the user agent with some sort of shared secret visual or audio clue that would be hard to guess, and therefore hard to spoof, by web site content [9] ("Use Shared Secrets to Establish a Trusted Path"). Existing research has only covered visual clues, so that utility of audio clues in this context is not very well understood. Translation to an audio interface tehnique would mimic the visual secret with a specific, private audio signal each user configures, that is used by their user agent, to signal the start (and end) of trusted information communication. As with logotype audio information, the best way would be to make trust information available on demand through web API calls to assistive technology. Standards efforts in this area are needed to provide this information through user agent APIs. Screen readers could then speak aloud this information based on verbosity rules set by the users. These verbosity rules could include different voices for reading out the trust information than the voices used for reading primary or secondary content. This allows the user to choose a voice for security context information that they may associate with trust, assurance, or authority, and should be hard for an attacker to guess (e.g. personal).

One of the earliest pieces of guidance the WSC WG got from accessibility experts is that having a single place that displays all security context information, that the user can go to at will, is both good accessibility and good usability. wsc-xit would require complying user agents to provide such an overview and summary ("Additional Security Context Information"). This simple guideline may be the first clearly articulated guideline for accessible and usable security.

3.Accessibility Issues in wsc-xit

Despite WSC's initial consultations with and review from accessibility experts, wsc-xit still has a number of recommendations that are specifically visual, for which we have not yet developed non visual recommendations. Several of our recommendations rely on the differentiation between chrome and content ("Keep Security Chrome Visible" and "Do not mix content and security indicators"). What techniques, if any, do voice interfaces use to make the difference clear, to provide some basis for authority or assurance in the information conveyed by the chrome, which otherwise might be spoofed in an attack by the content? We touched on some possibilities for that in the previous section (conveying that information on demand, or configuring difficult to spoof audio signals or voices, to be used by screen readers).

We recommend that visual indicators of identity and TLS state in the primary chrome be placed in a consistent visual position for easy user reference ("Identity signal" and "TLS Indicator"). Is there a similar concern for the representations that assistive technologies generate?

Recent research has produced concrete guidelines on security warning techniques and their effectiveness [10]. wsc-xit has two recommendations from that work that specifically target visual interfaces. One is that notifications and status indicators used in situations where the risk level may vary by user preference be placed in the browser's persistent primary chrome ("Notifications and Status Indicators") Is there an equivalent form of non intrusive notification for voice interfaces? A related recommendation is on warning messages, which are used when the system has good reason to believe that the user may be at risk based on the current security context information, but a determination cannot positively be made. The header of a warning message must include something that means "caution" or "warning", and be the locus of attention ("Warning/Caution Messages"). Techniques in voice interfaces that ensure attention is paid could include pitch variations in the voice currently being used, a different voice, or a faster rate of speech.

Some of the recommendations that are specific to visual interfaces cover attacks targeted specifically at visual interfaces. In those cases, it is questionable whether the attack translates to aural interfaces, and if it does not, whether the aural interface population is large enough to provide enough return to attract attacks that are profit based (any population may be large enough to attract an attack for other motives). One visual attack is interaction flooding, where the user rapidly dismisses many dialogs, and in that sequence, also allowing some action they would have otherwise denied ("Pop-up Window APIs"). The same attack seems possible with voice interaction, as lots of pop ups translate to a large amount of speech output through screen readers, which is just as irritating and confusing.

As we mentioned above, many of the recommendations rely on the difference between chrome and content (e.g. "Do not use security context indicators to suggest trustworthiness"). Are there techniques that signal the difference between chrome and content in aural interfaces, to help with this distinction? Note that even in a visual interface, there is the potential for confusion between these areas, which our shared secret recommendation addresses.

A related area that WAI-ARIA, the accessible rich internet applications suit, is dealing with is in the area of semantic attributes on form fields to indicate the need for special users processing (for example, "required" fields). One of the attributes under consideration is for "secret" data, to signal when input will not be echoed. However, there is some concern that the introduction of this attribute would be an aid to phishers and other attackers, who would be spoofing a familiar seeming login page to the user. The many unknowns in accessible presentation of security context information leave the likelihood of this form of attack an open question.

A similar question arose with the aural equivalent to masking passwords during input, when WSC was considering a recommendation in that area. There is a precedent for providing an audio echo where no visual echo is ever provided. For example, in some accessible ATMs, the audio is delivered to an earphone jack, which provides a level of privacy not available for the visual interface. In the case of computer access, screen readers allow the user to configure the echo to be nothing, stars, or the text typed, leaving the security/usability tradeoff to the user. The usual default is stars for both password fields and any text field that visually shows stars, providing equivalent per keystroke acknowledgement. There is considerable concern among accessibility experts that this level of user choice (allowing configurations that speak password input) opens a security hole in situations that echo to the computer's speakers, while that option, and therefore that potential hole, does not exist in visual interfaces.

4.Conclusions

This position paper has outlined the initial questions, issues, and resolutions around accessible processing of standardized usable security context information. The existing research and deployment experience that informs many of the wsc-xit recommendations [11] is all in visual representations of that information. A sensitivity to accessibility issues, coupled with some consultation with accessibility experts, has provided a thorough outline of the accessibility issues in our current draft of wsc-xit, but, to date, limited resolution of them. Fundamental guidelines on communicating the difference between chrome and content are still needed, as are more in depth studies on attention management in aural interfaces.

5.ACKNOWLEDGMENTS

Particular thanks to Al Gilman and Janina Sajka, who provided invaluable guidance on the accessibility aspects of this position paper.

6.REFERENCES

[1] Web Security Context Working Group home page, http://www.w3.org/2006/WSC/.

[2] Zurko, M. E. and Johnson, M. Standardizing Usable Security and Privacy: Taking It To the Next Level, or Settling for Less? SOUPS 2007 Discussion session, http://cups.cs.cmu.edu/soups/2007/slides/StandardsDiscussion.ppt.

[3] Roessler, T and Saldhana, A., eds. Web Security Context: Experience, Indicators and Trust. http://www.w3.org/TR/wsc-xit/.

[4] Web Accessibility Initiative, http://www.w3.org/wai.

[5] Web Security Experience, Indicators and Trust: Scope and Use Cases. http://www.w3.org/TR/wsc-usecases/.

[6] Downs, J., Holbrook, M., and Cranor, L. "Decision Strategies and Susceptibility to Phishing", SOUPS 2006.

[7] Niu, Y., Hsu, F., and Chen, H., "iPhish: Phishing Vulnerabilities on Consumer Electronics", UPSEC 2008.

[8] Santeson, S., Housley, R., and Freeman, T., eds. Internet X.509 Public Key Infrastructure: Logotypes in X.509 Certificates, RFC 3709, February 2004.

[9] Dhamija, R. and Tygar, D. "The Battle Against Phishing: Dynamic Security Skins", SOUPS 2005.

[10] Egelman, S., Cranor, L., and Hong, J. "You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings", SIGCHI 2008.

[11] W3C Web Security Context Wiki – Shared Bookmarks. http://www.w3.org/2006/WSC/wiki/SharedBookmarks.