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

Mary Ellen Zurko

W3C WSC WG Chair

W3C’s Web Security Context Working Group

- Web Security Context (wsc-ui) – first standards effort in usable security
  - Displaying security context information
  - Server identity
  - Security error handling
  - TLS user trust
  - Robustness of channel for security information

Bringing in Accessibility

- W3C has an explicit commitment to accessibility in all of its work
- Many of the known best practices in presenting usable security context information presume visual display
- wsc-ui targeted at web user agent (e.g. browser) display of trustworthy information
- Current accessibility work centers on web site content best practices
  - Current assistive technologies do not make browser security cues available (e.g. the "padlock")
  - Some user agents do not display the URL for the https: cue
- Have a single place with all security context information that users can go to
  - Perhaps the first clearly articulated guideline for accessible and usable security

Logotypes in X.509 Certificates

- Visual and/or audio branding information to help with trust decisions
- RFC 3709 does not address accessibility specifically
- Accessibility concerns – user confusion and time
- Accessibility recommendations
  - Assistive technology speaks text out loud when the user requests it
    - Do _not_ automatically play the logotype or speak text
  - Existing studies show that users do not seek security context information out
    - Accessibility experts insist that these requests are second nature to the visually impaired
  - Allow configuration of specific voices for security context information
    - Calls out the difference
    - Hard for an attacker to impersonate if personalized

Issues and questions

- Is there an accessibility analog to a consistent visual position for easy user reference?
- What for does or should non intrusive notification take in the case where the risk level cannot be determined?
- When attention must be paid to security information, do pitch variations, a different voice, and/or a faster rate of speech work?
- Is there an audio equivalent to the information flooding attack?
- Does allowing a configuration that speaks password information open a hole for a vulnerability that would otherwise be considered unacceptable?
    - Screen readers do this, though it is not the usual default

Notable Gaps

- Generally accepted guidance on designing usable accessible and secure interfaces
  - Are there references for the claims of our accessibility experts, particularly around providing information on demand?
- Research and findings in the area of differentiating chrome and content aurally
- Guidelines for attention management in aural interfaces

Thank you

- Questions and comments?
- http://www.w3.org/TR/wsc-ui/
  - Will be there shortly, for last call
- http://lists.w3.org/Archives/Public/public-wsc-wg/
- mzurko@us.ibm.com