Developing Accessible and Usable Security (ACCUS) Heuristics

Daniela Napoli
Carleton University
Ottawa, Canada
daniela.napoli@carleton.ca

Abstract

Currently, usable security and web accessibility design principles exist separately. Although literature at the intersect of accessibility and security is developing, it is limited in its understanding of how users with vision loss operate the web securely. In this paper, we propose heuristics that fuse the nuances of both fields. With these heuristics, we evaluate 10 websites and uncover several issues that can impede users' ability to abide by common security advice.

Author Keywords

usable security, accessibility, heuristics, expert evaluation

ACM Classification Keywords

H.5.m [Information interfaces and presentation]: Accessibility design and evaluation methods

Introduction

Sixty per cent of Canadians with vision loss report that the Internet improves the quality of their daily life [6]. Since the likelihood of developing a seeing disability increases with age, the population with visual impairments who rely on a universal Web will also likely increase over time.

The discourse at the intersect of cybersecurity and accessibility is limited [10]. Common usable security design principles [14] do not address the unique needs of users with vi-

CHI, '17 Montreal, Quebec Canada
ACM 0-12345-67-8/90/01.
http://dx.doi.org/12.3456/12345678910

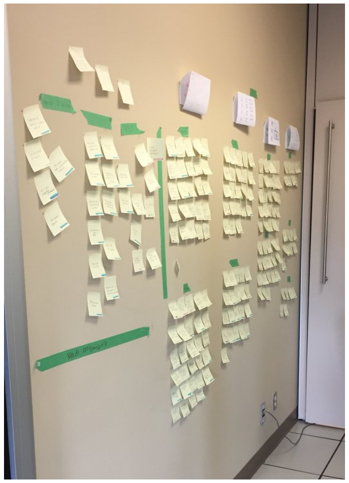


Figure 1: Data analysis process guiding formation of the ACCUS heuristics.

sion loss. Similarly, widely adopted Web accessibility guidelines [7] do not provide explicit methods of ensuring secure non-visual browsing environments.

To address this gap, we are using a two-phase approach including an initial expert evaluation and an observational user study. This paper focuses our first phase in which we assess the current non-visual security cues intended to allow individuals with visual impairments to use the Web securely – or at least, to abide by common security advice like parsing URLs, checking for evidence of SSL certificates, and generally being careful and mindful [12].

This paper's two main contributions to the HCI community include: a first iteration of heuristics that can guide the design and evaluation of security mechanisms that address accessibility and usability requirements, and a security-focused assessment of usability issues identified through an expert evaluation of 10 websites.

Background

Individually, guidelines for accessible web design [7] and usable security systems have existed for quite some time [14]. In 2008, the W3C proposed the second iteration of their Web Content Accessibility Guidelines (WCAG) that are rooted in making designs perceivable, operable, understandable, and robust. While, in 1999, Whitten and Tygar proposed a pivotal definition of usable security with four main priorities: ensure users can know what security tasks are required, show them how to successfully complete those tasks, prevent dangerous errors, and make users comfortable enough to use the system again.

However, little research addresses both usable security and accessibility. Of the existing work, studies have identified major accessibility and usability issues regarding inputting credentials during log in processes [9], and task interruptions after page refreshes [5]. Other work in this realm has focused on improving audio CAPTCHAs [11], proposing novel authentication methods [4], and identifying general security concerns [2].

Since preventative browsing behaviours differ greatly between people with average sight and those with vision loss [3, 1], it is critical to address the unique nuances between these two user groups when discussing usable security.

In our work, we focus on understanding the security obstacles users with vision loss face while browsing the Web. Thus far, related work has not been generalized into a set of heuristics that explicitly address the design of web-based security cues for users with visual disabilities. In this paper, we explore how to provide these users sufficient opportunities to securely share personally identifiable information on the Web.

Proposed Heuristics

Our first task was to develop heuristics that blend accessible and usable security (ACCUS) concepts pertaining to the design and evaluation of security-related systems. We extracted, analyzed, and open-coded 172 usable security and accessibility best practices, expert recommendations, and sighted/non-sighted user behaviours documented in 25 peer-reviewed conference papers and journal articles published between 1999 and 2017 (Figure 1). We iteratively categorized the data to extract common themes and developed heuristics that best reflected the data. The resulting nine heuristics are as follows, and they should be interpreted in the context of security and privacy for non-visual usage:

ID	*Webpage*
A	www.canadapost.ca
B	www.ontario.ca/page/serviceontario
C	www.ecampusontario.ca
D	easyweb.td.com
E	www.gsapplications.carleton.ca
F	www.hydroottawa.com
G	www.mail.google.com
H	www.prestocard.ca
I	www.viarail.ca
J	www.facebook.com

Table 1: The homepage URLs of websites evaluated.

	Total	*Mean*
ID	*Issues*	*Severity*
A	110	3.4
B	57	3.4
C	75	3.0
D	109	3.2
E	58	3.2
F	135	2.8
G	82	2.9
H	37	2.9
I	97	3.1
J	76	3.1

Table 2: A summary of evaluation results.

Informative. All textual content must be brief, informative, and parsable. Demonstrative non-textual artefacts must be described in a way that is meaningful to the user.

Reliable. The current state of security/privacy and related functions must be explicitly available. All security information must be described with plain language and no jargon.

Recognizable. The interface must be distinguishable and organized in a way that reflects users' expectations. All functionalities are clearly available and traversable.

Assistive. Users are guided through decisions to be made. Error prevention conventions are in place. Users can recognize, diagnose, and correct mistakes. Defaults are appropriate and can be modified within reasonable confines.

Functional. The site works as expected in a quick and complete manner. No functionalities impede on users' goals nor security/privacy.

Controllable. The site is compatible with assistive technology. The interface offers robust and customizable means to protect users with various needs.

Responsive. All actions, errors, and threats are effectively communicated without interrupting users' workflow. Users can identify when a task is completed.

Diverse. All content and context is communicated in a way that can accommodate various abilities. Satisfactory alternatives, both visually and aurally, are clearly available.

Memorable. All system functions and related user actions require a low cognitive load. The system is designed for learnability and evokes high recall abilities.

Website Evaluation

Using the ACCUS heuristics, one researcher with expertise in web accessibility and usable security assessed 10 websites (Table 1) that allowed users to exchange sensitive information for services such as updating official government documents, paying bills, and shopping online.

During our expert evaluation we attempted to complete three tasks per website: 1) verify the site is legitmate, 2) login to the site, and 3) complete a site-specific transaction. While completing each task, we evaluated audible feedback against the ACCUS heuristics. We noted each issue and rated its level of severity on a scale of 1 (low-priority) to 4 (catastrophic). We browsed the sites with JAWS 18 screen reading software to identify potential accessibility issues. We chose not to disable the screen during the evaluation to observe the discrepancies between visual and aural information. We used commonly reported keyboard shortcuts to try to complete the tasks, but followed no predefined sequence of actions since screen reader users tend to use several various workarounds [5]. Usable security studies involving JAWS tend to employ Internet Explorer (IE) when performing related experiments [9]; similarly, we used IE 11.64.16299.0 on a Windows 10 computer for this study.

Navigating with a screen reader can be a lengthy process due to accessibility issues and the forced sequential nature of information delivery, so we imposed time and trial limits to manage our scope. We alloted ample time for each task with a maximum of 30 minutes to verify the site's legitmacy, 15 minutes to login, and 45 minutes to complete site tasks. Additionally, our attempts ceased if they could not be with three[1] different attempts during the allotted time.

[1] Interfaces are about three times more usable for sighted users than non-sighted [8]. Therefore, we argue that browsing with JAWS during our evaluation should not exceed this number of trials.

ID	*Verify*	*Login*	*Task*
A	*45	*40	*25
B	*20	N/A	37
C	*11	35	*29
D	*38	21	50
E	*15	N/A	*43
F	*30	34	*71
G	*30	32	20
H	*13	10	14
I	*18	*30	*49
J	*21	24	*31
Total	**241**	**226**	**369**
Tasks completed	***0/10***	***6/8***	***4/10***

Table 3: Number of issues related to tasks for each website. Asterisks mark the tasks that were abandoned by the evaluator due to time or trial limitations.

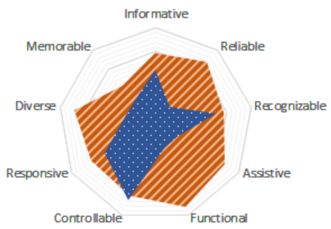


Figure 2: Comparing the total number of issues (blue, dotted) and the mean severity (orange, striped) for each ACCUS heuristic.

Results

Generally, we spent 60 to 90 minutes evaluating each website. Table 3 describes the number of instances an ACCUS heuristic was violated by each website. The greatest number of issues occurred while attempting to complete site-specific tasks (Table 3). At a high level, Figure 2 shows that the greatest number of issues discovered were related to the *controllable* heuristic (N=172) and the most severe issues found were related to the *functional* heuristic (M=3.6).

The number of uncovered issues varied greatly depending on the site's general compatibility with JAWS. Ultimately, some sites had significantly fewer issues but were not necessarily more accessible or usable. For example, we were unable to verify the legitimacy of any of the ten sites. In fact, sites with fewer issues were often so inaccessible that we could not complete some tasks to properly explore the site. Therefore, to better understand our findings, we discuss a few of the most concerning issues further.

Verifying Page Legitimacy

JAWS was unable to access the text within Internet Explorer's security report dialogue box (Figure 3) when attempting to verify the sites' SSL certificates. The browser provided alternative text for the lock icon, "Tool bar security report button. To activate press the space bar." Yet, the text within the offered report could not be accessed by various JAWS reading commands including all four `arrow keys` and `insert + up`. Furthermore, since the close button was automatically selected by default, the system cued users to exit the report immediately, "Security report. Close button. To activate press space bar."

With further investigation, a JAWS user can eventually find readable text regarding the site's certificate by clicking through the report's *View Certificates* link, selecting the new window's *Certification Path* tab, and finally reading, "Certificate is OK," letter by letter with the left and right `arrow keys` (Figure 4).

Login Processes

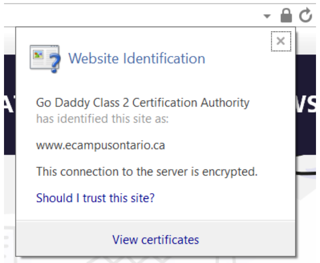
As illustrated in Vigo and Harper's study on screen reader browsing strategies [13], users are presented miscellaneous links, headers, and navigation bars before the main content of a page. Users can listen to each section or skip to relevant content. However, communicating change in the main content upon refresh or redirect with JAWS is not as direct as a visual scan since users must find and listen to changes to notice the update.

A successful login usually redirected the user to a new page containing personal account information which JAWS would automatically begin reading. The page change was visibly explicit but, for the majority of websites, there was no audible feedback to demonstrate that the credentials were correct and that the user was being directed to a new page.

After an unsuccessful login attempt, the same page would refresh and present an error message visually cuing the user to try again. However, the page refresh was not announced. JAWS would then reread the same page without explicit explanation. Furthermore, the error messages pertaining to incorrect credentials were not announced unless selected while the user skimmed through the page manually, or consequently read aloud if the user allowed JAWS to automatically read the page until it passed through the login section. Since there is minimal audible feedback during the login process, users are forced to follow a trial-and-error process of skimming through page content to establish progress towards their goal.

Site-Specific Tasks

The transactional tasks we attempted could only be successfully completed on 4 of the 10 tested pages. Most tasks


Website Identification

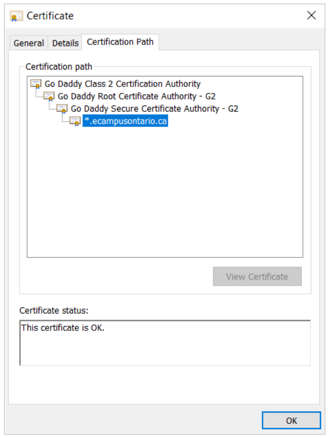
Go Daddy Class 2 Certification Authority
has identified this site as:

www.ecampusontario.ca

This connection to the server is encrypted.

Should I trust this site?

Figure 3: The text within Internet Explorer 11’s security report was unreadable with a JAWS screen reader.


Certificate

Certification path

Go Daddy Class 2 Certification Authority
Go Daddy Root Certificate Authority - G2
Go Daddy Secure Certificate Authority - G2
*.ecampusontario.ca

Certificate status:

This certificate is OK.

Figure 4: A user can use JAWS to read that a site host’s certificate is "OK" with further investigation.

were inhibited by accessibility issues such as insufficient alternative text and limited JAWS compatibility. These issues prolonged evaluations beyond the established time and trial limits and thus restricted our exploration of the related pages. It is likely that these accessibility obstacles would also impede non-sighted users’ ability to achieve site-specific tasks and abide by security advice.

Discussion

The usability and accessibility issues we identified can stop a user from following common security advice while browsing online.

Firstly, security advice typically urges users to check SSL certificates to protect against threats such as man-in-the-middle (MITM) attacks. Information about a certificate’s status and the entity establishing the secure connection can also help a user to identify potential phishing sites.

During the evaluation, IE did not allow JAWS to read textual information pertaining to the certificate. Since most users tend to be more task-focused than security conscious, it is also likely users will exit the security dialogue upon cue and will not explore the window to discover the single readable sentence regarding the state of the certificate. Thus, IE users with vision loss are currently limited in their ability to follow advice pertaining to certificates and may, therefore, be more vulnerable to exposing sensitive information than their sighted counterparts.

Secondly, much of the recent usable security research has focused on passwords. However, we discovered that screen reader users attempting to login to personal online accounts are provided insufficient cues to signal that access to their personal information has been granted, and that they are being rerouted to new pages containing such information. This is particularly concerning because they are unable to identify if and when protected information is being visibly shown. This lack of sufficient feedback could increase their vulnerability to visual eavesdropping and thus nullify precautionary actions like using strong passwords and storing credentials in password managers.

Thirdly, security advice also recommends that users be generally thoughtful when clicking on unfamiliar URLs or downloading attachments that may put them at risk.

Interfaces that are incompatible with screen readers restrict non-sighted users’ ability to analyze information and make informed, secure decisions. General usability issues such as convoluted URLs or authorized sites without evident trust indicators (https, SSL certificates, or a familiar domain name) can also interfere on both sighted and non-sighted users’ ability to carefully browse the Web. Yet, these usability issues can more severely impact non-sighted users if they are reliant on audible outputs and limited in assessing other page characteristics that sighted users may utilize.

Future Work

Our ACCUS heurisics allowed us to categorize issues and identify the impact on visually impaired users’ online security and privacy. We will further refine the proposed heuristics to specifically address concerns at the intersect of accessibility and usable security. For example, we aim to identify specific criteria for describing SSL certificates or optimizing login-related feedback.

Future iterations of the ACCUS heuristics will also integrate user behaviour data collected from upcoming user studies involving screen reader users with vision loss. Integrating feedback from individuals with disabilities will also improve the reliability and authenticity of our website evaluations.

Conclusion

Despite advances in Web accessibility and usable security, the results of our expert evaluation suggest are there still major issues in allowing people with vision loss to interact with the Web securely. Most websites, even transactional sites that require users to exchange sensitive information, fail to adequately address accessibility for security and privacy concerns. Our findings suggest that the ACCUS heuristics can assist web designers in improving the usability and accessibility of security features.

Acknowledgements

This work is guided by Professor Sonia Chiasson, and is supported by a Digital Inclusion Research Grant from eCampusOntario for 2017-18.

REFERENCES

1. A. Abdolrahmani and R. Kuber. 2016. Should I Trust It When I Cannot See It?: Credibility Assessment for Blind Web Users. In *ASSETS*. ACM, 191–199.
2. T. Ahmed, R. Hoyle, K. Connelly, D. Crandall, and A. Kapadia. 2015. Privacy Concerns and Behaviors of People with Visual Impairments. In *CHI*. ACM, 3523–3532.
3. M. Alsharnouby, F. Alaca, and S. Chiasson. 2015. Why Phishing Still Works: User Strategies for Combating Phishing Attacks. *International Journal of Human-Computer Studies* 82 (2015), 69–82.
4. S. Azenkot, K. Rector, R. Ladner, and J. Wobbrock. 2012. PassChords: Secure Multi-touch Authentication for Blind People. In *ASSETS*. ACM, 159–166.
5. Y. Borodin, J. Bigham, G. Dausch, and I. Ramakrishnan. 2010. More Than Meets the Eye: A Survey of Screen-reader Browsing Strategies. In *W4A*. ACM.
6. Statistics Canada. 2006. *Partcipation and Activity Limitation Survey 2006 Facts on Seeing Limitations*. Technical Report. Canada.
7. World Wide Web Consortium. 2008. Web Content Accessibility Guidelines (WCAG) 2.0. (2008).
8. K. Coyne and J. Nielsen. 2001. *Beyond ALT Text: Making the Web Easy to Use for Users With Disabilities*. Technical Report. Nielsen Norman Group.
9. B. Dosono, J. Hayes, and Y. Wang. 2015. "I'm Stuck!": A Contextual Inquiry of People with Visual Impairments in Authentication. In *SOUPS*. USENIX, 151–168.
10. H. Hochheiser, J. Feng, and J. Lazar. 2008. Challenges in Universally Usable Privacy and Security. In *SOUPS*. USENIX.
11. J. Lazar, J. Feng, T. Brooks, G. Melamed, B. Wentz, J. Holman, A. Olalere, and N. Ekedebe. 2012. The SoundsRight CAPTCHA: An Improved Approach to Audio Human Interaction Proofs for Blind Users. In *CHI*. ACM, 2267–2276.
12. R. W. Reeder, I. Ion, and S. Consolvo. 2017. 152 Simple Steps to Stay Safe Online: Security Advice for Non-Tech-Savvy Users. *IEEE Security Privacy* 15 (2017), 55–64.
13. M. Vigo and S. Harper. 2013. Challenging Information Foraging Theory: Screen Reader Users Are Not Always Driven by Information Scent. In *Conference on Hypertext and Social Media*. ACM, 60–68.
14. A. Whitten and J. Tygar. 1999. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In *USENIX Security*, Vol. 348. 169–184.