POSTER: Assessing Non-Visual SSL Certificates with Desktop and Mobile Screen Readers

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

Sonia Chiasson
Carleton University
Ottawa, Ontario
chiasson@scs.carleton.ca

ABSTRACT

Effective SSL warnings can point out network attacks or potential phishing sites. Much focus has been placed on tweaking text, colours, and symbols to improve users' comprehension and adhesion. These optimized visualizations do not necessarily aid people with visual disabilities who hear warnings rather than see them. To assess the non-visual aspects of these security warnings, we conducted an expert evaluation of Google Chrome and Mozilla Firefox's SSL certificate dialogues with JAWS and Apple VoiceOver screen readers. Our findings suggest that warnings are mostly unreadable with assistive technology and, when accessible, do not effectively describe threat sources, at-risk data, or false positives. Future work will explore the effectiveness of potential non-visual redesigns through usability studies with visually impaired screen reader users.

CCS CONCEPTS

• **Security and privacy → Human and societal aspects of security and privacy**; **Usability in security and privacy**;

KEYWORDS

usable security, accessibility, SSL certificates, screen reader

ACM Reference Format:
Daniela Napoli and Sonia Chiasson. 2018. POSTER: Assessing Non-Visual SSL Certificates with Desktop and Mobile Screen Readers. In *Proceedings of ACM SIGSAC Conference on Computer & Communications Security (CCS'18).* ACM, New York, NY, USA, 3 pages. https://doi.org/10.475/123_4

1 INTRODUCTION

Common security advice urges people to use websites with HTTPS when sharing sensitive information online [10]. Early studies suggested that users did not notice nor adhere to in-browser security indicators [5]; however, more recent large-scale field studies have suggested that effectively designed SSL warnings can significantly deter users from potential danger [1].

In this study, we conduct an expert evaluation to explore whether the audible outputs from a brower's SSL warnings and dialogues are comprehensible and effective in enabling screen reader users to assess their online security. We evaluate the audible feedback provided by desktop and mobile screen readers when using Chrome and Firefox based on design principles proposed in usable security literature. Our main contributions include:

- An expert evaluation of SSL dialogues via desktop and mobile screen readers
- Early recommendations for designing non-visual security warnings for users who rely on screen reading software

2 BACKGROUND

Security warnings have been recognized as poorly accessible for quite some time [8]. Despite this challenge and the fact that people with visual impairments are increasingly reliant on the Internet for tasks like online banking and social media, the accessibility of security warnings has not been deeply explored.

Research that considers the accessibility of cybersecurity has focused on better understanding visually impaired users' general security concerns and proposing novel accessibility solutions like audio CAPTCHAS [9], observation-resistant passwords [2], and accessible password managers [3]. But a gap exists in assessing the adequacy of non-visual information currently provided by browser security warnings.

When interfaces are not well designed for screen readers, users with visual impairments are forced to listen to irrelevant or incoherent aspects of a page before finding the content they require [12]. To compensate, screen reader users typically speed up output speech rates and use shortcuts to target sections they can understand and think will progress their goals [4]. These habits have lead users to skip important content and misinterpret their security and privacy while browsing [6]. Therefore, audible security information for this demographic must be accessible and comprehensible.

Felt et al. [7] propose guidelines for designing effective visual SSL dialogues. They emphasize that for users to adhere to SSL warnings, they must understand three dimensions of their security: 1) how they are being threatened, 2) what is at risk, and 3) whether the danger is real. Through improved comprehension, users can make better informed decisions rather than ignore security warnings and continue unsafe behaviours. We adapt Felt et al.'s three categories of comprehension to assess whether the audible information being offered from SSL dialogues can be understood and followed by visually impaired users.

3 METHOD

One of the authors knowledgable in both accessibility and usable security assessed the SSL dialogues in Chrome and Firefox on desktop and mobile setups. For the desktop, we used Chrome 63.0 and Firefox 57.0 on a Windows 10 operating system with JAWS 18

CCS'18, October 2018, Toronto, Canada

ACM ISBN 123-4567-24-567/08/06.
https://doi.org/10.475/123_4

With a valid SSL certificate							
Browser	**Device**	**Screen Reader**	**C1** *(max. 12)*	**C2** *(max. 12)*	**C3** *(max. 8)*	**Total Score** *(max. 32)*	**Adherence Rate**
Chrome	Desktop	JAWS	10	4	2	16	50%
Firefox	Desktop	JAWS	9	4	2	15	47%
Chrome	Mobile	VoiceOver	9	9	5	23	72%
Firefox	Mobile	VoiceOver	9	5	2	16	50%
Without a valid SSL certificate							
Browser	**Device**	**Screen Reader**	**C1** *(max. 12)*	**C2** *(max. 12)*	**C3** *(max. 8)*	**Total Score** *(max. 32)*	**Adherence Rate**
Chrome	Desktop	JAWS	9	4	2	15	47%
Firefox	Desktop	JAWS	7	6	2	15	47%
Chrome	Mobile	VoiceOver	0	0	0	0	0%
Firefox	Mobile	VoiceOver	0	0	0	0	0%

Table 1: Summary of the study's devices, browsers, screen reading software, and assessment results.

screen reading software. For the mobile device, we used Chrome 63.0 and Firefox 10.4 on iOS 11.2 and used its built-in screen reading software, VoiceOver.

We used Amazon (https://www.amazon.com) as a sample website with a valid SSL certificate. SSL warnings when using eCommerce sites like Amazon are important when exchanging financial information and other personally identifiable information online. Conversely, we used an evidently malicious website (http://www.validate.creditcard) to assess security warnings that may appear when visiting sites without a certificate. This website displays security (Verisign) and bank logos to strengthen their phishing attempts to collect credit card information from users. Security warnings are critical to steering users away from such predatory websites.

We assessed each browser's security dialogue interface on the two devices with the screen readers. We kept the devices' screens on during the evaluation to observe discrepancies between visual and audible information. For our assessment, we formulated eight guiding questions per Felt et al.'s [7] three comprehension criteria (Table 2). While going through the interfaces, we took note of the issues encountered and answered the guiding questions on a four-point Likert scale ranging from strongly disagree (1) to strongly agree (4). SSL dialogues that were inaccessible to the screen reader were assigned a zero in all categories. Through this method, each dialogue was awarded a total score out of 32.

Criteria	Guiding Questions
C1. Threat source	(1) Is the user informed that the network is secured or vulnerable? (2) Is there evident guidance to help the user consider the security of the network connection and ISP? (3) Is it clear that the threat would be/is related the connection to the server and not the website?
C2. Data risk	(1) Is the user informed that their data will be secured or vulnerable? (2) It is clear whether their data already on the site is secured or vulnerable? (3) Does the warning cue the user to consider the sensitivity of their data?
C3. False positives	(1) Is the user informed that SSL warnings can be triggered without an attacker? (2) Does the warning cue the user to consider the reputation of the website host, or past experiences with the site, to allow the user to assess the actuality of the threat?

Table 2: Evaluation's guiding questions based in Felt et al.'s SSL comprehension guidelines.

4 RESULTS

Table 1 summarizes our assessment's results. In brief, the audible information in most dialogues did not adhere to our evaluation criteria and most poorly informed users of false positives (C3). Chrome and Firefox security dialogues disappeared when visiting the HTTP website on mobile and thus SSL information was totally inaccessible. The absence of SSL information would be problematic for any user, but a lack of security information is a more severe issue for visually impaired users who cannot compensate by using other visual cues to assess their security.

As Felt et al. emphasize, information pertaining to each category is critical to improving users' comprehension of SSL security and the potential for proper adhesion.

C1. Threat source. SSL warnings which identify threat sources stemming from the server, rather than the website, enables users to assess the security of their internet connections and make appropriate decisions in protecting themselves from data interception.

When accessible, both desktop and mobile versions of the browsers emphasized the secured nature of the connection to a website, e.g. *"Secure connection dialogue. To navigate use tab,"* on Chrome *"Secure connection. Show connection details."* on Firefox. This is intended to tell the user whether the communication between the client and the server is secure.

However, specific information pertaining to the connection's security was difficult to find; on desktop, it was tacked on to the end of one run-on sentence listing the page's URL, titles, and lock icon alternative text. SSL information which is buried under generic site information may be overlooked by screen reader users if they choose to skip to the next section to avoid redundancy and manage their cognitive load. Furthermore, mobile users have to tap through the dialogue multiple times to reach the portion which includes network security information. Users are unlikely to tap through the entire dialogue unless they are suspicious of the website.

C2. Data risk. Messages describing at-risk data informs users of what personal information is vulnerable and enables them to consider the sensitivity of the information they share. Felt et al. suggest that users should also be aware that data already on a site can be vulnerable during an attack. Per our results, most dialogues did not provide information identifying what data was at risk. On desktop and mobile, Chrome provided examples of information that is safe on a HTTPS site, e.g. "*Your information for example passwords or credit card numbers is private when it is sent to this site.*" On a HTTP website, no similar information was offered by Chrome's desktop and mobile dialogues. This fails to cue users to consider the security and privacy of their data when it is most vulnerable.

C3. False Positives. The third SSL comprehension category, false positives, pertains to warnings that may be incorrectly triggered by things such as misconfigured SSL certificates. False positives can affect users' confidence in security mechanisms. Therefore, warning information should enable users to consider the context of the warning to weigh the actuality of the threat.

No dialogues mentioned the concept of false positives. However, both browsers' dialogues on HTTPS sites included the name of the certificate's issuer and its expiry date which may enable users to better assess the reputation of the involved organizations. Again, when using HTTP websites, users were not given information to assess their circumstances nor consider potential threats.

5 DISCUSSION

Our initial results point to four areas of non-visual SSL design for future consideration. For one, especially on mobile browsers, SSL dialogues do not provide enough information for users to comprehend potential threats. This is an issue for users, particularly for those who are visually impaired and limited to portions of a browser that are accessible through screen reading software. SSL dialogues need to better describe potential threats, especially on HTTP websites, textually and audibly.

Secondly, our results suggest defining SSL information to more effectively communicate with screen reader users. Screen readers communicate serially, and one optimized sequence of information delivery may be: 1) immediately identify the state of security without the need to enter the SSL dialogue, 2) provide relevant examples of the types of data is safe/at risk, and 3) describe circumstances in which SSL attacks are more likely to be imminent rather than a false positive. User testing could assess the effectiveness of this information sequence on visually impaired users' comprehension of security warnings.

Thirdly, to elaborate on the first piece of our proposed sequence, it may be most effective to communicate the state of a connection early on without requiring the user to explore the SSL dialogue. Like a visual pop-up, implementing this well can be complicated. We suggest methods which do not interfere with the user's workflow or mental load such as a chime indicating the presence or absence of SSL before hearing the page's title, URL, and major headings.

Furthermore, many words can denote safety to a user. Within our evaluation, the word "validate" was included in the phishing website's title and URL. When reading SSL dialogues, there was no audible differentiation between the browser's use of the word versus the site's misuse of the word. Future studies may explore methods of helping screen reader users comprehend differences between legitimate and illegitimate uses of security terminology, for example through different voices for browser dialogues and web page content.

Conclusion. We conducted an expert evaluation of the accessibility of SSL dialogues through the use of screen readers. Our results suggest that none of the SSL security dialogues were entirely accessible; when accessible, the information did not comprehensibly describe threat sources, at-risk data, nor false positives. This lack of effective non-visual SSL information places visually impaired users' at increased risk. We recommend audible SSL information should be immediate, relevant, and clear. In the future, we will further assess non-visual SSL information and conduct usability studies with visually impaired users to explore how to improve security warnings to meet their unique needs.

REFERENCES

[1] D. Akhawe and A. Felt. 2013. Alice in warningland: A large-scale field study of browser security warning effectiveness.. In *USENIX Security Symposium*, Vol. 13.
[2] S. Azenkot, K. Rector, R. Ladner, and J. Wobbrock. 2012. PassChords: secure multi-touch authentication for blind people. In *ASSETS'12*. ACM, 159–166.
[3] N. Barbosa, J. Hayes, and Y. Wang. 2016. UniPass: Design and Evaluation of a Smart Device-Based Password Manager for Visually Impaired Users. In *Pervasive and Ubiquitous Computing*. ACM, 49–60.
[4] 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, 13.
[5] R. Dhamija, J. Tygar, and M. Hearst. 2006. Why phishing works. In *CHI'06*. ACM, 581–590.
[6] B. Dosono, J. Hayes, and Y. Wang. 2015. "I'm stuck!:" a contextual inquiry of people with visual impairments in authentication. In *SOUPS'15*. 151–168.
[7] A. Felt, A. Ainslie, R. Reeder, S. Consolvo, S. Thyagaraja, A. Bettes, H. Harris, and J. Grimes. 2015. Improving SSL warnings: comprehension and adherence. In *CHI'15*. ACM, 2893–2902.
[8] H. Hochheiser, J. Feng, and J. Lazar. 2008. Challenges in universally usable privacy and security. In *SOUPS'08*, Vol. 2008.
[9] 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'12*. ACM, 2267–2276.
[10] R. 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.
[11] F. Schneider, B. Ager, G. Maier, A. Feldmann, and S. Uhlig. 2012. Pitfalls in HTTP traffic measurements and analysis. In *Int. Conf. on Passive and Active Network Measurement*. Springer, 242–251.
[12] M. Vigo and S. Harper. 2013. Challenging information foraging theory: screen reader users are not always driven by information scent. In *Conf. on Hypertext and Social Media*. ACM, 60–68.