

“I’m Stuck!”: A Contextual Inquiry of People with Visual Impairments in Authentication

Bryan Dosono
Syracuse University
bdosono@syr.edu

Jordan Hayes
Syracuse University
jhayes05@syr.edu

Yang Wang
Syracuse University
ywang@syr.edu

ABSTRACT

Current authentication mechanisms pose significant challenges for people with visual impairments. This paper presents results from a contextual inquiry study that investigated the experiences this population encounters when logging into their computers, smart phones, and websites that they use. By triangulating results from observation, contextual inquiry interviews and a hierarchical task analysis of participants’ authentication tasks, we found that these users experience various difficulties associated with the limitations of assistive technologies, suffer noticeable delays in authentication and fall prey to confusing login challenges. The hierarchical task analysis uncovered challenging and time-consuming steps in the authentication process that participants performed. Our study raises awareness of these difficulties and reveals the limitations of current authentication experiences to the security community. We discuss implications for designing accessible authentication experiences for people with visual impairments.

1. INTRODUCTION

Logging into a website with usernames and passwords (i.e., authentication) is an essential part of users’ everyday Internet activities. However, this mundane operation can be daunting for users with disabilities. While many users can input a username and a password (their “login credentials”) to verify their online identities with relative ease, users with disabilities contend with challenges that may prevent them from experiencing a straightforward login process. In this paper, we focus on users with visual impairments. We seek to illuminate their challenges to portray the experiences of these users and raise awareness of current technology limitations that may inhibit them from taking full advantage of these technologies.

We conducted a contextual inquiry to understand the difficulties users with visual impairments encounter when using their computers, mobile phones, and the Internet. Our participants reported their experiences and opinions using different authentication mechanisms, such as passwords and biometrics. Participants experienced the most difficulty

authenticating due to inaccessible design within the systems they were using. We found that many websites bury their authentication forms beneath cluttered graphics, flash advertisements and a myriad of other web elements. Encountering these unnecessary elements further prolonged their ability to successfully locate the authentication area on a webpage. Assistive technologies like screen readers offered limited options for users to receive appropriate feedback regarding the degrees of accuracy and success when entering in their login credentials.

These system limitations significantly inconvenience users with visual impairments. They lead participants to experience significant lags and frustration when attempting to authenticate to the services they enjoy when using their computers. As a result, users are required to explore several alternative strategies such as using keyboard shortcuts to navigate their way around cluttered website designs to compensate for poor design.

This paper makes three main contributions. First, we discover specific difficulties users with visual impairments experience in a wide range of authentication scenarios as well as how they mitigate these challenges. Second, we reveal limitations of current authentication systems. Some of these limitations were related to web accessibility issues, which, to our knowledge, have not been systematically examined in the context of authentication. Third, we provide concrete recommendations towards making authentication experiences more accessible.

2. RELATED WORK

Authentication ensures that users are who they claim to be. There exist numerous types of authentication mechanisms in use within today’s security systems. Research and development in identity management [1] categorize modern authentication schemes into three main types: knowledge-based, token-based and biometric authentication systems. Each authentication scheme comes with its strengths and weaknesses. At the moment, however, no single authentication method satisfies the needs of all users, especially considering the wide range of conditions that users may have.

Cassidy et al. researched haptic ATM interfaces for assisting visually impaired users and reported that audio-assisted systems reduce users’ awareness of environmental sounds, meaning that users are less likely to hear someone come up behind them, which increases their vulnerability to

Copyright is held by the author/owner. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee.

Symposium on Usable Privacy and Security (SOUPS) 2015, July 22-24,

potential attackers [2]. Braille labels and keyboards provide limited tactile feedback to blind users due to the small density of information they can encode [3]. While this is true, not all users with visual impairments utilize Braille or know how to use it well [4]. Emerging technology, such as brain computer interfacing systems, are highly dependent on outside factors such as background noise and the health condition of the individual user [5]. Due to the delicate balance between usability, accessibility, and security in designing authentication systems, adding one modality to user interfaces may affect their usability and can increase the resulting complexity of these systems [6].

A number of papers related to accessible authentication research examine the needs of authentication and proposed technologies to support blind users [7]. In Azenkot's study of 13 blind smartphone users, most participants were unaware of or not concerned about potential security threats [8]. Ahmed et al. conducted an exploratory user study with 14 visually impaired participants to understand how new technologies such as Google Glass may be able to help protect their privacy [9]. The findings of this study show that forced dependence on others, especially strangers was a reoccurring privacy risk. Although low-cost wearable and mobile computing are likely to drive even more advances in accessible authentication [11,15], the unique privacy and security needs of blind users remain largely unaddressed.

Visually impaired users run into problems when interacting with the web. Borodin et al. highlights browsing strategies that they observed screen reader users employ when faced with challenges, ranging from unfamiliar web sites and complex web pages to dynamic and automatically-refreshing content [12]. However, they have not attempted to quantitatively evaluate the effectiveness of employing these strategies. User interface design for effective security remains an ongoing problem [13] and current authentication schemes are not usable enough for those with vision impairments. Relating tactics to technical problems and coping situations allows researchers to understand how users with visual impairments manage undergoing problematic situations [14]. For example, audio CAPTCHAs (Completely Automated Public Turing test to tell Computers and Humans Apart) were introduced as an accessible alternative for those unable to use more common visual CAPTCHAs. A study of more than 150 participants demonstrated that existing audio CAPTCHAs were more difficult and time-consuming to complete compared to visual CAPTCHAs for both blind and sighted users [15].

We did not find any empirical studies investigating concrete challenges and difficulties in authentication for users with visual impairments. In response to a dearth of literature that documents computer and web authentication experiences of these users, our work shares in-depth accounts from the perspective of participants through a contextual inquiry approach. These users shed novel insight into the various types of authentication challenges that designers and

developers should consider and address in creating accessible authentication experiences.

3. METHODOLOGY

3.1 Contextual inquiry

To understand how people with visual impairments use computer systems and authentication mechanisms in their natural environment, we adopted a contextual inquiry approach by which we visited participants at places where they regularly used computers or mobile devices (e.g., home, workplace, public library). This approach consists of three main components of gathering qualitative data [16]. First, researchers observe and talk with users in the settings where they perform their everyday tasks. Second, researchers establish a mutual understanding with the user to examine the topic at hand. Acknowledging the user as the expert clarifies that the researchers did not come to solve problems and answer technical questions, which saves the researchers from misinterpreting actions [17]. Third, researchers guide the contextual inquiry on a clearly defined set of participants' concerns, allowing room for conversation to extend beyond a list of specific questions.

We began our contextual inquiry with a semi-structured interview by asking participants a series of questions to understand their computer and Internet use as well as their knowledge and perception of authentication systems. We then asked them to perform a set of authentication tasks. We first asked participants to log into their computer, second their primary email account, third their online banking account or an e-commerce site they use, fourth their social media network of choice and fifth their mobile phones. These tasks were chosen because they cover a diverse set of common authentication scenarios. We also told participants that they could skip any of these tasks if they do not feel comfortable. We encouraged participants to think aloud during these tasks. We audio and video recorded how they performed these tasks with their permission. We conducted each study session with at least two researchers: one leading the study and another taking notes and recording the session. To protect their privacy, we turned the camera away from the keyboard and focused the camera on the device's screen any time they logged in with their credentials. We did not ask them to reveal their usernames and passwords to us during the study. The script we used for each session is included in the Appendix (Figure 7). Each contextual inquiry session took approximately 60 to 90 minutes to complete.

We compensated participants with \$30 in cash. We also rewarded participants an additional \$10 payment for any extra referrals that completed the study. Our Institutional Review Board (IRB) approved the study.

Table 1: Demographic information of participants and their measured time of logging into various domains of authentication.

Participant Characteristics						Timed Attempt at Authentication in Seconds					
ID	Age	Sex	Occupation	Self-description	Assistive Tech	Computer	Email	Banking	Commerce	Social Media	Mobile Phone
P1	50-60	M	Librarian	Blind	JAWS	271	351	376	N/A	86	N/A
P2	40-50	F	Sales	Low Vision	None	N/A	65	N/A	62	40	192
P3	40-50	M	Instructor	Low Vision	ZoomText	78	123	N/A	N/A	N/A	N/A
P4	50-60	M	Banker	Blind	JAWS	12	49	N/A	N/A	N/A	N/A
P5	50-60	M	Retired	Blind	JAWS	N/A	215	N/A	N/A	N/A	N/A
P6	50-60	M	Veteran	Low Vision	ZoomText	229	67	N/A	N/A	N/A	N/A
P7	50-60	F	Retired	Blind	JAWS	N/A	127	58	400	N/A	N/A
P8	50-60	M	Sales	Blind	JAWS	396	37	N/A	223	N/A	10
P9	50-60	F	Instructor	Blind	JAWS	154	11	263 (failed)	N/A	N/A	10
P10	50-60	M	Retired	Blind	JAWS	164	39	N/A	N/A	N/A	N/A
P11	50-60	F	Instructor	Blind	JAWS	33	33	308 (failed)	129	N/A	5
P12	50-60	M	Lawyer	Low Vision	JAWS	254	43	N/A	N/A	N/A	8
Mean						177	97	316	174	63	54
Median						164	57	308	129	63	10
Std. Dev.						124.4	98.0	56.9	142.7	32.5	92.2

* Note: N/A (not applicable) indicates that the participant does not own either a relevant device or an account to authenticate.

3.2 Participant recruitment

From May to July 2014, we recruited 12 participants who self-described as having a visual impairment, including eight blind users and four with low vision. We conducted all study sessions face-to-face. Table 1 describes their demographics. In summary, eight males and four females with an estimated age range of 40-60 volunteered to participate in the study. Three participants reported being retired while eight reported they were still employed and one reported being a veteran. Nine participants used the JAWS (Job Access With Speech) screen reader as their preferred assistive technology while two used ZoomText and one participant did not use any assistive technologies at all. We reached a point of saturation where no new themes emerged after our tenth contextual inquiry session. The remaining two participants confirmed the results.

We recruited participants in the Syracuse, NY metropolitan area via online discussion boards, mailing lists, flyers, YouTube videos, online advertisements and newsletters affiliated with local disability organizations. We also volunteered in local events to gain familiarity with local disability communities. Due to the nature of the study, we found recruiting participants a challenging task. In this vein, we recruited ten of our participants via word of mouth and relied on snowball sampling techniques to recruit from among their acquaintances. We directed potential participants to a recruitment survey that asked respondents to self-describe their disability statuses and we then selected respondents accordingly (see Figure 5).

3.3 Content analysis

We analyzed data collected from each participant by reviewing from each session the transcribed interview and video observation components. We segmented each

transcript according to the various parts of the contextual inquiry and proceeded to develop an open coding scheme to generalize the key findings each participant contributed to the study using a grounded theory approach [18]. Seeking to highlight difficulties most salient to authentication, we probed into the various opinions, common practices and difficulties participants encountered when logging into their accounts; their reasons for or against password-protecting their computers and other accounts they used; whether or not they automatically save their login credentials; their willingness to give their login credentials to others; the mental models they conceptualize when creating personal usernames and passwords; their general difficulties using computers and navigating the web and difficulties they encountered when performing the tasks of logging into the computers and accounts they use.

We developed approximately 15 qualitative codes to summarize the most relevant findings we learned from each participant, which we clustered into sets of high-level themes. We also timed attempts of all authentication tasks to get a sense of how time-consuming they were for each participant (see Table 1). Not all participants performed every task as some of them did not use social media or own a mobile phone. We also reviewed videos captured of each participant and noted the actions they took, the visual output observed on the device interface and any voice feedback from assistive technology.

3.4 Hierarchical task analysis

We recorded participants' responses in both audio and video formats with their permission, cleaned up and organized notes from observations and interviews, transcribed audio recordings, coded qualitative data for inductive content analysis [19] and grouped reoccurring themes.

Table 2. Summary of difficulties when participants performed the login tasks, including the source of each difficulty, the average amount of time taken by each participant, and the total number of occurrence for each difficulty.

ID	Difficulty	Source of Difficulty	Average Time (seconds)	Standard Deviation	Total Occurrence
D1	Locating the authentication area on a web page	Accessibility	87	92.1	13
D2	Determining if another user is already logged in on a shared computer	Authentication	133	0.0	1
D3	Waiting for screen reader output to either start or finish speaking in order to find desired information quickly	Accessibility	35	25.3	72
D4	Attempting to verify successful authentication	Accessibility & Authentication	79	49.0	3
D5	Entering passwords correctly due to design of screen reader software	Accessibility & Authentication	14	4.9	2
D6	Receiving insufficient audio feedback from JAWS about error messages	Accessibility	89	33.8	3
D7	Proper finger placement over fingerprint recognition system	Authentication	11	0.0	1
D8	Determining if mobile browser successfully stored login credentials	Authentication	16	0.0	1
D9	Encountering unexpected distractions (i.e. pop-ups, dialog boxes, new windows) while attempting to authenticate	Accessibility	33	0.0	1
D10	Answering security questions correctly	Accessibility & Authentication	166	0.0	1

While analyzing the data following the contextual inquiry process, we noticed some participants who failed to complete some of their login tasks or took a relatively long time to complete them (see Table 1). To help pinpoint which aspects or steps of the authentication process that are time-consuming and/or challenging, we conducted a hierarchical task analysis [20] to identify the steps that were taken and what actually went wrong in those circumstances. For each authentication task, we began by watching the respective video and listening to the audio recordings to identify the steps the participant took to complete the task. We created a high-level task flow diagram from the steps we identified while reviewing the relevant parts of the audio and/or video recording. We then broke down the high-level steps in need of further analysis into one or more separate, more detailed flowcharts in the same diagram with the goal of outlining the specific sub-steps the participant took to complete the higher-level steps. To triangulate different sources of data, we included example quotes and comments from the observation notes and interview transcripts that were relevant to the sub-steps. We also noted the time, in seconds the participant took to complete each step and sub-step on the diagram to understand how time-consuming they were. A few example task flow diagrams are included in the Appendix (Figure 7).

4. RESULTS

By triangulating data from the observations, interviews, and task analysis, we identified a number of difficulties (see Table 2) our participants faced in their authentication experiences. Furthermore, our findings show most of these difficulties can be attributed to a general lack of knowledge and experience of the websites and assistive technologies (e.g. screen readers) they are using, as well as the way in which web designers and software developers have implemented such technologies. Next we discuss these difficulties in detail.

4.1 Locate or identify login elements on page

Participants expressed confusion and frustration over where to find the appropriate area on a web page to log into their accounts. We found this process to be significantly time-consuming and hinder participants' abilities to access the secure services that can only be accessed via successful authentication. P1 felt that websites should be designed to include the most critical information, such as the login area on the top of the page in order for users to quickly access relevant information as soon as the page loads. Results of the hierarchical task analysis also revealed that P7 struggled the most while attempting to identify the area she needed to authenticate into the PayPal website (See Figure 7E in Appendix). She completed this step in 73.5 seconds. P7 was unsure whether she needed to find a link or button to log in, describing her actions and explaining her confusion by saying: "I didn't know it was a button. I thought it was a link, so, that's the trick. If you, if you don't find it one way, you look for it another way." Her resourcefulness showed her ability to adapt to different web interface environments and use alternative methods if her original plan does not work successfully. P7's PayPal task shared similar characteristics with her email task as well as P1's email task in that all three tasks involved spending the most time locating the login area. She depended on using a keyboard shortcut to list all of the links on the page in her email task helped her identify the clickable and interactive webpage elements. She relied on past visits to the website to find the authentication area as a link and then was confused as she realized the login element was actually a button. P7 used her instinct to try and find any authentication-related links and was puzzled as to why she couldn't find any. For example, she became perplexed while locating links beginning with the letter 'L' but no links saying 'log in': "No, that's not there, either...oh, let's see..." Furthermore, P7 expressed the same frustration while failing to find any links beginning with the letter 'S' related to 'sign in': "it's not here, I don't know why not."

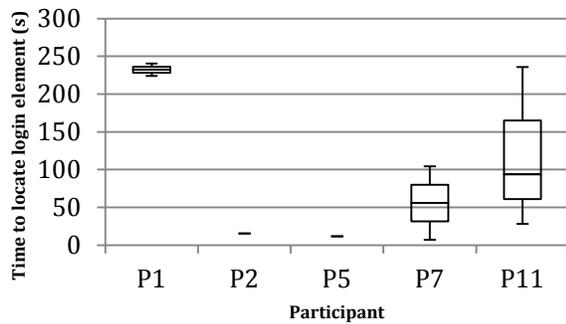


Figure 1: The distribution of time participants spent while attempting to locate the authentication area on a page. All other participants either did not complete certain tasks, or they completed the tasks but did not need to locate the authentication area (e.g., log into a computer), or no video recordings were available to depict them performing such tasks, and therefore are not shown on this graph.

Participants expressed confusion over which “Sign In” or “Log In” buttons or links to use because multiple buttons or links of the same type are placed on one web page. P11 entered the URL of the bank directly into the Google search bar, as opposed to entering search terms. P11 spent the most time struggling in an effort to identify the sign-in link for her bank’s website on the Google search results page. Each attempt to locate her bank’s “Sign In” link from the Google search results page took 140.5 seconds and 100 seconds respectively to complete, totaling 240.5 seconds. Both of P11’s attempts to find this link produced no luck. She may have unintentionally skipped the link as the speech output reported, *“this browser does not support inline frames”* right before announcing its existence of the link. P11 cut off the second word and continued to press the Down Arrow key to sift through the rest of the search results without catching it.

During her second attempt, she became more frustrated as she continued down the search results page, still not being able to find the desired link: *“Come on...why doesn’t it ask me to sign in? It wants me to get into the Rewards thing, you know? I’ve gotta find out...”* P11 continued to express disgruntlement during her second attempt as the screen reader identified every other link belonging to her bank’s website except for Sign In: *“wants me to follow on Twitter, and yada, yada... [sighs]... Yep, they’ve changed this. Uh, let’s see.”* P11’s failure to successfully authenticate into her online banking site can also be attributed to confusion over both the layout of the search results as well as which service she was actually logging in to use. She frustratingly skimmed through the search results after encountering an unfamiliar link and noticed, *“they must have changed the way it was set up since I last used it.”* P11 found a “Sign In” link on the page, which she perceived to be that of her online banking site, yet in reality the link directed her to a Google Account settings page. She realized this upon hearing her screen reader prompt her to log into a different

service altogether with an account she does not have: *“I don’t understand. I should have an [online banking] account, not a Google account.”*

Participants spent an average of 96 seconds attempting to locate the authentication area of the web pages they accessed, as shown in Figure 1. The hierarchical task analysis results show that this step alone was the most time-consuming part of the authentication process for three participants: P1, P7 and P11. Not all participants are included in Figure 1 because some participants did not locate an authentication area on a webpage while performing their tasks or no video recordings were available for the research team to determine the completion time.

4.2 Logging in as another user

One participant struggled to determine whether or not another user was already logged into Gmail on the public library’s Dell desktop computer he was using before he could locate the authentication area (see D2 in Table 2). According to the hierarchical task analysis, P1 inferred that another user had previously logged into this computer. However, he needed to find the name of the other user to confirm and finally did so after frustratingly combing his way through the Gmail Sign-In page in an effort to locate the other user’s account: *“OK, there it is... so that’s her email.”* After finding the name of the other user, P1 then struggled to find the button he needed to log into his own account because he was unsure of the terminology used to describe the login area: *“sometimes it’s ‘log in as another user’, sometimes it’s ‘sign in as another user’, sometimes it’s ‘change user’.”* He feels constantly changing the terminology of login elements introduces a new learning curve regarding how to locate the authentication area quickly and efficiently: *“unfortunately, this is somethin’ that we run into a lot, is, you don’t know what they call things, and every time they update the website, you have to re-learn how to do it.”* Standardization of terminologies would greatly aid users of screen-reader technology.

4.3 Delay in finding necessary information

By default, screen readers such as JAWS read contents of a web page in a linear fashion, beginning with text located at the top and then gradually moving down to the bottom of the page. Websites are generally designed with authentication forms placed closer to the center of the page beneath a considerable amount of graphics and text. This practice posed a significant challenge to participants who depend on screen readers to access the information they need quickly. Users with visual impairments are further impeded from efficiently accessing the authentication area they are attempting to locate because they must weave through a complex layout of webpage elements to access the login form.

We found our participants used an array of keyboard shortcuts to cut down on the time waiting for screen readers

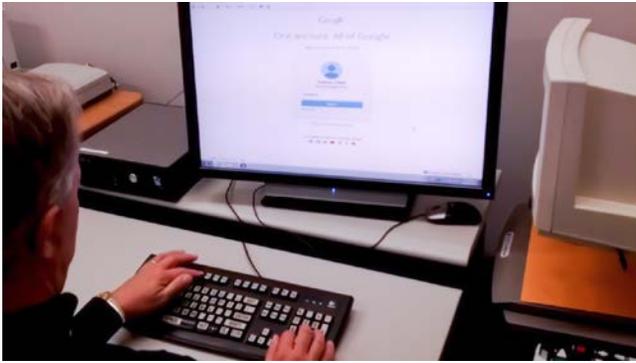


Figure 2: P1 diligently continued to troubleshoot through an authentication error by finding an alternate way to log into his email account using a variety of keyboard shortcuts.

to identify the information they need (as illustrated in Figure 2). However, these shortcuts do not always work for them and can sometimes lead to additional obstacles inhibiting their ability to authenticate.

According to the hierarchical task analysis results, participants spent an average of 39 seconds waiting for the JAWS speech output to start speaking, finish reading all the elements on a web page or both as shown in Figure 3 and D3 in Table 2. This waiting period significantly added to the total completion time of each task. For example, P7 took the most amount of time just waiting for JAWS to read the information she needed to perform the necessary steps to log into her PayPal account (see Figure 7D in Appendix). While waiting for the PayPal page to load after entering the URL, P7 waited and listened for the presence of any buttons, links or text. After she entered the URL into the Open dialog box in the Internet Explorer browser, the JAWS output read: “Search the catalog,” indicating the

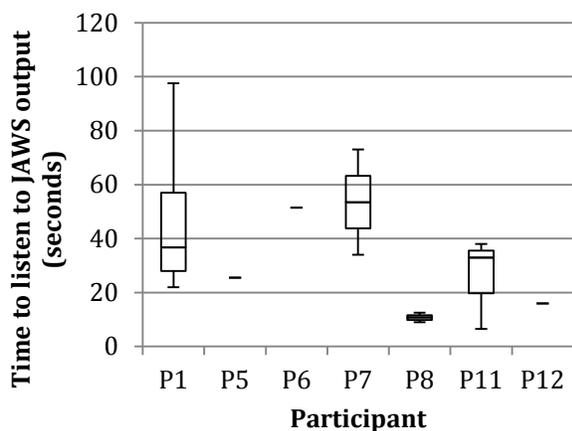


Figure 3: The distribution of time participants spent either waiting for their screen reader to begin speaking or listening to their screen reader finish reading web page elements aloud. All other participants are not shown in this graph because they did not use a screen reader when performing their tasks or no video recordings were available.

browser had not left the home page yet. P7 then indicated the page was taking a little extra time to load than usual: “OK, it hasn’t loaded yet...should load.” She eventually remarked: “Oh, we are loaded” after pressing multiple keyboard commands to obtain information from the screen reader, confirming she was now on the PayPal home page. This entire process lasted for a total of 25 seconds.

4.4 Verifying successful authentication

Three participants were uncertain about whether their authentication attempts were successful (see D4 in Table 2). They searched for specific web elements or textual cues to infer their authentication status. The results of the hierarchical task analyses showed that P11 attempted to authenticate into Amazon and encountered account management links usually associated with post-authentication activities that are present even if users are not logged in at all. Some of these links, for example included “Your Account,” “Manage Your Content and Devices,” “Manage Your Cloud Subscriptions,” “Your Games and Software Library” and “Your Watch List.” This process of locating the “Sign In” link from the search results after typing the URL into the Google search bar took her 56 seconds to complete. P11 was confused as to why there was no “sign in” link in the search results and assumed Amazon had already recognized her credentials: “See, it put me already right into, uh... this isn’t helping you, because it must have remembered my password, which I was very willing to enter in.” She was unsure when the screen reader announced a link in the Google search results that she heard called “Try Prime Cart” (this is actually a combination of two links, one inviting users to evaluate Amazon’s premium subscription content service called Prime and another for the user to manage his/her shopping cart) after hearing the “Shop by Department,” “Sign In” and “Your Account” links. P11 curiously selected the link to find out what it was but continued to stray further away from her desired destination: “‘Try Prime Cart’? I don’t know what that is. Let’s see.” From the Amazon pages, she continued to express frustration and confusion as she encountered unnecessary links for managing her Amazon account such as “Your Amazon Music Settings,” “Your Video Library” and “Your Games and Software Library,” rather than ways to authenticate into the website: “I don’t want that right now. I wanna sign in for you.” P11 ultimately gave up her attempt at authenticating into Amazon, expressing her ultimate confusion as to why she couldn’t successfully log in: “I don’t know why I’m not getting into the ‘Sign In’ thing.”

P1 did not encounter any account management links associated with post-authentication, but was unsure whether he successfully authenticated into Gmail after eventually finding the fields necessary to do so. He inferred successful entry of his login credentials when he browsed around the user interface of the actual Gmail client. When P1 found his email address on the Gmail page after submitting the login form confirming successful authentication, he expressed:

“Yes, it did. It logged me in.” This entire process took him 24 seconds to complete, which added to the total completion time of 351 seconds for this task.

P7 shared similar difficulties along with P1 in terms of self-validating her successful attempt at logging into her PayPal account (see Figure 7F in Appendix). This step took the longest for P7 to complete, totaling 118.5 seconds. She attempted to locate her name on the page that loaded after entering her credentials and remarked about the amount of time taken to find the information she desired: *“huh, that’s not what I want...must take a while to load. Sometimes it does.”* When failing to find her name on the screen, P7 gave up on her own efforts and asked the research team to confirm for her whether or not she had successfully completed this task. She asked to start over before making a decision whether or not to actually repeat the process of authenticating into PayPal, which she ultimately decided against, since Researcher 2 had notified her of a successful login. Unsure of this fact, P7 asked him a second time and Researcher 2 again reassured her successful login.

4.5 Limitations of assistive technology

4.5.1 Password masking

Our users depended on JAWS to assist them with using their computers to navigate through elements on any given web page. However, these screen readers did little to ameliorate their authentication experiences (see D5 in Table 2). For example, P1 expressed frustration at how JAWS verbally concealed passwords as he and other users he assists type them into the field: *“[As a librarian], I show the public how to log into websites and how to do searches, and they’re sure that they’ve typed it in right but all they hear when they type is the screen reader say ‘star, star, star,’ so they don’t know if they hit the wrong key, or if the caps lock key happened to be on or something. They don’t know.”*

This design choice was purportedly made to prevent shoulder surfing attacks (i.e., someone standing next to the user and overhearing the password). However, P1 had no way of confirming whether or not he correctly typed in the password until either a verification or error screen propagated from the field submission. To accommodate for this difficulty, P1 suggested the following design modification of screen readers such as JAWS: *“Give people options. If they want to mask the password, then they can choose to do that, but if they don’t want to, if there was a checkbox that you could check and say, ‘don’t mask the passwords for me logging in,’ so then you could hear it and know if you did it right or not. That would make it easier.”*

4.5.2 Lack of feedback using case-sensitive passwords

One participant was also mystified when trying to determine the correct capitalization for entering in case-sensitive credentials. The confusion contributes to whether or not users mistyped their usernames and passwords. P3 expressed uncertainty in figuring out whether or not she

enabled the caps lock function on her keyboard. Even though she activated ZoomText, an accessibility software application that enlarges everything displayed on a computer screen with increased clarity—to assist her with navigating her computer, the screen reader portion of ZoomText does not indicate to her the case of the letters she typed. P3 is concerned about her uncertainty when entering in her passwords: *“I’ll try two or three times. Sometimes, I’ll lock myself out, ‘cuz I don’t see that right away.”*

4.5.3 Lack of screen reader output for error messages

Participants experienced the most difficulties when attempting to log into their computer systems because they were unaware of an error message that obstructed them from successfully authenticating into these systems (see D6 in Table 2). For two participants, JAWS provided no speech output when the error message appeared on the computer screen. P1 had attempted to enter his credentials and received an error message from Windows stating one or both of his credentials were incorrect. He was unsure of whether or not he was successful after hesitantly entering his password while attempting to log into the computer’s Administrator account. He does not normally sign in and out of this computer on a regular basis because the computer he was using is programmed by the IT department to log into Windows automatically upon initial boot-up. While anticipating the available users to appear after initiating the “Switch user” command on the Windows Start Menu, P1 remarked: *“Now, I’m waiting...sometimes the screen reader program reads the new screen automatically, sometimes it doesn’t.”* As the screen reader indicated the Administrator account was currently selected, P1 confirmed this: *“Now that said ‘Administrator account.’ Let’s see.”* After prompting him to enter his password, the screen reader he was using did not read this error message aloud. P1 was unsure what to do because of the silence created from the lack of audio feedback: *“It’s not talking to me. So I’m waiting. I’m sitting here thinking, ‘OK.’ Either it’s gonna do something in a few seconds or it’s not’, but I don’t know.”* He then desperately used various keyboard shortcuts to elicit some response from the computer, but this trick did not work: *“I haven’t got any...it’s not talking to me.”*

P1 wondered whether the computer logged in or if something went wrong: *“So at this point, I don’t know if it switched or not.”* He then asked the research team for assistance: *“if you can see, but the screen’s on, right?”* He continued to express confusion and began to explore alternate methods of solving his problem by saying, *“So I don’t know if that worked. So what I would have to do then would be start over, unless you can see something else for me to click on there.”* P1 attempted to log in again after shutting down and restarting his computer. This second attempt was successful and did not require him to enter in any login credentials because the computer automatically logged in and loaded the Windows desktop. P1 remarked about making this computer as accessible as possible for

anyone who uses it by simplifying the authentication process: “We have such a variety of users that our technical staff tried to streamline things and so they write this little automatic login just for the boot-up part.” Researcher 2 confirmed successful login as did P1, who noted the JAWS output: “so the screen reader started automatically.” The presence of this initial speech output indicates the computer successfully bypassed the Windows login dialog and loaded the Windows desktop. Each restart attempt took 150 seconds and 83.5 seconds, respectively to complete.

P8’s case was similar to that of P1, except he used a fingerprint recognition system to log into his Lenovo laptop computer, attempting to do so eight times before ultimately giving up and authenticating using his username and password instead. This fingerprint-based authentication attempt took him 88 seconds to complete. For a few attempts, he had to take the time to position his finger over the fingerprint reader and was not sure whether or not his first swipe registered. He pointed out: “well, it didn’t do it yet” after not receiving a response from the computer. P8 seemed to become more frustrated after the following unsuccessful attempts and began to wonder whether or not his placement over the fingerprint reader was a contributing factor to this (see D7 in Table 2): “I might not be touching it in the right place. I’m never quite sure where to touch it.” P8 continued to express his utmost frustration after three more attempts as he lowered his head, sighed, grunted and explained: “See, it isn’t responding. But if it had...didn’t seem to respond. I wonder why. It, maybe, I don’t think it’s forgotten it.”

The computer did respond after every attempt P8 made to swipe his finger and authenticate, yet this response was an error message displayed on the screen that P8 was not able to see due to a lack of any notification from JAWS. While our video recording did not capture the error message text, it is very likely that the error message returned a visual notification to the user that the computer could not recognize his fingerprint. The error message appeared on P8’s computer screen 3.5 seconds after his first attempt and remained there for all attempts following. In addition, a second error message appeared on top of the existing message after four (non-consecutive) attempts and disappeared a few seconds later. JAWS did not provide any speech output as those two messages popped onto the screen and therefore P8 was unaware of such a notification.

Usually, he would power up his computer and JAWS starts up just after the operating system loads and just before the Windows logon box appears on the computer screen. The screen reader announces, “JAWS for Windows is ready,” indicating to P8 the machine is ready for authentication. The screen reader provided him with this notification on start-up, but did not give any feedback during his attempts to authenticate using his computer’s built-in fingerprint reader. When attempting to log in using text-based credentials, JAWS notified P8 of successful startup and

automatically positioned the cursor at the password field since his username had already been filled.

One participant took advantage of password-saving mechanisms like auto-fill features on common Internet browsers. P2 voiced an issue associated with keeping track of multiple credentials: “It’s kind of a pain because I have to remember all these passwords.” There were times when P2 was concerned this browser-saving trick would not always work. P2 used one to help her keep track of her password for the business she manages online. She felt concerned if the browser did not remember her credentials but was ultimately relieved to discover the browser had indeed remembered them (see Figure 4 and D8 in Table 2): “Let me see. Oh, it does remember me!” If this were not the case, she may not have been able to log in because she said she was unsure she could remember them herself. In the event the password manager had failed to remember her credentials, P2 referenced alternative password recovery mechanisms, making small modifications to the same base password to create a new one. She used this strategy to her advantage in the event of a forgotten password, sometimes making attempts at a login area to crack her code. She limited the number of times she attempted this stunt in an effort to prevent sites from locking herself out after a number of unsuccessful attempts.

4.5.4 Difficulty with password recovery mechanisms

Other participants we observed showed the most difficulty using screen readers to recover their login credentials in case they lost or forgot those they originally created. P7 provided the most prominent example of this, explaining how screen readers were not always capable of reading new passwords provided by the system via email after attempting to reset her login credentials. P7 referred to instances outside the authentication tasks in our study where she clicked the “lost/forgot password” link on websites. She further explained how users must request assistance from elsewhere to obtain the necessary information: “You’re not always able to get the information on the screen, and you have to get somebody to come in and read you the temporary password. You know, ‘H-J-3-9-4-8-

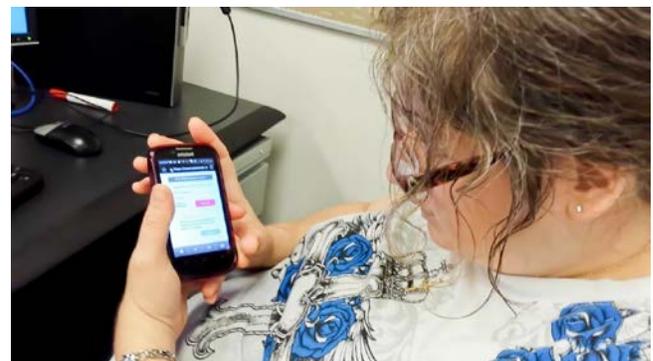


Figure 4: P2 expressed relief when finding out her login credentials were successfully saved into her small business account when using her mobile phone’s browser.

4-9-6-9-1,' etc., and then, you got to try to remember it." The entire process of asking others for help, remembering the characters they tell users and attempting to enter in those credentials takes additional effort and adds to the frustration of multiple login failures.

Another overlooked aspect of authentication systems involved the actual terms used to identify specific login credentials. Some users may not understand the difference between the meaning or purpose of a username and a password. P8 provided valuable insight into his mental model he used to distinguish between the two: "You know, if you called me 'ugly', you know, that would be a name, or 'handsome' or whatever name. So I'm never sure the difference between a user-name and a password. I guess a word is a name, but anyway, but that's my confusion about it." P8 went further on to clarify what would fit his definition of an appropriate password as he logged into his computer: "I could have said that, OK...if it was 'hound dog', that's a password to me." This distinction between usernames and passwords is an interesting way of looking at how most sites requiring these credentials may trap users who contemplate specific mental models of what credentials they tend to create for themselves and what each credential means to them personally.

4.6 Other unexpected distractions

During the authentication process, users with visual impairments may encounter additional obstructions that may further hinder their ability to log in either on the webpages or software applications they use (see D9 in Table 2). Navigating around these obstacles continues to add to the confusion and frustration users with visual impairments face. For example, P6 had attempted to locate his email client, which had already been logged in. However, when pressing the TAB key to navigate to the email client, he encountered a Dropbox software application, which was already open on his desktop PC. P6 expressed frustration to the research team about encountering this unexpected obstacle: "[sighs] I hate that. I actually only got into Dropbox somehow and I'm gonna turn that off." Since the research team analyzed this task using the audio recording, the presence of a "yes" or "no" button is unknown. However, upon downloading the Dropbox application and re-constructing this step, the research team can determine the existence of an "OK" and "Cancel" button with the cursor positioned over the latter. There was no mention from either JAWS or P6 regarding the outcome of completing this step. P6 eventually was able to continue and successfully get into his Juno email client. As his computer screen displayed a browser window associated with Juno, P6 can also infer he is where needs to be: "I think I'm back in my email." After pressing ALT + Tab two steps later, the computer screen displayed Juno's main window. P6 confirmed he had indeed accessed the client after hearing the JAWS speech output mention the name of the email client. The research

team verbally notified P6 he was automatically logged into Juno 4.5 seconds after he verbally confirmed it himself.

4.7 Hassles authenticating into mobile phones

Six participants owned a smartphone, but only two participants password-protect their devices. They disliked adding an additional layer of security to their mobile phones because most of them cannot see the keys or characters required to authenticate into them. For example, P3 owned an iPhone and used many of its accessibility features. However, when asked if she password-protected her phone, P3 stated: "No, it is not password-protected, and that's only because I can't see what's on the dim phone screen in bright areas. I won't be able to see it if I'm outside. Like, every time you get a text, you have to put your password in, I get confused." P3 felt she is at more of a security risk by not password-protecting her phone, referring to the potential risks associated with one of her children having his phone stolen. However, she must accommodate for her visual impairment when password-protecting her smartphone.

5. DISCUSSION

5.1 Reflection of key findings

Our findings illustrate the challenges participants face as a result of accessibility issues hindering them from successfully authenticating into the websites and services they use, while also shedding insightful light on these challenges. In addition, we highlighted the strategies they use to overcome them as reported in the literature we reviewed. We situate these challenges in the specific experiences our participants faced in order to provide novel awareness of how they contribute to the holistic authentication experience. The authentication experience involves numerous stakeholders in the process, all of whom play a significant role in users' efficient and timely access to the services and information they want and need. Finally, our results show that participants take a relatively long time to access the authentication area by struggling to find the login fields themselves and/or waiting for the screen reader to provide them with enough information to proceed. This is significantly longer than the average time taken by the general population to authenticate.

According to Table 2, four of the ten difficulties participants faced arose from general accessibility issues, while three derived from issues related to the underlying authentication mechanisms themselves. Three were associated with a combination of issues related to both. The most common difficulties include: screen readers failing to notify users of error messages; participants struggling to efficiently locate the authentication fields on a web page; participants expressing uncertainty when verifying their attempts to log in; and participants waiting an unnecessarily long amount of time for the screen reader to either start or finish reading webpage elements aloud. With the exception of waiting for JAWS to finish reading the webpage elements aloud and some aspects of inefficiently locating

the authentication area, these common difficulties mentioned above create significant barriers to accessing the areas of websites they use that require them to authenticate.

E-commerce websites such as Amazon providing account management links associated with post-authentication such as “Your Account” and “Your Orders” misleads users with visual impairments with a false sense of logging into their accounts. Users who click these account management links are taken to an authentication page where they are supposed to enter their credentials and submit the form. This compounds the frustrating task of finding their way to the website’s authentication mechanism for users with visual impairments because encountering the misleading post-authentication account management links before landing on a login page would trick these users into thinking they have already logged into the site when indeed the opposite is the case. Bonneau, et al. demonstrated how numerous aspects of password implementation lack standardization [21]. In our study, we did not look into actual password implementation, but we did find inconsistency regarding the names of login fields.

Our findings reveal key accessibility-related issues that create significant obstacles not reported in accessibility-related communities such as ASSETS. Additionally, no security literature discusses the difficulties we encountered in the context of authentication. We present this novel, insightful evidence in the form of difficulties that participants experienced in our contextual inquiry study. These difficulties directly impact authentication as well as directly relate to accessibility since these issues related to the design and implementation of web content render authentication systems nearly unusable by those with visual impairments, regardless of the level of security they may provide to their users. The security community must seriously consider these accessibility difficulties and contemplate how the empirical evidence we present here directly corresponds to the usability of authentication systems and mechanisms, similar to the way we critically examine key usability issues we feel relate to security. The most advantageous form of authentication is one that can both be utilized by and accommodate users of all needs, including users with visual impairments.

5.2 Sources of difficulties

5.2.1 Socioeconomic conditions

System designers need to be cognizant of the various socioeconomic hurdles that financially burden users with visual impairments, as they often cannot afford the latest technology on the market. Several participants in our study explicitly stated how they could only afford lower end models of electronic devices and services. In many instances, these devices and services either come with no accessibility support (e.g., a feature phone instead of a smartphone) or corporate providers discontinue support for legacy systems altogether (e.g., Windows XP). Thus, assistive technologies such as screen readers should be

backwardly compatible with older operating systems. Furthermore, screen readers such as JAWS are becoming more expensive to purchase. However, the availability of open-source screen reading applications such as Non-Visual Disabled Access (NVDA) is increasing in popularity. This provides reasonable means for users with visual impairments to access to the software they crucially depend on in order to operate their computers without sacrificing any necessary expenses. However, our findings show that none of the participants used any of these open-source screen readers.

5.2.2 Technical learning curves

All participants informed us of the sharp learning curves that came with using a screen reader for the first time. They expressed that it took a considerable amount of patience and practice to use assistive technology efficiently. Users must know which particular elements they want to find and determine their location in relation to their current point of control on the screen. This takes a great mental skill of trial-and-error and reasonable deduction using repetitive up-and-down-arrow keystrokes and actively listening to the auditory output JAWS provides. As a result of these technical learning curves, users with visual impairments may take a significantly long time to perform simple tasks using their computers.

5.3 Implications for design

Based on our findings, we propose four concrete suggestions to address the difficulties our participants faced when authenticating into the systems they use. First, we suggest web designers should improve accessibility to the authentication areas (i.e., login forms). Placing fields for credentials and submit buttons to an easier location on the page closer to the top or changing the code would allow screen readers to say where the login form is located. Placing only one sign-in element on a page at a time reduces the confusion of users locating their desired authentication field and removing any links referencing “your account” also reduces the possibility for users to enter a false sense of being logged in after encountering links associated with post-authentication and multiple points of authentication. Developers of web services should also provide confirmation messages to users with visual impairments indicating the success of their authentication attempts by creating a page or prompt simply stating whether or not users have successfully logged in, which can be launched immediately after users submit the login form on a page. Furthermore, we suggest screen reader developers add an additional keyboard shortcut allowing for users to immediately identify any authentication fields on the page, which immediately takes them to the authentication area. Finally, we suggest the introduction of web design standards regarding consistent terminology related to authentication mechanisms, which will reduce the amount of confusion users with visual impairments may face when trying to locate any authentication area on a

webpage. Doing this can potentially reduce this confusion and provide some stability across various websites.

Most of the difficulties we found specifically apply to users with visual impairments. However, some of our suggestions can also apply to the general population of users. For example, developing guidelines related to accessible authentication elements would allow users with visual impairments to quickly find the authentication fields they need while also reducing the time for sighted users to navigate through a cluttered page. A variety of users can also benefit from the concrete assurance from a confirmation page or message notifying them whether or not their login attempts are successful. Taking into account this notion of universal design allows web developers to address issues that may help one specific marginalized population of users overcome these difficulties while also making significant changes that will benefit all users.

Designers of assistive technology should include users with visual impairments as part of the design, evaluation and testing process. They should encourage users who are the most affected by their designs to test their prototypes themselves. This would allow those with visual impairments the opportunity to provide insightful feedback regarding the strengths, weaknesses and potential improvements that could be made. Actively involving users in the design, evaluation and testing process would allow them to better understand their needs and help influence future designs. At the same time, however, designers of assistive technologies as well as web designers should be aware of any security and privacy risks associated with any suggestions made by users with visual impairments before implementing them (e.g., using only security questions as suggested by some of our participants).

5.4 Considerations for alternative authentication practices

Our participants either used or commented on alternative authentication methods that they preferred over the traditional username/password scheme. However, these alternatives are not silver bullets, either.

5.4.1 Using password managers to remember login credentials

Participants can use password managers provided with their browsers to remember login credentials. This mechanism reduces the remembering of multiple sets of usernames and passwords. For example, P2 used one to help her keep track of her password for the business she manages online. If this were not the case, she may not have been able to log in because she said she was unsure she could remember them herself. She relied on browsers and other password-saving mechanisms to help reduce this burden. However, she may increase her vulnerability to hackers and cybercriminals and put herself at risk for identity theft if attackers target the master password. Even if the master password remains safe from such attacks, the original web passwords remain as vulnerable as before [22].

5.4.2 Using biometrics

In order to further reduce the frustration and confusion associated with conventional login systems, most of our participants expressed interest in seeing biometric authentication become more widely used by society. They perceived biometrics would reduce the need of memorizing and entering in their login credentials. P2 felt that authenticating into the systems she used would be easier if she could just *"put [her] hand up to the computer. It's going to know it's [her] and it's going to let [her] into everything."* Other users, such as P7, were more skeptical of using biometric authentication systems because they are *"starting in the wrong direction"* and will become more intrusive as this type of emerging technology evolves. She illustrated, *"Once something like that starts, everybody's going get a chip implant when they're born and they'll know where everybody is all the time."* P12 argues that biometric systems may not work for all users with disabilities, especially those whose natural physical traits have been replaced by artificial ones: *"It could be as simple as having no motor skills or having had your fingerprints damaged as a result of a fire or some kind of body injury. Or if biometrics becomes basically retina scans and somebody has prosthetic eyes, and same with biometrics using fingerprints and somebody has prosthetic limbs. That would be problematic. So you will always have to be able to design systems of authentication that account for the possibility that there will be a subset of the population that can't access everything through biometrics."* Using an ability based-design approach allows systems to adapt to users' needs rather than their disabilities [23]. We should build systems that use this approach so that we work upon users' abilities instead of their disabilities.

5.4.3 Using security questions

Typically, security questions are used as an additional layer of verifying users' identities after entering in their usernames and passwords [24]. They could also be used as a way to replace them as a set of authentication credentials. P7 suggested doing so as an alternative to using passwords for routine authentication. While she provided this alternative to simplify the authentication experience, employing this mechanism creates more security issues than using the conventional practice of using login credentials. For example, answering security questions just swaps out the need to remember one set of information for another (i.e. passwords as opposed to answers to security questions). In addition, security questions are mostly used as a secondary authentication scheme in password-reset situations where users attempt to answer them, and if successful, must enter a new set of credentials.

Screen readers do not mask answers to security questions, as they do for passwords. We observed P9 attempting to answer security questions when attempting to log into her online banking account and noticed JAWS speaking out her answers to the security questions. This poses significant risks to participants because others can use this additional

information to gain unauthorized access for fraudulent purposes if they successfully authenticate using these security questions. Supplementing usernames and passwords with answers to security questions ensures users are who they claim to be by providing the system with an additional layer of uniquely identifiable information. This practice, however does pose significant security risks as opposed to using login credentials to authenticate. Users may not easily remember the answers to the security questions they created after not using them in a long time.

5.5 Study limitations

We did not aim to report on a representative capture of all possible variations, but we rather aimed to gain a deeper understanding of analyzed cases. As we were only able to recruit participants who used technology, we did not study those who were afraid of using technology or those who refused to use computers altogether. Our study did not collect data of our participants performing authentication tasks captured from their browsing history. Most of our participants described themselves as living with blindness or having a visual impairment, therefore the generalizability of our findings to other types of conditions was limited. We note that most of our participants are 50 years or older, therefore the difficulties we observed might also be due to their age. It is difficult to disentangle the effect of their visual impairments with age as a confounding factor.

The timings of the authentication tasks that we reported are not intended to be a precise, quantitative measure of the exact amount of time participants took to complete each task as well as their various steps and sub-steps. Instead, these timings are intended to be indicative of which tasks or steps and sub-steps are relatively time-consuming for participants to complete. Calculating the time participants took to locate the authentication area reveals that certain steps are quite time-consuming for many participants, as shown in Figure 1. We note that the timings we measured could be affected by many factors related to individual participants such as their self-described conditions, skills, use of assistive technology, setting in which the computer is being used (i.e., shared public terminal vs. home machine), computer configuration including the hardware and software (i.e., browser) installed on the machine as well as previous knowledge and experience. Since participants sometimes spoke aloud describing what they were thinking or doing during the authentication tasks to the research team, the timings we measured might be longer than if they did not think aloud. Nevertheless, our evidence suggests that a few specific steps, such as locating login area and waiting for screen reader output are particularly challenging and for some users and need to be improved.

6. CONCLUSION

Current authentication interfaces are difficult to use for users with disabilities. This causes frustration and leads to insecure behavior. Our study provides a nuanced account of various difficulties these users encounter with

authentication. Our recommendations aim to inform future related research and authentication system design. As the security community actively creates new authentication mechanisms, they should take into account the various characteristics of users and potential challenges they may face. New authentication mechanisms should be fast to use and work well with assistive technologies such as screen readers. We hope the authentication community can use our study insights to make their authentication mechanisms more accessible.

7. ACKNOWLEDGEMENTS

The contents of this paper were developed under a grant from the National Institute on Disability, Independent Living, and Rehabilitation Research (NIDILRR grant number 90DP0061-01-00). NIDILRR is a Center within the Administration for Community Living (ACL), Department of Health and Human Services (HHS). The contents of this paper do not necessarily represent the policy of NIDILRR, ACL, HHS, and readers should not assume endorsement by the United States Federal Government.

We would like to thank our participants for sharing their experiences and insights. We also acknowledge Natã Barbosa, Huichuan Xia, Yun Huang, Kevin Du, Joon Park and other colleagues in the Social Computing Systems (SALT) Lab at Syracuse University as well as Markel Vigo, Mike Just, Jeffery Bigham, Amy Hurst, Aaron Steinfeld, Sonia Chiasson and anonymous reviewers for their feedback and help.

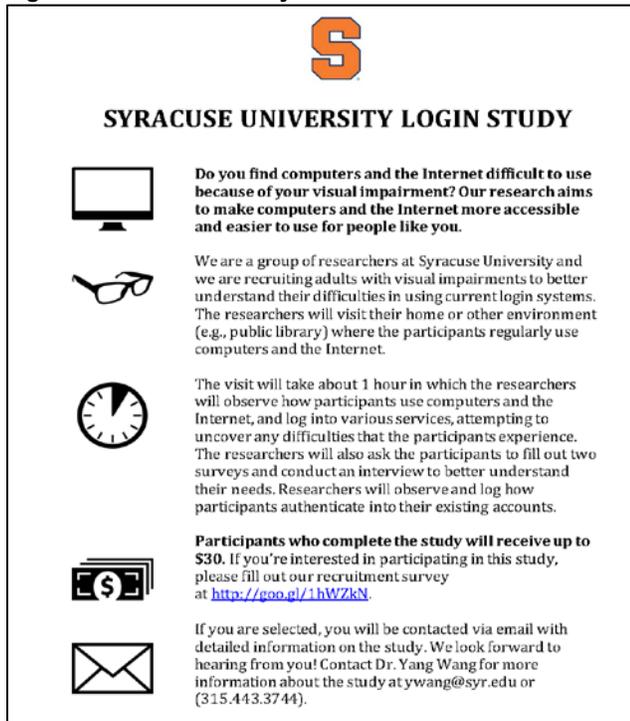
8. REFERENCES

- [1] L. Fritsch, K. S. Fuglerud, and I. Solheim, "Towards inclusive identity management," *Identity in the Information Society*, vol. 3, no. 1, pp. 515–538, 2010.
- [2] B. Cassidy, G. Cockton, and L. Coventry, "A haptic ATM interface to assist visually impaired users," *Proceedings of the 15th International ACM SIGACCESS Conference on Computers and Accessibility*, pp. 1–8, 2013.
- [3] K. Helkala, "Disabilities and authentication methods: Usability and security," *2012 Seventh International Conference on Availability, Reliability and Security*, pp. 327–334, 2012.
- [4] E. Murphy, R. Kuber, G. McAllister, P. Strain, and W. Yu, "An empirical investigation into the difficulties experienced by visually impaired internet users," *Universal Access in the Information Society*, vol. 7, no. 1–2, pp. 79–91, 2008.
- [5] G. Al-Hudhud, M. Abdulaziz Alzamel, E. Alattas, and A. Alwabil, "Using brain signals patterns for biometric identity verification systems," *Computers in Human Behavior*, vol. 31, pp. 224–229, 2014.

- [6] J. Holman, J. Lazar, and J. Feng, "Investigating the security-related challenges of blind users on the Web," in *Designing Inclusive Futures*, Springer, 2008, pp. 129–138.
- [7] N. Saxena and J. H. Watt, "Authentication technologies for the blind or visually impaired," *Proceedings of the USENIX Workshop on Hot Topics in Security*, p. 7, 2009.
- [8] S. Azenkot and K. Rector, "PassChords: Secure multi-touch authentication for blind people," *Proceedings of the 14th International ACM SIGACCESS Conference on Computers and Accessibility*, pp. 159–166, 2012.
- [9] T. Ahmed, "Privacy concerns and behaviors of people with visual impairments," *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 2015.
- [10] M. M. Haque, S. Zawoad, and R. Hasan, "Secure techniques and methods for authenticating visually impaired mobile phone users," *2013 IEEE International Conference on Technologies for Homeland Security*, pp. 735–740, 2013.
- [11] G. Kristin and B. Johansen, "e-Me Mobile: Accessible authentication for mobile devices Table of Contents," *Mobile Information Systems*, 2011.
- [12] Y. Borodin, J. P. Bigham, G. Dausch, and I. V Ramakrishnan, "More than meets the eye: A survey of screen-reader browsing strategies," *Proceedings of the 2010 International Cross Disciplinary Conference on Web Accessibility*, pp. 1–10, 2010.
- [13] A. Whitten and J. D. Tyger, "Why Johnny can't encrypt: A usability evaluation of PGP 5.0," *USENIX Security*, 1999.
- [14] M. Vigo and S. Harper, "Coping tactics employed by visually disabled users on the web," *International Journal of Human Computer Studies*, vol. 71, no. 11, pp. 1013–1025, 2013.
- [15] J. P. Bigham and A. C. Cavender, "Evaluating existing audio CAPTCHAs and an interface optimized for non-visual use," *Proceedings of the 27th International Conference on Human factors in Computing Systems*, p. 1829, 2009.
- [16] M. E. Raven and A. Flanders, "Using contextual inquiry to learn about your audiences," *ACM SIGDOC Asterisk Journal of Computer Documentation*, vol. 20, pp. 1–13, 1996.
- [17] K. Holtzblatt and S. Jones, "Contextual inquiry: a participatory technique for system design," *Participatory Design: Principles and Practice*, 1993.
- [18] A. Strauss and J. M. Corbin, *Basics of qualitative research: Grounded theory procedures and techniques*. Sage Publications, Inc., 1990.
- [19] Mayring, "Qualitative content analysis," *Forum Qualitative Sozialforschung*, vol. 1, no. 2, p. 10, 2000.
- [20] J. Annett, "Hierarchical task analysis," *Handbook of Cognitive Task Design*, pp. 17–35, 2003.
- [21] J. Bonneau, "The password thicket: Technical and market failures in human authentication on the web," *Information Security*, vol. 8, no. 1, pp. 230–237, 2010.
- [22] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," *IEEE Symposium on Security and Privacy*, pp. 1–15.
- [23] J. O. Wobbrock, S. K. Kane, K. Z. Gajos, S. Harada, and J. Froehlich, "Ability-Based Design," *ACM Transactions on Accessible Computing*, vol. 3, no. 3, pp. 1–27, 2011.
- [24] S. Schechter, a. J. B. Brush, and S. Egelman, "It's no secret: Measuring the security and reliability of authentication via 'secret' questions," *IEEE Symposium on Security and Privacy*, pp. 375–390, 2009.

9. APPENDIX

Figure 5: Recruitment Flyer



The flyer features the Syracuse University logo at the top. Below it, the title "SYRACUSE UNIVERSITY LOGIN STUDY" is centered. The flyer is divided into four sections, each with an icon and text:

- Icon:** Computer monitor. **Text:** "Do you find computers and the Internet difficult to use because of your visual impairment? Our research aims to make computers and the Internet more accessible and easier to use for people like you."
- Icon:** Eyeglasses. **Text:** "We are a group of researchers at Syracuse University and we are recruiting adults with visual impairments to better understand their difficulties in using current login systems. The researchers will visit their home or other environment (e.g., public library) where the participants regularly use computers and the Internet."
- Icon:** Clock. **Text:** "The visit will take about 1 hour in which the researchers will observe how participants use computers and the Internet, and log into various services, attempting to uncover any difficulties that the participants experience. The researchers will also ask the participants to fill out two surveys and conduct an interview to better understand their needs. Researchers will observe and log how participants authenticate into their existing accounts."
- Icon:** Money (dollar sign and dollar bill). **Text:** "Participants who complete the study will receive up to \$30. If you're interested in participating in this study, please fill out our recruitment survey at <http://goo.gl/1hWZkN>."

At the bottom, there is an envelope icon and text: "If you are selected, you will be contacted via email with detailed information on the study. We look forward to hearing from you! Contact Dr. Yang Wang for more information about the study at ywang@syr.edu or (315.443.3744)."

Figure 6: Contextual Inquiry Script

Introduction

Let me start by telling you a bit about this project and what we are trying to do. Our research team is trying to understand the challenges and difficulties that people with visual impairments face in using current authentication systems (e.g., logging into a computer or website). We want to understand your thought process so that we can develop technology that enhances current authentication systems.

We consider you the expert at so there are no wrong answers to any of our questions. While you answer questions or guide us through tasks, please focus on the details of how you actually log into your computer and online accounts. It may help to think about the last time you performed the task and explain it to us as if we are going to need to perform the task just as you did.

To backup my notes, I'd like to tape record our session. My research team will be the only users to listen to this. Are you okay with me recording the conversation? Thanks.

Please review and sign the consent form before we proceed.

Do you have any questions before we begin? Let's get started. (Make observations of the interviewee's work environment.)

Observation

I'll be observing you and when it won't disrupt your flow, I'll stop you when I see something interesting and ask questions. Or, I'll wait until there is a break or talk to you

between tasks. I'll also share my observations so you can tell me if I really understand what you do.

So, let's start by getting a bit of an overview of what you do that involves authentication systems. Keep in mind that although I will be making observations about your log in activities, I will not be recording your passwords nor will I be watching what you type in password fields. Please think out loud and verbally guide me through your thought processes and actions.

- Can you please turn on/restart your machine and walk me through how you log into it?
- Is your computer system password protected? Why or why not?
- Do you face any challenges with logging into your machine? For example, do you frequently forget your username or password, enter one or both incorrectly and don't know what to do about it?
- How frequently do you change your password? When was the last time you changed it?
- Describe your thought processes as you change your usernames and/or passwords or create new ones. Do you have any particular strategies for creating your usernames and/or passwords? If so, please describe them.
- Who knows this password? Is it just you?

Let's go over any of the collaboration and coordination tasks you have to do. I'd like you to go over with me what you do on your computer on a daily basis. Let's first see how you check your email. Again, please think out loud and verbally guide me through your thought processes and actions.

- Do you use any desktop icons or browser bookmarks to access your email client?
- If so, do you find these shortcuts convenient for you? How so?
- Do you have your passwords automatically saved on your email client, or do you manually enter your password each time to check your email?
- Is the login text easy for you to read and understand?
- Are there times where you've typed in the incorrect password? Have you ever been given a warning for typing the incorrect password too many times?

I'm now curious to learn how you manage your personal finances online. All of these sites have strict authentication systems, and I want to understand how you navigate through their web interfaces.

- Have you signed up for any online banking systems to track your balance? If so, which ones? Let's log into the one you check most frequently.
- Do you use different passwords for various online services, or do you generally stick with one or two for signing into multiple sites? Why?
- Are you comfortable making online purchases? Or would you prefer to conduct transactions offline and in person?
- Do you ever run into problems with verifying your online identity?

- Do you feel like authentication systems for money are more or less strict than authentication systems for checking email?

Let's move onto how you communicate with family and friends through your computer. Just a reminder, please continue to think out loud and verbally guide me through your thought processes and actions.

- Are you connected in any social media networks (e.g. Facebook, Twitter, Tumblr)?
- Can you walk me through logging into Facebook?
- Why did you choose to save/not save your password as a cookie on your browser? Do you find this convenient?
- How does logging in through social media sites differ from checking your financial activity online?
- Do you share any of your passwords with family or friends?

(Skip this section if user does not own a smartphone, tablet or other portable device besides their personal computer that they normally use.) I think you've given me a good overview of the work that you do on your computer. What I'd like now is for you to start logging into other sites that you normally check on a routine basis through your smart phone. I'd like for you to walk me through this process as well by thinking out loud.

- Is your smart phone password-protected?
- Does the smaller screen pose any additional/new challenges for you?
- Are you familiar with two-factor authentication? Using two-factor authentication provides an additional layer of security by asking you to enter an additional piece of information, such as a verification code, to log in after entering your username and password. Have you ever used your smart phone as a token for verifying your identity?
- Do you use any of the disability/accessibility features on your smartphone (e.g. iPhone's "Assistive Touch")?
- Have you downloaded any applications on your smart phone that help accommodate for your disability? If so, can you walk me through opening these applications and enabling them?

Great. I just have several more questions to ask you before we wrap up here.

- Do you have any suggestions to improve these login experiences?
- Aside from passwords, what would be the ideal way to log into these services?

Wrap up

I really appreciate all the time you've given me. As we wrap up, let me summarize some of the key points I've learned about your role here.

- Create a large interpretation of your learning about the user's role. The wrap-up is an opportunity to summarize what you learned about the user's role and work. It is a way for you to check your high-level understanding with the user.
- Clear up any thought processes that need further

clarification.

- Ask the user to reflect on his or her experience after completing the test. Clear up any thought processes that need further clarification.
- Ask if there is anything else regarding the usability of authentication systems the user would like to add and whether or not this test has changed his or her perspectives and/or attitudes towards current authentication practices.
- Can the user suggest another interested person of disability who would like to get involved with the study?
- Thank the user for his/her time and give the user a gift card. Exchange contact information so that the user/researcher can ask any follow up with any questions.

Figure 7: Task Flow Diagrams

We assigned a light-gray color to each step and sub-step on the diagram that the participant actually completed, while white-colored boxes indicate steps that participants did not take. In the process of doing this, we also included any quotes, comments and/or observations from the notes and interview transcripts that were of interest and relevant to the sub-steps involved in completing the task. We then placed each annotation next to the applicable step in the diagram and assigned them a different color in order to distinguish the annotations from the actual steps and sub-steps.

We calculated the total task completion time by adding all of the timings in each step in the high-level diagram and placed the final sum on the final step of this diagram.

We include an example of P7's PayPal task in Figure 7, which took a total of 400 seconds to complete. The high-level diagram contained too many steps to legibly fit on one page; therefore we split this diagram into three separate parts. Furthermore, we then selected two particular steps we felt were the most complex and time-consuming for P7 to complete her entire task. Specifically, these complex steps are Step 7 and Step 9.

Figure 7A. PayPal (P7) HTA High-Level Diagram (part 1)

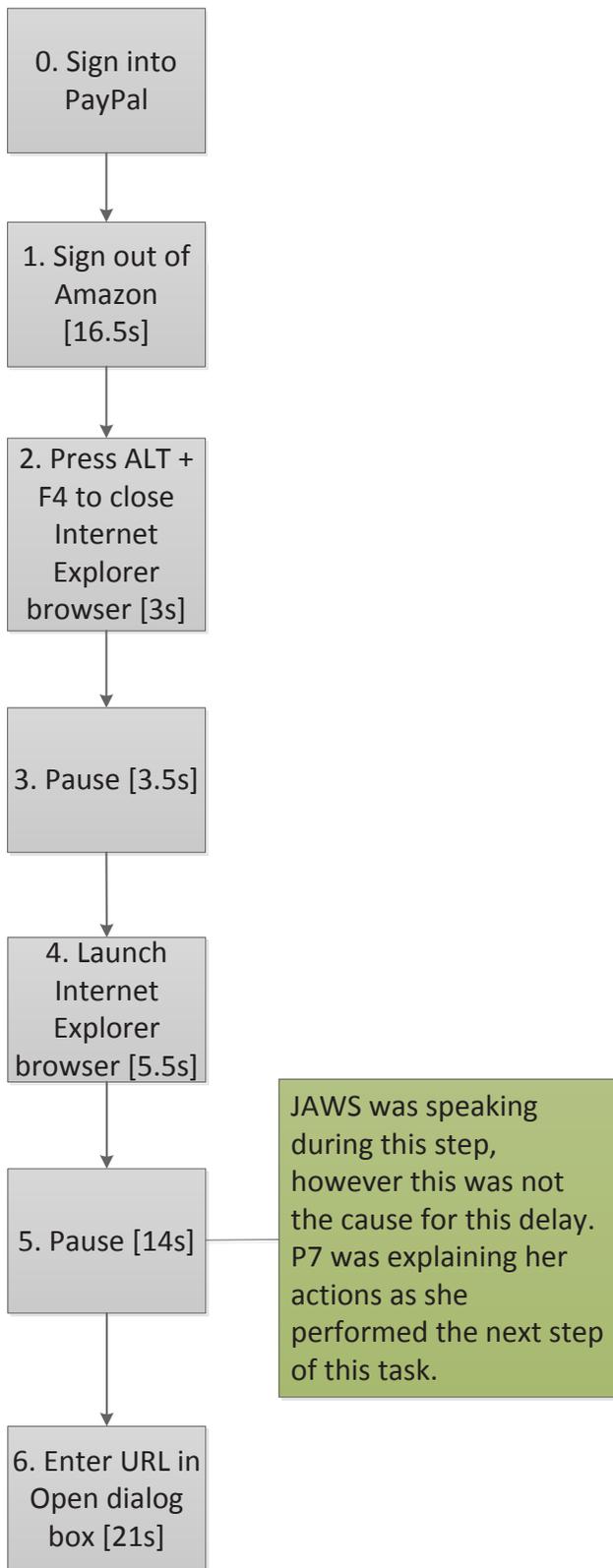


Figure 7B. PayPal (P7) HTA High-Level Diagram (part 2)

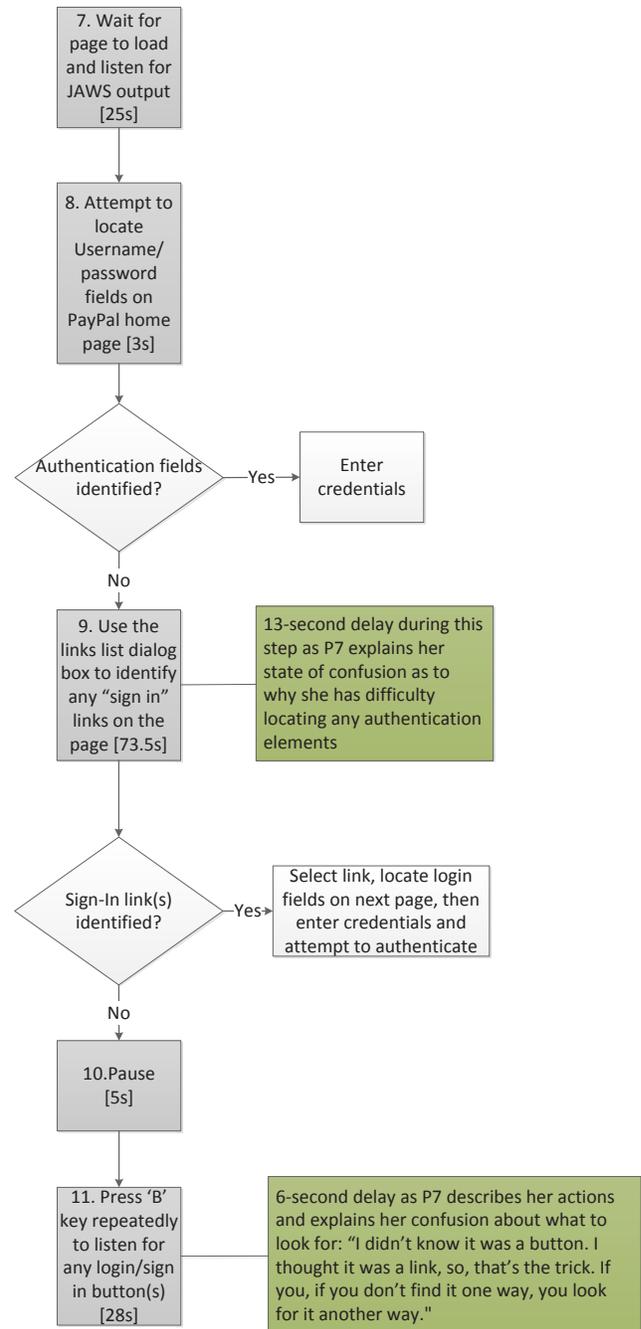


Figure 7C. PayPal (P7) HTA High-Level Diagram (part 3)

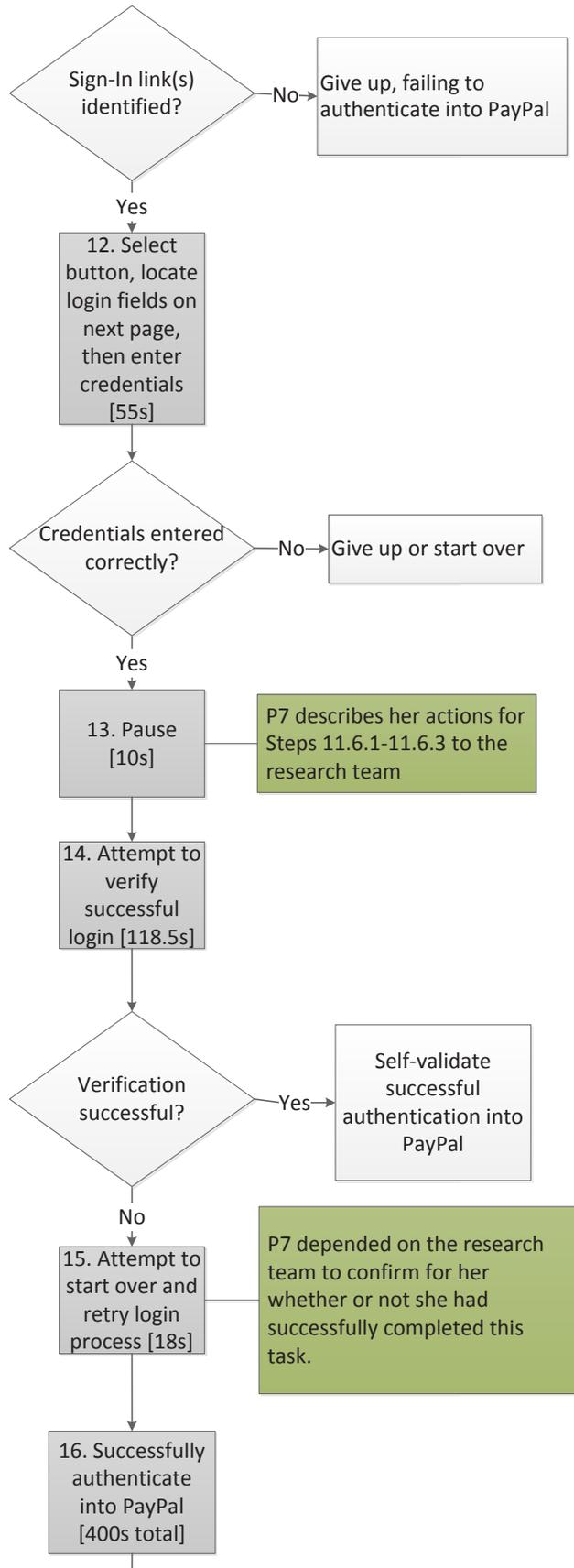


Figure 7D. PayPal (P7) HTA Step 7 Diagram

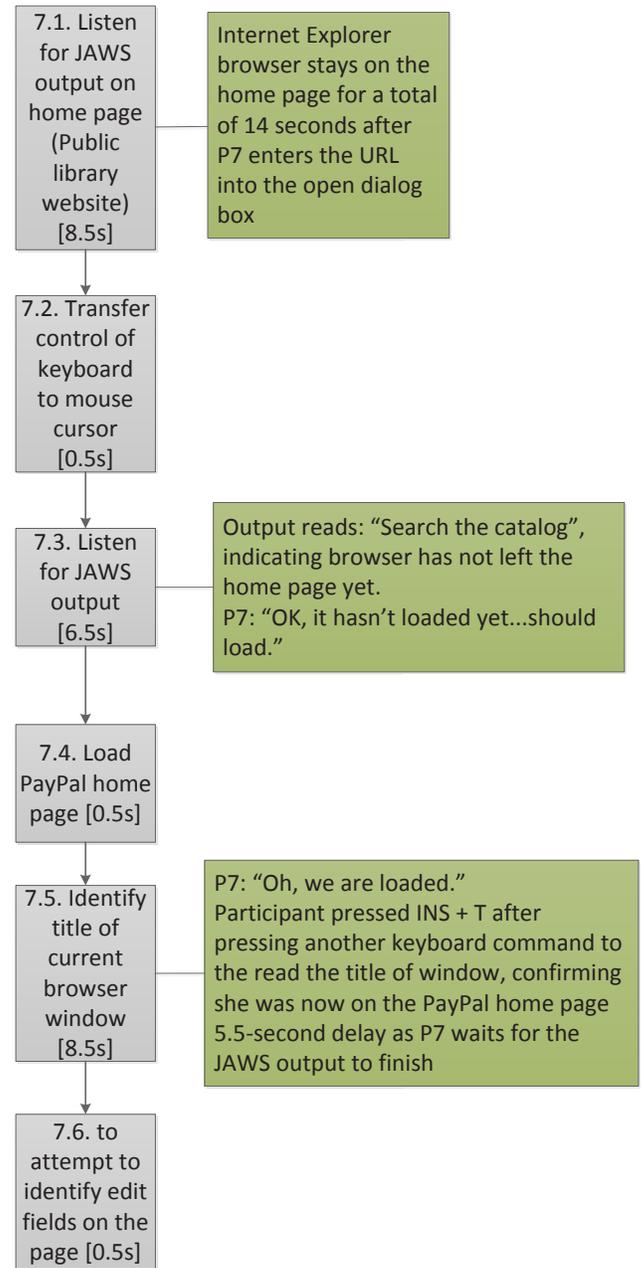


Figure 7E. PayPal (P7) HTA Step 9 Diagram

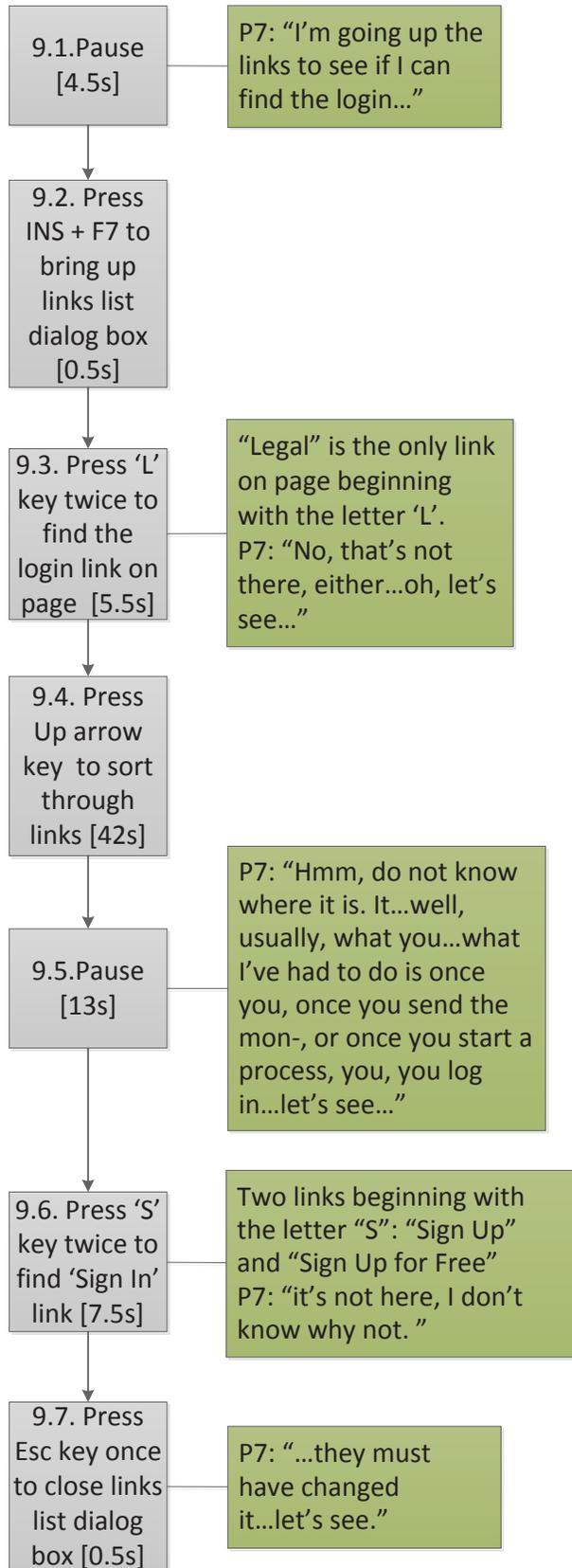


Figure 7F. PayPal (P7) HTA Step 14 Diagram

