

Accessibility

Lecture 25

Prof. Daniel Votipka
Spring 2022

(some slides courtesy of Adam Aviv)

Administrivia

- Project presentations start on Monday (4/25)
 - 10 min talk + 5 min Q&A = 15 min total
 - Everyone should submit slides on Monday
- Focus group after class with AI

What we did last time!

- Vulnerable populations
 - Journalists
 - Undocumented Immigrants
 - Victims of intimate partner abuse

What are we doing today?

- Accessibility
 - Visually Impaired
 - Passwords
 - CAPTCHAs
 - Older Adults
 - Are they different from younger adults?

Usability for Visually Impaired Users

Visual Impaired Design



Accessibility in Android

Developing Apps for Users with Visual Impairments

UX Accessibility Guidelines



When designing your application's GUI, there are a number of things you can be used by as wide an audience as possible, whether you are designing for a specific user group or not. Don't be fooled into thinking that this is just a case of "making it work", and that you shouldn't bother if you know a disabled user won't use it. Following these guidelines will improve the overall usability of your application, including you!

- 1.9.1. General
- 1.9.2. Keyboard Navigation
- 1.9.3. Mouse Interaction
- 1.9.4. Graphical Elements
- 1.9.5. Fonts and Text
- 1.9.6. Color and Contrast
- 1.9.7. Magnification
- 1.9.8. Audio
- 1.9.9. Animation
- 1.9.10. Keyboard Focus
- 1.9.11. Timing
- 1.9.12. Documentation

- Provide **efficient keyboard access to all application features**. Some users may be unable to use a mouse, and many "power-users" prefer to use the keyboard anyway. Also, some specialized assistive technology input devices may simulate keyboard events rather than mouse events. Since typing is difficult or even painful for some users, it is important to provide a keyboard interface that minimizes the number of keystrokes required for any given task.
- Use a **logical keyboard navigation order**. When navigating around a window with the **Tab** key, keyboard focus should move between controls in a predictable order. In Western locales, this is normally left to right and top to bottom.
- Ensure **correct tab order for controls** whose enabled state is dependent on checkbox, radio button or toggle button state. When such a button is selected, all its dependent controls should be enabled, and all the dependent controls of any other button in the group should be disabled. When the user selects a checkbox, radio button or toggle button that has dependent controls, do not automatically give focus to the first dependent control, but instead leave the focus on the button.

Security and Privacy for Visually Impaired Users

Visual Impairment in Authentication

SOUPS 2015

“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

- Contextual Inquiry
 - Visit participants at places where they regularly used computers or mobile devices
- Identify inaccessibility within the design
 - Clutter graphics/flash/web elements
- Screen readers offer limited support

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.

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

Contextual Inquiry

- Visit participants where they actually live and work and use computing equipment
- Observation
 - View and talk with participant as they perform the tasks
- Mutual Understanding
 - Acknowledge the user as the expert and the researcher is not there to solve the problem or tell them how to do the interaction
- Discussion
 - Review a set of participants concerns
 - Semi-structured additions

Procedure

- Semi-Structure Interview
 - Computer and internet usage
- Authentication tasks
 - Log into computer
 - Log into email, banking, social media
 - Authenticate on their phone
- Think allowed during task
 - Speak about what they are doing while doing it
- Audio and video recordings
 - Did not record actual usernames and password
- Two researchers
- 60-90 minutes
- \$30 minutes
 - \$10 for referrals (snowballing)

Why might they need referrals?

Anything else you notice?

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

ID	Participant Characteristics					Timed Attempt at Authentication in Seconds					
	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.

Thoughts on average task timing



JAWS®

JAWS, Job Access With Speech, is the world's most popular screen reader, developed for computer users whose vision loss prevents them from seeing screen content or navigating with a mouse. JAWS provides speech and Braille output for the most popular computer applications on your PC. You will be able to navigate the Internet, write a document, read an email and create presentations from your office, remote desktop, or from home.

JAWS® Solutions

For Home

For School

For Business

How screen readers are used



Difficulties with Login Task

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

Difficulties with Login Task

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
	Locating the authentication area on a web page	Accessibility & Authentication	87	92.1	13
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

Locating/Identifying Page Elements

“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.”

“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...”

wants me to follow on Twitter, and yada, yada... [sighs]... Yep, they’ve changed this. Uh, let’s see.”

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...”

Difficulties with Login Task

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	Authentication	133	0.0	1
D3	to find desired information quickly	Accessibility	35	25.5	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

Determining who is logged in

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.”*

“sometimes it's 'log in as another user', sometimes it's 'sign in as another user', sometimes it's 'change user'.”

“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.”

Difficulties with Login Task

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
	Waiting for screen reader output speaking in order	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

Delays from Screen Readers

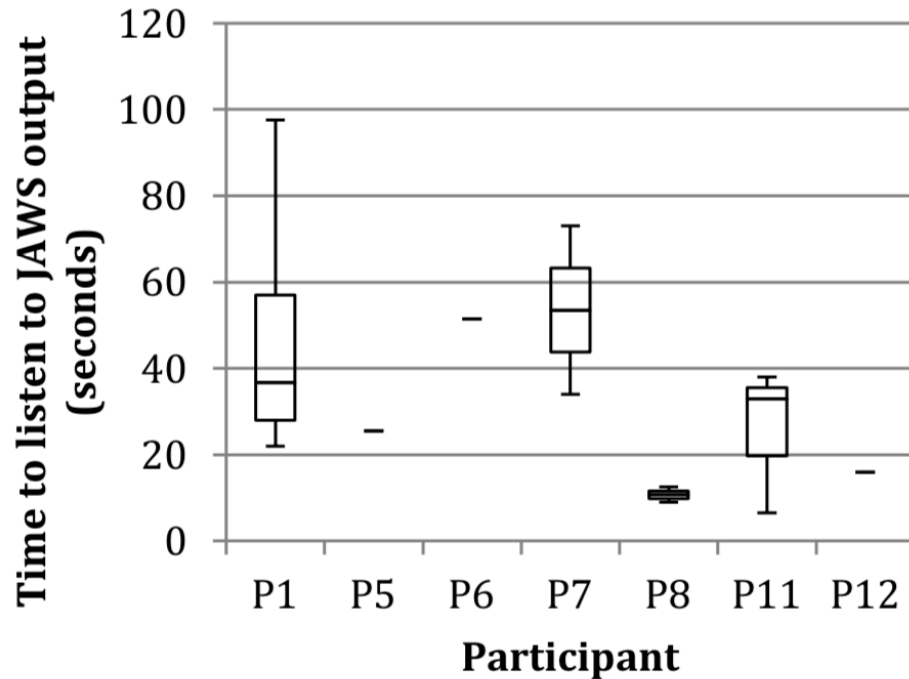


Figure 3: The distribution of time participants spent either waiting for their screen reader to begin speaking or listening to their screen reader finish reading web page elements aloud. All other participants are not shown in this graph because they did not use a screen reader when performing their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

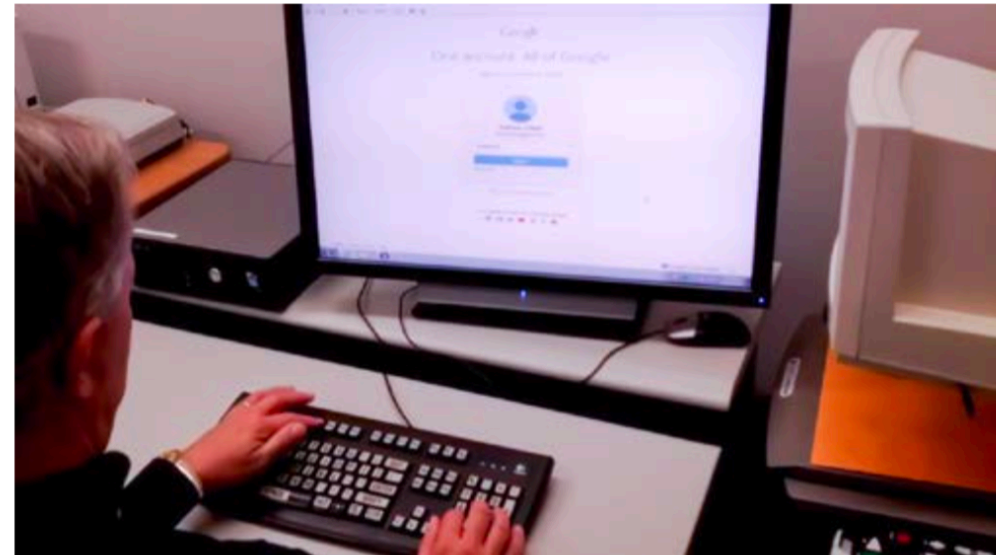


Figure 2: P1 diligently continued to troubleshoot through an authentication error by finding an alternate way to log into his email account using a variety of keyboard shortcuts.

Difficulties with Login Task

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
	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

Verifying a successful authentication

- Hard to determine if logged in based on the page feedback
 - Search for negative results
 - Lack of sign in
 - Elements there after sign in
 - “Your account”
 - “Manage your content and devices”
 - Find your username on the page
 - Like your email

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.

14.1. Press Up or Down arrow to sort through page content [8.5s]

P7: "...isn't that my name up there? It probably should."
Researcher 1: "No."

14.2. Pause [5s]

14.3. Press Up or Down arrow to sort through page content [19.5s]

14.4. Pause [6.5s]

P7: "maybe it just isn't loaded yet."

14.5. Press Up or Down arrow to sort through page content [3.5s]

14.6. Pause [12.5s]

P7: "Huh, that's not what I want, must take a while to load. Sometimes it does."

14.7 Press CTRL+Home to return to top of page [9.5s]

8-second delay as P7 listens for the JAWS output [2s] and then describes her actions to the research team [6s]

14.8.Press Up or Down arrow to sort through page content [10s]

P7: "Huh, no, that's not it."

14.9.Press ENTER [0.5s]

14.10.Press Up or Down arrow to sort through page content [43s]

P7: "...see if we have any..."

14.11. Pause [10s]

P7: It doesn't seem to work. Maybe this is one of the issues you're talking about."

Difficulties with Login Task

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	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

Limitations of Assistive technology

- Password masking
 - JAWs verbally conceals passwords
 - How do you know if you've mistyped?
 - *"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."*
- Lack of screen reader output for error messages
 - *"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."*

Password Recovery

- Screen readers struggle with reading passwords
 - Temporary password sent to a user in email that needs to be typed
- *“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-3-9-4-8-4-9-6-9-1,’ etc., and then, you got to try to remember it.”*

Mobile Authentication

- Most did not lock their device
 - To much of a “hassle”
- *“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.”*

CAPTCHAs and Visual Impairment

What about captchas?



And what happens with a screen reader?

Modern Captchas

- Click the box ... but how do you do that if you're blind?

Sample Form with reCAPTCHA

First Name


Last Name

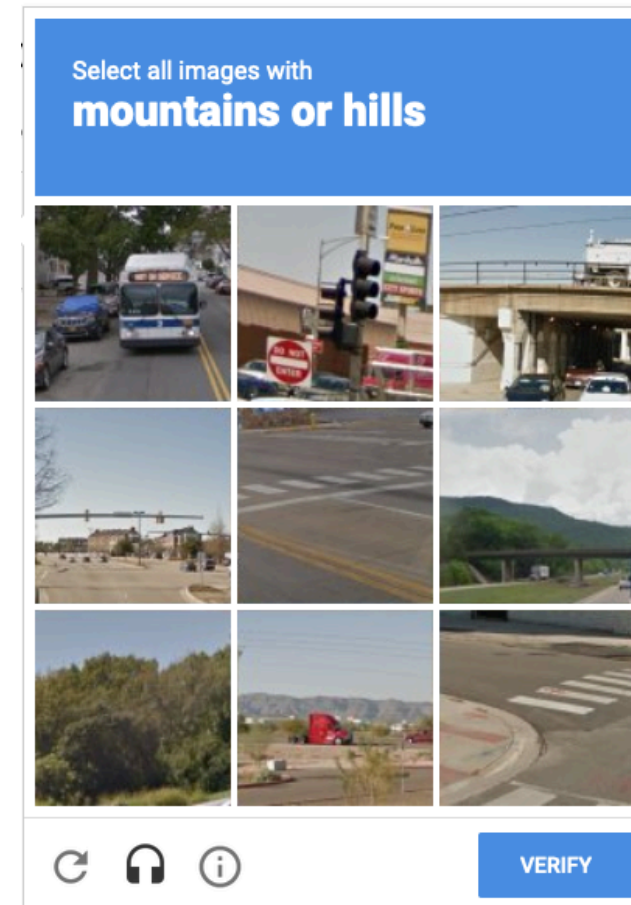
Email

Pick your favorite color:

Red

Green


I'm not a robot 
reCAPTCHA
Privacy - Terms



Audio Captcha

CAPTCHA Preview

Retype the characters from the picture:



Improving CAPTCHAs for Screen Readers

SOUPS 2020

Blind and Human: Exploring More Usable Audio CAPTCHA Designs

Valerie Fanelle
Georgia Institute of Technology

Sepideh Karimi
Georgia Institute of Technology

Aditi Shah
Georgia Institute of Technology

Bharath Subramanian
Georgia Institute of Technology

Sauvik Das
Georgia Institute of Technology

Audio interference is one of the biggest issues that users face with existing audio CAPTCHAs [3]. For example, many PVIIs rely on screen readers to help navigate user interfaces. When these users start typing the characters they hear in a CAPTCHA challenge, their screen reader software will read each typed letter out loud while they are simultaneously listening for the next character in the challenge. The audio conflict between the typed letter and the spoken letter thus creates unnecessary user frustration and errors. Owing to these frustrations, in a 2017 global study by WebAIM, of the 1,792 PVIIs surveyed, 90% ranked audio CAPTCHAs as somewhat or very difficult [34]. These respondents also ranked CAPTCHAs as the second most problematic daily issue on the web, after Adobe Flash. The goal of our paper is to offer insights and designs that bridge the usability gap between audio and visual CAPTCHAs.

Abstract

For people with visual impairments (PVIIs), audio CAPTCHAs are accessible alternatives to standard visual CAPTCHAs. However, current audio CAPTCHA designs are slower to complete and less accurate than their visual counterparts. We designed and evaluated four novel audio CAPTCHAs that we hypothesized would increase accuracy and speed. To evaluate our designs along these measures, we ran a three-session, within-subjects experiment with 67 PVIIs from around the world — the majority being from the U.S. and India. Thirty three participants completed all three sessions, each separated by one week. These participants completed a total of 39 distinct audio CAPTCHA challenges across our prototype designs and the control, all presented in random order. Most importantly, all four of our new designs were significantly more accurate and faster than the control condition, and were rated as preferable over the control. A post-hoc security evaluation suggested that our designs had different strengths and weaknesses vis-a-vis two adversaries: a random guessing adversary and a NLP adversary. Ultimately, our results suggest that the best design to use is dependent on use-context.

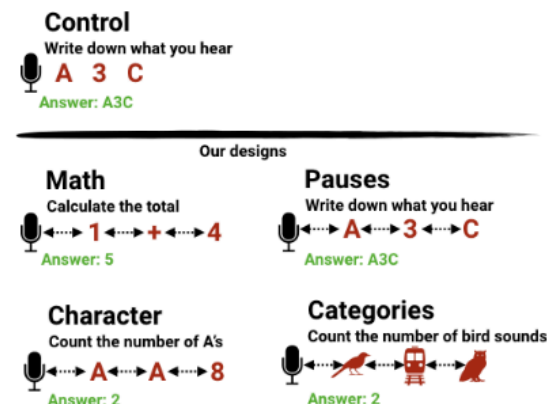
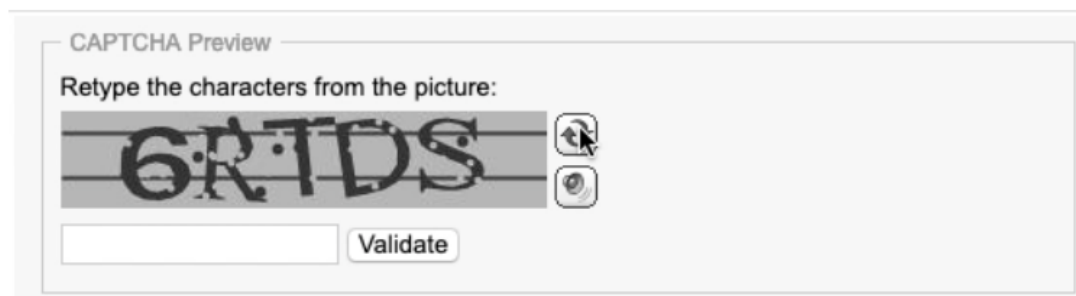


Figure 1: We designed, implemented and evaluated four novel audio CAPTCHAs. The Math prototype asked users to calculate a running total; the Character prototype asked users to count the occurrence of a character in an alphanumeric series; the Pauses prototype asked users to transcribe the alphanumeric characters they heard, but it incorporated longer

Designs



Notice that non-control consider screen readers by either

- Adding pauses
- The response is a single item

Prototype	Instructions	Sample Challenge	Correct Answer
Control (Content-Based)	Record each letter or number you hear.	8G6JVF	8G6JVF
Math (Rule-Based)	After you press play, please perform all of the calculations and provide one total at the end.	7+4-2-1	8
Character (Rule-Based)	Count the number of times '6' is spoken. Type the sum in the text box.	6R169Y6	3
Pauses (Content-Based)	Record each letter or number that you hear.	010J14	010J14
Categories (Rule-Based)	Count the number of times you hear sounds associated with those made by birds.	robin, train, motor, owl, rooster	3

Table 1: High-level summary of the prototype challenges we tested on our participants.

Some results ...

	Avg Accuracy	Avg Speed	Pref. to control	Security Random	Security NLP
Control	43%	53.6s	2.7%	++	-
Math	89%	31.7s	52%	+	+
Character	87%	32.7s	67%	-	+
Pauses	76%	35.4s	73%	++	-
Categories	70%	31.1s	61%	-	+

Table 5: Summary of key results. The Math prototype had the highest accuracy; the Categories prototype had the highest speed; the Pauses prototype was most preferred; the control and Pauses prototype were most resilient to random guessing; and, the Math, Character and Categories prototypes were most resilient to NLP.

	Accuracy Model (Logistic)	Time Model (Linear)
<i>Fixed effect coefficients</i>		
Session Number	0.35*	-0.17***
Math v. Control	2.78***	-0.73***
Character v. Control	2.50***	-0.70***
Pauses v. Control	1.77**	-0.61***
Categories v. Control	1.53*	-0.76***
Character v. Math	-0.27	0.03
Pauses v. Math	-1.00	0.12
Categories v. Math	-1.24*	-0.03
Pauses v. Character	-0.73	0.09
Categories v. Character	-0.97	-0.06
Categories v. Pauses	-0.24	-0.15
Age	0.005	0.002
Intercept	-0.87	-0.89***
<i>Random intercepts variance</i>		
Participant (N=67)	0.50	0.19
Challenge (N=39)	0.61	0.02

p <= 0.05, ** p <= 0.01, *** p <= 0.001

Table 2: Mixed-effects regression modeling both accuracy and completion time against prototype, session number, and age, with each participant and each challenge having its own random intercept. For the accuracy model, we ran a logistic regression and for the completion time model, we ran a linear regression. Broadly, the highlighted rows on the top indicate that all of our prototypes were significantly more accurate and faster than the control, and that participants grew more accurate and faster in subsequent sessions. The variance in random intercepts suggest significant variation across participants and challenges in success but not in completion time.

Discussion

- How unique are these experiences to visual impaired as compared to generic users?
- How might technology has changed since 2015 (2014) that might improve some of these situations?
 - Do you think some of these design issues have improved?
- Are there other security/privacy considerations not presented here?

Privacy and Security for Older Adults

Technological and Accessibility Challenges with Older Adults

- Digital Literacy
 - Less knowledge of internet security hazards
 - Use technology less frequently
 - Lack of efficacy
- Declining physical and mental abilities
 - Dexterity for entering security credentials reliably
 - Understandings and mental models of how security and privacy operates online

Threat Models and Mitigations

- How do older adults situation amplify their risks?
- What are older adults mental models for security and privacy concerns?
- What are older adults mitigation strategies?

SOUPS 2019

Privacy and Security Threat Models and Mitigation Strategies of Older Adults

Alisa Frik,^{1,2} Leysan Nurgalieva,³ Julia Bernd,¹ Joyce S. Lee,² Florian Schaub,⁴ Serge Egelman^{1,2}

¹*International Computer Science Institute (ICSI)*

²*University of California, Berkeley*

³*University of Trento*

⁴*University of Michigan*

afrik@icsi.berkeley.edu, leysan.nurgalieva@unitn.it, jbernd@icsi.berkeley.edu, joyce@ischool.berkeley.edu, fschaub@umich.edu, egelman@cs.berkeley.edu

Abstract

Older adults (65+) are becoming primary users of emerging smart systems, especially in health care. However, these technologies are often not designed for older users and can pose serious privacy and security concerns due to their novelty, complexity, and propensity to collect and communicate vast amounts of sensitive information. Efforts to address such concerns must build on an in-depth understanding of older adults' perceptions and preferences about data privacy and security for these technologies, and accounting for variance in physical and cognitive abilities. In semi-structured interviews with 46 older adults, we identified a range of complex privacy and security attitudes and needs specific to this population, along with common threat models, misconceptions, and mitigation strategies. Our work adds depth to current models of how older adults' limited technical knowledge, experience, and age-related de-

market for caregivers is projected to shrink [59]. These factors are stimulating investment in emerging “smart” technologies for older adults—aimed at sustaining independent living, increasing quality of life, and mitigating health issues via early detection [83]. Emerging smart technologies such as wearable medical devices, fall sensors, and therapeutic robots [10] may yield benefits, but due to their novelty, complexity, and propensity to collect vast amounts of information, they also pose security and privacy risks.

Due to limited technological literacy and experience, and because of declining physical and mental abilities [44, 96], older adults are particularly unaware of and susceptible to those privacy and security risks [5, 16]. Specifically, older adults have less knowledge of Internet security hazards [36, 40], use technology less frequently [19, 28, 40, 43, 52, 101], are more vulnerable to security risks [41], and are more often targeted

Methods

- Semi structured interviews
 - 1-1.5 hours
- Discussion
 - Privacy- and security-related concerns and threats
 - Risk management strategies
- Thematic Coding
 - Four total coders
 - Two coders coded each transcript
 - Annotated excerpts
 - Resolved disagreements
 - 3 of 4 coders to move forward

Participants

- 65-95 Years Old
 - Mean 76
- 65% Female
- 76% White/Caucasian
- 44% Advanced Degree
- 63% Live alone

Individual characteristics	N	%
Income level		
Less than \$35,000	16	35%
\$35,001-75,000	16	35%
\$75,001-150,000	6	13%
More than \$150,000	4	9%
Preferred not to answer	4	9%
Housing		
Independent/assisted living (w/ health facilities)	6	13%
Senior/retirement community	10	22%
Mainstream housing (rent or own)	30	65%
Self-reported health conditions		
Excellent	8	17%
Good	23	50%
Fair	11	24%
Poor	3	7%
Very poor	1	2%
Caregivers		
No one	37	80%
Hired caregiver	4	9%
Informal caregiver	3	7%
Both hired and informal caregivers	2	4%

Table 1: Participant characteristics based on survey responses.

Devices and Usage

Device Type	Daily	Sometimes	Never
Mobile phone, smartphone	52%	22%	26%
Tablet	22%	24%	54%
Computer/laptop	61%	22%	17%
All three	11%	39%	–

Table 2: Device use among participants.

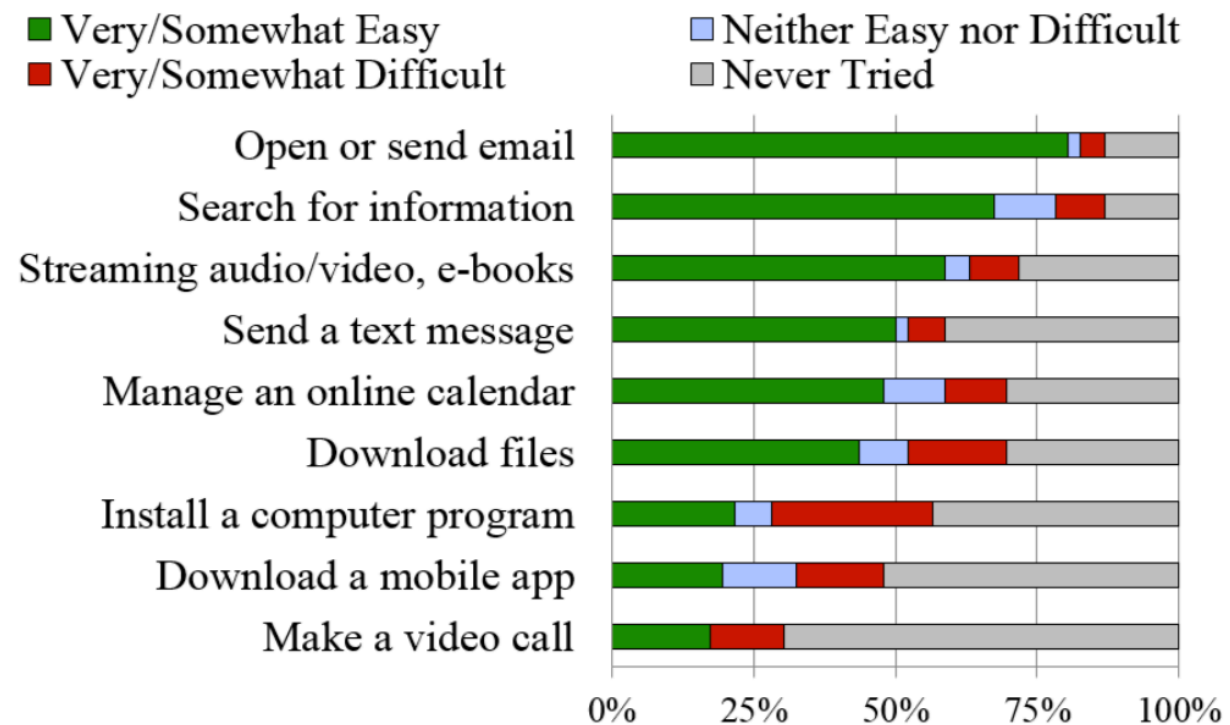


Figure 1: Participants' facility at performing online tasks.

Privacy and Security Threats

- Solove's Taxonomy
 - Information Collection
 - Information Processing
 - Information Dissemination
 - Privacy Invasions

University of Pennsylvania

Law Review

FOUNDED 1852

Formerly
American Law Register

VOL. 154

JANUARY 2006

No. 3

ARTICLES

A TAXONOMY OF PRIVACY

DANIEL J. SOLOVE[†]

Privacy is a concept in disarray. Nobody can articulate what it means. As one commentator has observed, privacy suffers from "an embarrassment of

[†] Associate Professor, George Washington University Law School; J.D. Yale. A project such as this—one that attempts a taxonomy of the sprawling and complex concept of privacy—cannot be created by one individual alone. I owe an enormous debt of gratitude to many people who provided helpful comments on the manuscript or parts thereof at various stages in its development: Anita Allen, Howard Erichson, Jim Freeman, Robert Gellman, Rachel Godsil, Stan Karas, Orin Kerr, Raymond Ku, Chip Lupu, Jon Michaels, Larry Mitchell, Robert Post, Neil Richards, Michael Risinger, Peter Sand, Heidi Schooner, Paul Schwartz, Lior Strahilevitz, Charles Sullivan, Michael Sullivan, Peter Swire, Robert Tuttle, Sarah Waldeck, Richard Weisberg, and James Whitman. Thanks to Michael Weisberg and Brian Leiter for directing me to useful resources on systematics. I would also like to thank my research assistants, Poornima Ravishankar, Jessica Kahn, and Tiffany Stedman for their excellent assistance. Additionally, I benefited from helpful comments when I presented this paper at a workshop at Washington University and at a conference sponsored by the International Association of Privacy Professionals. The George Washington University School of Law scholarship fund provided generous support for this Article.

Privacy and Security Threat Models

(Information Collection)

- Lack of transparency about information gathering and people's inability to control it
 - Synchronization viewed as a "black box"
 - *"I was concerned that [...] you think you know what shares, but stuff can wind up on another computer so easy with an Apple." "The sharing just surprises me sometimes. You don't know how stuff can go from one to the other, you are surprised it's there." (P123).*
- Information used as unsolicited marketing, particularly from technologies like smartTVs
 - *"It's scary. Just like, it invades—if the government were to put a microphone in everybody's house and listen to everything you say, people would object. But they are voluntarily putting these devices in their homes and it's doing the same thing," P108*

Privacy and Security Threat Models

(Information Collection)

- Privacy from bystanders
 - *“All my charge cards, all my whatever, everybody knows exactly what I’m doing, even though I never put it on a computer. It’s on a computer from someplace else. [...] Every phone call you make is recorded somewhere,”* P43.
- Personification of data collection
 - *“Whenever you look something up, you get an ad. So a lot of people are reading what you do,”* P5
 - *“The computer [...] probably tracks what you are watching, what you are going to, what you are inquiring about, and keeps a record of it internally. [Interviewer: For what reason?] Because Steve Jobs made it that way. To track data,”* P69
 - *“On Facebook, I started—and then they have this Zuckerberg thing about what they were capturing,”* P104)

Information Collection in Senior Care

- “Care Surveillance”
 - Monitoring by family members, medical staff, or facilities, e.g., via video or other digital means
 - *“There are sensors so that if you don’t go up and go to the bathroom, someone will come down the hall and see if you are okay,” (P69)*
- Understood as benign but can still induce anxiety
 - *“I know a lot of these devices have cameras in them, and rightly so because they are designed to be helpful, but you know, it’s always a concern, I think, when you are using some of the new electronic, is how private are the things that you do,” P22*

Privacy and Security Threat Models (Information Processing)

- Understood data could be aggregated to invade privacy, but thought risk was unlikely
 - *If I were the evil genius, who had that record, I think I could [...] probably tell you more about yourself than you would know about yourself. Or I may be exaggerating, but not too much. [I: Do you believe anyone has the record on you?] I hope not, but, you know... I think most people would find it rather boring, but... [I: Do you think there's some evil genius exists somewhere in the world?] N-n-no, no. This is a hypothetical," P51*
- Limits willingness to engage in online political discourse
 - *"I am always chatting about politics and, even on the phone, sometimes I hesitate because I know they cap all that information," P46; "I would do a [Facebook] Like, or submit, and now I've decided not to do that because you just don't know what's being captured. But I really want to support those [political figures]. I don't think we know enough about what's being captured," P104*
- Medical fraud and scams
 - *"I got a bill from the hospital for \$26,000. They had padded it. [...] I can't prove that none of that stuff happened," P5*

Privacy and Security Threat Models (*Information Dissemination*)

- Data being sold for profit
 - *“If it’s confidential and private, I don’t care if they have all my information. [...] As long as [...] it wouldn’t be abused, or I’d get a bunch of salesmen calling me trying to sell a device or a pill or something,”* P10
- Desire for safeguards
 - *“I would just like to see some kind of safeguard [...] in the technology so that strangers [...] don’t have access to knowing everything about you, because strangers don’t really need to know,”* P47
- Purposeful disclosure being used for illegitimate purposes
 - *“I no doubt shared my social security number with some other benevolent entity [...] but that someone decided that that might be of value in the open market,”* P51
- Purposeful disclosures not being shared
 - *“I wish [doctors] would share [my medical records with each other], but they don’t. It’s so compartmentalized that it’s [...] really frustrating. [...] It’s a benefit and it’s a curse, [...] because [...] unless you tell them, [...] they don’t know what is going on with the [other] doctors in your life,”* P46

Privacy and Security Threat Models

(Privacy Invasion)

- Physical incarnations

- *“When you are having a private discussion with someone, you ought to be able to feel that it’s as private as those that are involved in it are willing to be, you know. You can’t obviously be sure that they won’t go blabbing it all to the next person they talk to, but, I wouldn’t want technology doing that for me,” P15*

- Decision Making

- *“I think that they expected that Facebook information would be effective in addressing specific group of voters. When you think about it, it is not far-fetched. It is perfectly reasonable,” P121*

Device Ownership

- Public Devices

- Blood pressure monitors
- Issues of high costs or lack of perceived utility
- Misconceptions about risk
 - *“That’s another reason why I don’t want a home computer. I go to the library, and if [the computers there] crash, they’ll deal with it. [...] If I had one, and it crashed [...] I’d just leave it off. I don’t want to have to pay for the repairs,”* P10

- Second-Hand Devices

- *“Grandpa gets the oldest phone. When they get upgraded, the phones trickle down. [...] I am thrilled with it, and it is too old for anyone else to use in that household,”* P121
- Old data on the phone
- Lack of security updates over time

Managing Privacy and Security Risks

- Pessimism/loss-of-control
 - *“I wish they would take the word privacy out of the dictionary. There is no such thing anymore. [...] I think it’s the genie out of the box. I don’t think it can be addressed,”* P43
- Lack of knowledge and skills to protect data
 - *“I’m not sophisticated when it comes to all these electronic gadgets and so I don’t know what the possibilities are for control that is unavailable to hackers and thieves,”* P20
- Attribution to age
 - *“Don’t forget, I’m old. And some things [...] you just sort of have to let go and you don’t want to use your energy at it. [...] I want my information back and they say no, sometimes you just have to go ahead [...] Not everybody can fix everything. You just have to live with the consequences. That’s why you shouldn’t be saying nasty things on the Internet, because it comes back to haunt you and you can’t fix them,”* P107
- Privacy should be restored
 - *“I value privacy. I don’t necessarily want anyone who wants information about me to be able to get it too easily, and too cheaply. If they are going to get it, I want them to work for it, and pay for it, as a way of discouraging them,”* P113

Managing Passwords

- *“I have a list of [passwords], and sometimes the computer will remember them, which is helpful, and then sometimes not. I have it written down and sometimes they make you change the password and I forget to write it down,” P6*
- *“I use the same password for everything and I have used the same password for years. Even though we have been advised not to do that. [...] It’s hard enough for me to come up with a password that I can remember and not write down—they tell you not to write it down so I don’t do that,” P110*

Misconceptions and Blind Spots

- Information Flow
 - Misconceptions where data is collected, transferred and used
 - Which devices are Internet connected
- Data Persistence
 - What does it mean to permanently delete information
 - Overwritten rather than stored permanently
- Helpless to find solutions
 - Loss of control of information, and unable to reclaim it
- Reliance on ineffective measures
 - Scam “security services”
 - Identity insurance
- Over confidence in a product
 - Apple is not vulnerable
- Ineffective protections
 - Changing password regularly
- Mitigate consequences rather than risks
 - Call blockers vs. removal from call lists

Belief in nothing to hide

- *“Who would really care how many steps a day I take? [...] I can’t see how anybody could use that information to make money. [...] Unless maybe they wanted to sell me some exercise equipment, like a treadmill. [...] I don’t see that as a realistic possibility of ever happening,” P7*

Discussion

- Did we learn new things about older adults or about privacy risks/threats generally?
- How unique are these findings compared to other papers we've read this semester?
 - What makes this paper older-adult relevant or just generally relevant?

How does this compare to younger users?

PoPETS'21

USENIX Sec'21

sciendo

Proceedings on Privacy Enhancing Technologies ... (..):1-21

Hirak Ray*, Flynn Wolf, Ravi Kuber, and Adam J. Aviv

“Warn Them” or “Just Block Them”?: Investigating Privacy Concerns Among Older and Working Age Adults

Abstract: Prior work suggests that older adults are less aware of potential digital privacy risks compared to younger groups. We seek to expand on these findings by using drawmetrics with 20 older adults (60+) to visualize their experiences with digital privacy via drawing sessions. We further compared older adults with 20 adults of working age (18-59) with the goal of identifying both overlapping concerns and key differences that may be missed when viewing each group in isolation. We extended our evaluation with a survey with questions and themes derived from open-coding of the drawn images and confirmed three key differences between the age groups. These include older adults perceiving a greater threat from using online banking and e-commerce compared to working age adults, older adults exhibiting greater levels of concern about global scale threats, and working age adults showing more privacy-related concern regarding social media. Our findings can be used to potentially tailor applications to better accommodate privacy concerns for older adults.

Keywords: Older Adults, Privacy, Internet

DOI Editor to enter DOI

Received ...; revised ...; accepted ...

tion from the perspective of privacy for a number of reasons. While known to contribute to and gain from technological advancement, older adults have been found to be more disconnected from information and communication technologies compared to individuals in other age groups [34]. Researchers also suggest that technology exposure and education varies by age group [22]. As a population, older adults are also known to be less informed of both possible online privacy violations and the protective measures they can take against those attacks [21]. This leads to negative outcomes, including victimization in scams and data breaches [8].

There is much to gain from studying the privacy and security concerns of older adult populations, such as determining requirements to better tailor interface design to the needs of this community [18] and developing stronger, more targeted security guidance [11]. However, there has been less effort in directly comparing the privacy beliefs and concerns between older and younger adults. Here, we focus on isolating these differences through the use of a *drawmetrics* approach (using picture-drawing sessions to understand mental models) [36]. Through a qualitative analysis of the drawings and discussion, we first present a reflection on the opinions of working age adults on older adults' perceptions.

Why Older Adults (Don't) Use Password Managers*

Hirak Ray, Flynn Wolf, Ravi Kuber
University of Maryland, Baltimore County
[hirakr1, flynn.wolf, rkuber]@umbc.edu

Adam J. Aviv
The George Washington University
aaviv@gwu.edu

Abstract

Password managers (PMs) are considered highly effective tools for increasing security, and a recent study by Pearman et al. (SOUPS'19) highlighted the motivations and barriers to adopting PMs. We expand these findings by replicating Pearman et al.'s protocol and interview instrument applied to a sample of strictly older adults (>60 years of age), as the prior work focused on a predominantly younger cohort. We conducted $n = 26$ semi-structured interviews with PM users, built-in browser/operating system PM users, and non-PM users. The average participant age was 70.4 years. Using the same codebook from Pearman et al., we showcase differences and similarities in PM adoption between the samples, including fears of a single point of failure and the importance of having control over one's private information. Meanwhile, older adults were found to have higher mistrust of cloud storage of passwords and cross-device synchronization. We also highlight PM adoption motivators for older adults, including the power of recommendations from family members and the importance of education and outreach to improve familiarity.

As a result, security experts often recommend password managers (PMs) as a means of automatic password generation, management and storage. PMs are an effective tool to achieve convenient authentication and improved security when accessing online accounts [32]. PMs come in many forms: standalone PMs, like LastPass or 1Password, that auto-fill, generate, and save passwords; browser-based PMs, like in Chrome or Firefox, that save entered passwords; and operating system PMs, like OSX Keychain, that manage passwords at an OS level across applications, like Wi-Fi passwords.

Given the wide range of choices of PMs, and the widely touted benefits of using these types of technology, Pearman et al. analyzed why users do (and do not) use PMs [25]. The researchers conducted semi-structured interviews with $n = 30$ participants split between those who do not use a PM, those who use a built-in browser-/OS-based a PM, and those who use a standalone PM. Participants described their password management techniques, trade-offs between convenience and security in PM adoption, motivations for and barriers against adopting PMs, and uncertainty regarding the source of password-saving prompts on browsers.

Comparing Privacy Concerns via “drawmetrics”

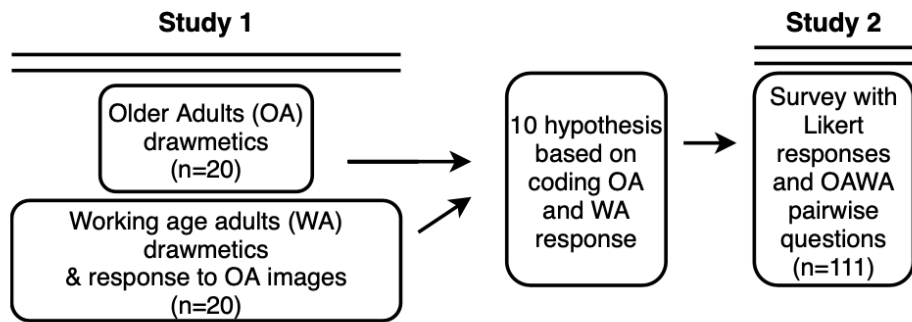


Fig. 2. P01's drawing of their sense of digital privacy, captioned, "Woe is me in a digital privacy sense." It depicts her beset by privacy threats (e.g., criminals, her own vulnerable data, technology companies, etc.)



Fig. 3. P10's illustration of his frustration in dealing with spam emails, being forced to delete them repeatedly or resorting to cleaning up his computer or installing new antivirus software.

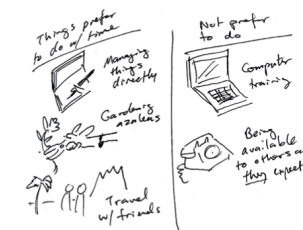


Fig. 4. P12's drawing of their sense of personal privacy, showing on the left-hand side, the interests they prefer (managing a checkbook, gardening, travel) separated from (on the right-hand side) tasks they wish to avoid (learning technology and answering sales calls).



Fig. 5. "And then the castle just falls..." P27's drawing of their depiction of ideal privacy, showing a well-guarded castle with threats (battering ram and Trojan horse) waiting to strike.

Views of Ideal Privacy. Three participants visualized ideal levels of privacy as having control over their environment. P27 described that a castle would be able to keep others out (Figure 5). However, he was aware that no solution was perfect.

"This is ideal-ish privacy. But even though it is a castle, it can be breached by a battering ram or like a Trojan horse if given the time. If the guards are not paying attention, the ram and horse can break in. And then the castle just falls."

Developed set of hypotheses from Study 1 to evaluate in Study 2 via closed-form survey

Hyp. No.	Qualitative Findings from Study 1	
H1	Older adults are more worried than working adults about society's privacy	Rejected
H2	Older adults are more likely than working adults to consider abandoning the use of technology to protect their private information	Rejected
H3	Older adults are more apprehensive than working adults about giving their private information to strangers if there are safeguards in place to protect them	Confirmed
H4	Older adults are more concerned with direct privacy attacks on their digital information	Rejected
H5	Older adults are more concerned about leaking private information through their mobile phone than any other device	Rejected

H6	Older adults feel more frustrated than working adults by global on-line attacks as opposed to local scam callers	Confirmed
H7	Older adults are less concerned than working adults about their private information being shared online through social media	Confirmed
H8	Older adults prefer to describe barriers (in order to protect privacy) in the form of metaphors and symbolism	Rejected
H9	Older adults feel more targeted and victimized by privacy attacks than working adults	Rejected
H10	Older adults prefer having power, control and ownership over objects when visualizing ideal privacy	Rejected

What we did today!

- Accessibility
 - Visually Impaired
 - Passwords
 - CAPTCHAs
 - Older Adults
 - Are they different from younger adults?

What's next?

- Final Presentations!!

Monday (4/25):

1. Steven, Tejas, and Xinhang
2. Hiba and Khanh
3. Syed, Ron, and Gun
4. Eli and Katie
5. Zoe, Yifan, and Jailing

Wednesday (4/27)

1. Changhao, Xue, and Hanfeng
2. Xenia and Robert
3. Joe, Hongyue, and Paul
4. Sruthi and Alan
5. Matthew and Emmett

Monday (5/2)

1. Thomson and Alexander
2. Vanessa, Mateo, and Zongyan
3. Nick, Max, and Carson
4. Sarah