(Work in Progress) An Insight into the Authentication Performance and Security Perception of Older Users

Sovantharith Seng*, Sadia Ahmed†, Mahdi Nasrullah Al-Ameen‡, Matthew Wright*
*Rochester Institute of Technology, Email: {ss2816,matthew.wright}@rit.edu
†University of Texas at Arlington, Email: sadia.ahmed78@mavs.uta.edu
‡Clemson University, Email: malamee@clemson.edu

Abstract—Older users (aged 55 and over) are generally thought to have limited knowledge in online security; additionally, their declining cognitive and perceptive abilities can further expose them to digital attacks. Despite these risks and the growing older population, little has been studied about older users' security performance, perception, and behavior. We begin to address this gap with this preliminary study. First, we studied older users' ability to memorize passwords through a multi-session user study with seven participants at a local retirement community. For this study, we leveraged a recently-proposed graphical authentication scheme that offers multiple cues (visual, verbal, spatial) to memorize system-assigned random passwords. To tailor this password scheme to an older population, we build on prior work in cognitive psychology that has been done to understand older users' needs. Second, we conducted a survey to further learn about their security perceptions and practices. Based on what we have learned and the challenges that we have faced during our study, we offer guidelines for other researchers interested in designing new systems and conducting usability study with older population, and we also outline the future work for our ongoing research.

I. INTRODUCTION

Faced with the task of making a password that is both secure and memorable, many users create weak passwords or have to write them down. As users age and their cognitive capacities decline, this becomes more of a concern, making older users more vulnerable to attacks on their online accounts. According to the Pew Research Center [14], older users aged 55 and over are increasingly adopting technology into their everyday lives, and this further raises the stakes for their online security. While numerous studies have examined the efficacy and usability of password alternatives with younger, Internet-savvy users, there has been only limited work on the usability of an authentication scheme for older users [12], [9].

In our study, we leveraged a recently-proposed graphical password scheme called CuedR [2], which helps users memorize system-assigned random passwords by providing them with memory cues at both registration and login. The study on CuedR showed promising login success rate for college-aged users [2]. In a follow-up study [1], Al-Ameen et al. found that offering users a combination of spatial (fixed position of images in a portfolio) and verbal cues (real-life facts corresponding to an image) performed best in terms of memorability, where 98% of users (mean age: 21) were able to log in successfully one week after learning their password at registration. Previously, Renaud et al. [12] recommended that an authentication system using recognition is more appropriate for older users. Since CuedR showed promise with younger users and is a recognition-based scheme, we explored how well it works for older users and whether we could make useful improvements to aid their comfort and login performance.

As informed by the literature on the cognitive ability of older users [5], [7], [8], [11], [12], we modified the interface of CuedR scheme in several ways, including the introduction of an audio cue at registration. We then tested the usability of this scheme for older users through a multi-session study. We found that all seven users who completed the study successfully recalled their password. We also collected information on the security perception and practices of older users through the survey conducted during this study. Based on our observations and user feedback from this study, we made further modifications to the interface of CuedR scheme. To understand users' satisfaction with these changes, we conducted a second study consisting of one session. Three participants from the first study returned for our second study, and all of them expressed their overall satisfaction with the modified CuedR interface.

Based on our results and experience from this preliminary study, we consolidate suggested guidelines for designing systems and conducting studies aimed at older users. We also identify the scope for future work for our ongoing research on the authentication performance and security perception and behavior of older users.

II. BACKGROUND

In this section, we give a brief overview of CuedR, our reasoning for choosing CuedR, and known design issues when working with older users.

A. CuedR

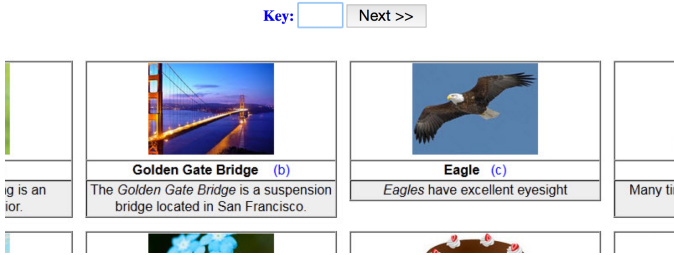CuedR is a graphical password system proposed by Al-ameen et al. [2], which combines different types of memory

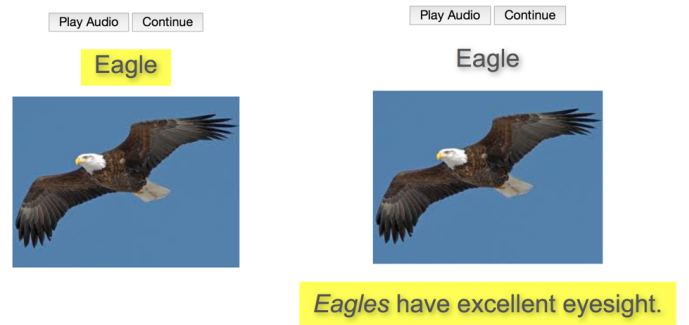Fig. 1. A portion of a portfolio shown in CuedR.

Fig. 2. Left: Step 1 of the registration process: keyword and picture are shown with highlighting to draw focus. Right: Step 2 of the registration process: verbal cue (i.e. an interesting fact about the keyword) is added to the screen with highlighting to draw attention.
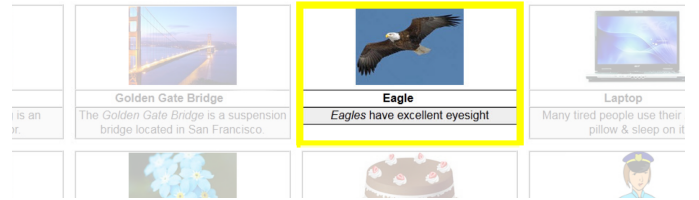

Fig. 3. Step 3 of the registration process: the portfolio is shown with a fading effect for the unassigned keyword. Highlighting is used to draw attention to the assigned keyword.

cues to help users memorize system-assigned passwords.

In CuedR, users are assigned a series of non-repeating *keywords*. Each keyword has a corresponding picture (*graphical cue*) and an interesting fact (*verbal cue*). Users are presented with five *portfolios* each containing 16 total keywords, and a user is assigned one keyword at random from each portfolio. When the keyword is presented in a portfolio, it also provides a *spatial cue*, since its location in that portfolio remains fixed across the registration and login sessions. Users are shown a single-character *key* for each keyword, and they need to enter the key letter into a text field at the top of the window to select that keyword. For example, in Figure 1, the keyword: "eagle" is presented with a picture of eagle (graphical cue) and an interesting fact: "Eagles have excellent eyesight" (verbal cue), where users are required to enter the letter "c" as the key to select this keyword. For a successful authentication, users are required to enter the correct key in each of the five portfolios, where a portfolio advances to the next one regardless of the correctness of the entered key. Thus, as required for security, the login interface does not provide any clue as to which of the five entered keys were incorrect in case of a failed login. In CuedR, the system assigns the user five keywords, each one from a distinct portfolio of 16 keywords. This offers 20 bits of entropy, which has been deemed to be sufficient against online guessing attacks [6].

Al-Ameen et al. [1] followed up their first study by examining the individual impact of different types of cues and user interaction on the memorability of system-assigned recognition-based graphical passwords, and they found that the combination of verbal and spatial cues for recognizing object images performed best among seven different schemes, offering 98% login success rate (one week after registration) for college-aged users. In a third study [3], the authors compared textual and graphical recognition-based schemes offering memory cues, and they found that adding images to textual information contributed to a significant improvement in usability.

We chose to use CuedR due to its security level and its design based on theories from cognitive psychology [2], which includes the use of *recognition* (e.g. picking from a list) to reduce users' cognitive load [13], the use of pictures to leverage the *picture superiority effect* [10], and the use of verbal and spatial cues to leverage the *depth of processing effect* [4]. Furthermore, Renaud et al. [12] also recommend recognition-based authentication that provides multiple cues for older adults.

B. The Needs of Older Users

To tailor the system to an older population, we build on prior work that has been done to understand older users' needs. Pattison et al. [11] note that the working cognitive capacity of older users is diminished, and thus, they should not be bombarded with complex data in a short amount of time. Furthermore, their cognitive processing time is increased, which means that any notification or attention grabber should not be flashing. Huppert [7] found that coupling visual and audio feedback can increase comprehension. In this case, Pattison et al. [11] note that the audio feedback should be simple and contain no high-pitched sounds. For visual content, Becker [5] recommended that text be large and should not be placed against a patterned background. For dexterity, Renaud et al. [12] recommended that the use of mouse and keyboard with fine control should be minimized.

III. SYSTEM MODIFICATIONS

For this study, we modified the CuedR system in two steps to meet the needs of older users.

A. Modifications: First Step

In the first set of modifications, we used findings and recommendations from prior research on older users to inform how we changed the system to help them learn system-assigned passwords.

The most significant change in the first set of modifications was to introduce incremental learning to the registration process. Older users show a decrease in cognitive processing efficiency over time, especially in learning new and complex
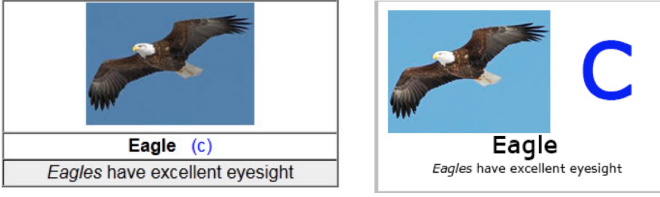
Fig. 4. Comparison between portfolios from Part 1 and Part 2. Notice the differences in layout, font and size of keys and keywords.

material [11]. Presenting the cues to the users incrementally breaks down the cognitive load and guides them through a process of learning. Each keyword and its cues were introduced to the participants in the following incremental order: graphical cue with keyword (step 1), verbal cue (step 2), spatial cue (steps 3 and 4), and key (step 5).

Following the suggestion of Huppert [7], we combined audio and visual information together by including audio cues in step 1 (reading the keyword aloud) and in step 2 (reading the verbal cue aloud). To get the cues, we used the output of a commercial text-to-speech service applied to the keywords and the verbal cues.[1] The audio is automatically played once the screen for the corresponding step is loaded. Also, the keyword or the verbal cue is highlighted to signal the participant to read along, as shown in Figure 2. The highlight is static instead of flashing to maximize user's attention [11].

In steps 1 and 2, the graphical cue was enlarged to take up most of the screen for easy viewing. Step 3 showed the entire portfolio so that the participant can learn about the spatial cue on the location of the keyword in the full context of the portfolio (Figure 3). We applied a fading effect to bring focus to the assigned keyword and added a highlighted box for emphasis. In step 4, the fading effect was removed to show the pictures neighboring the keyword, thus providing additional spatial cues. In step 5, the key was presented next to the keywords to complete the portfolio as it would be shown at login. A final change was to make the font sizes larger to accommodate difficulties with vision [8]. This meant, however, that users needed to scroll down to view the entire portfolio.

B. Modifications: Second Step

After the first part of our study (see §IV-A for detailed discussion), we used the participants' feedback and our observations to further tailor the system to meet older users' needs.

Since vision problems were still a significant issue, we made a number of changes to the look of the system. We changed the layout of the portfolios as shown in Figure 4, with the graphical cue shifted over to the left to make room for a much larger key (the letter 'C' in Figure 4). The gray background behind the verbal cue was removed to enhance contrast for better readability [11]. Also, we reduced the white space, which decreased the amount of scrolling needed. The font was changed to APHont, a low-vision-friendly font[2]. We chose APHont because it is a sans-serif typeface which is recommended by Becker [5]. Finally, some graphical cues were altered or changed due to participants' comments about low contrast or a mismatch with the keyword.

---

[1]Acapela Group, www.acapela-group.com
[2]APHont, www.aph.org/products/aphont

To make the interface simpler to use, we eliminate a part of required mouse actions: In the incremental learning phase, the cursor was automatically focused to the input text field, so that no mouse moving or clicking was required to move the cursor to the text field. For the login phase, the input text field was removed entirely, and the users simply type the key. The portfolio will advance once a key press is registered. This design has multiple benefits: i) It allows more space and clarity in accommodating the images in a portfolio, and ii) users could input the key quicker by simply pressing the key on the keyboard as soon as the portfolio appears.

Finally, we made a minor change in the incremental learning phase by removing step 4, which showed the portfolio without the keys, since the purpose of this step was confusing to some participants and not critical to learning the system.

IV. USER STUDY

In this section, we describe the procedure and results of our user study, which is divided into two parts. Our study was approved by the IRB of University of Texas at Arlington.

A. Part 1

1) Participants: In this study, all of the participants were the residents of Lakewood Retirement Community, and we conducted the study in rooms provided by the community managers. We did not have any restriction or requirement regarding their participation; we accepted anyone in the community who was willing to participate. However, there was a low level of interest in our study, which resulted in a small sample size.

Ten participants agreed to take part in our study, but two of them dropped out during registration. So, we only consider the results of remaining eight participants who completed the registration process, including six men and two women with an average age of 81. None of the participants had training or technical knowledge regarding cybersecurity. All of them used both computers and mobile devices to access the Internet. We compensated each participant with a $25 Walmart gift card for their participation in this part of the study.

2) Procedure: Part 1 of the study included three sessions. In the first session, we explained the study procedures and had them sign informed consent forms. Then the participants were shown a step-by-step demo of the system, followed by learning the password in the registration process. Once the participants confirmed their registrations by successfully logging in twice, we asked their demographic and background information. In the second session, held two days later, the participants attempted to log in with their assigned password, and answered survey questions about their perceptions, experiences, and beliefs regarding computer security. The final session, held one week after the second session, consisted of another login attempt and a survey on user feedback.

3) Results: Two participants dropped out during registration. Seven of the remaining eight participants were successful at entering their password in the second session, and the unsuccessful participant dropped out. So, there were seven participants who returned for the third session, where all of them logged in successfully on their first attempt. This indicates that memorability for CuedR seems reasonable for some older users, but the system may not work for everyone.

TABLE I.   TIME SPENT BY PARTICIPANTS IN PART 1

	Min (s)	Median (s)	Mean (s)	Max (s)
Registration	150	198	219.5	317
1st Login	36	86	126.5	264
2nd Login	41	74	75.1	113

TABLE II.   RESULT OF LIKERT SCALE SURVEY FOR PART 1. THE LAST THREE ITEMS ASK IF THE PARTICIPANTS WOULD PREFER TO USE THE SYSTEM FOR ACCOUNTS OF THE INDICATED TYPE [SD: STANDARD DEVIATION]

Statement	Mean	Median	SD
It was easy to sign up.	9.5	10	0.5
Audio cue was helpful.	7.1	10	3.9
Logging in was easy.	8.4	8	3.6
Password was easy to remember.	7.5	9	3.3
With practice, I could enter quickly.	9.0	10	1.9
Logging in was too time-consuming.	6.4	8	4.0
It would be easy to use in real life.	7.5	7	2.7
I would require to write down.	5.5	8	3.7
Financial	7.8	9	2.8
Email	7.4	7	2.5
E-commerce	8.0	9	2.6

Table I shows the participants' registration and login times. Registration required between three and four minutes for most participants, while login times averaged about two minutes in the second session and 75 seconds in the third session. So, the time spent by participants for logging in is quite high overall.

Table II shows the average scores of the user feedback survey. The survey used Likert scale responses with scores ranging from 1 (*Strongly Disagree*) to 10 (*Strongly Agree*). As our results show, user feedback survey sums up to a mean score between 7 to 10 for the questions concerning the ease of using the system and the prospective of adopting this system in real life for different types of online accounts.

4) Users' Remarks and Suggestions: After the survey, we asked participants for any additional suggestions or remarks about the system. We found that all of the participants found audio cues to be helpful for them during the incremental learning. On the other hand, five of the participants found the verbal cues to be helpful. All of the participants agreed that the font size of the verbal cues, keywords, and keys should be larger. Three participants voiced their concern about the need of scrolling to view the entire portfolio. We incorporated some of this feedback in changes to the layout of the portfolio in the second step of modifications (see §III-B).

Some of the feedback that we received did not result in modifications of the system. One participant suggested that the number of keywords per portfolio should be reduced. This would result, however, in either lowering the security level or increasing the number of portfolios. Another participant recommended that the verbal cue should be shorter, since longer sentences were harder to remember. We note that the goal is not to remember the cue, per se, but rather that the cue is to help users remember the keyword. One participant even commented that he did not utilize the verbal cues. Instead, he created a mental story for the password. Three of the participants mistakenly believed that the audio cue would also be available to them during login as well as at registration. Of course, this would be very insecure, since it would give away the keyword. One participant suggested that we use more cute pictures such as baby animals; however, we did not alter the portfolio since we believe this is more of a personal preference.

5) Our Observations: During the study, we observed that step 4 of the incremental learning was confusing to many participants. It seems that the difference between step 4, which showed the full portfolio without the keys, and step 5, which showed the keys as well, was too subtle for them to notice. The participants then assumed that there was an error or that they had made a mistake. We thus removed step 4 in the second step of modifications (see §III-B). Furthermore, some participants mistakenly clicked on the images instead of entering the corresponding key into the input text field. As a result, we modified the system to bring focus to the input text field in the incremental learning phases and eliminate the input text field entirely in the login phase.

B. Part 2

Having made the second set of modifications to CuedR (see §III-B), we sought to get feedback on these changes. So, we conducted Part 2 of our user study.

1) Procedure: This part of the study had one session, which consisted of registration, a login attempt, and the survey to gain user feedback. In Part 2 of our user study, we were able to recruit only three of the participants who had participated in Part 1 (two men, one woman, average age 82). Each participant was compensated with a $10 Walmart gift card.

2) Results: All three participants could log in successfully on their first attempt, and both registration and login times were improved from Part 1 of the study. The results of Likert scale survey mostly reflected slight improvements from Part 1. We note that the sample size is tiny and any improvement may reflect bias in participants' self-selection to continue the study. However, all of the participants expressed their appreciation of the changes in the interface. They also noted that the portfolios and the keys were presented in a much better manner. Furthermore, the lack of mouse interaction and scrolling needed in the new update were greatly appreciated.

C. Discussion

While the average time for registration (219.5 seconds) and login (75.1 seconds) in our modified system were much higher than the result from original CuedR system (31.2 seconds and 38 seconds, respectively [2]), our participants were able to successfully log in at a great success rate (85.7-100%) with the average of 1.6 tries. Although our data pool is too small to confidently determine their performance, we believe that their registration and login times were affected by many factors, such as their reduced motor skill and sensory abilities. Therefore, the data that we have collected gives a preliminary look into what is the expected performance of this population. We will need a study with bigger pool of participants and an updated study procedure that we derived from this study experience in order to further investigate their authentication performance.

While the participants seem to agree that the audio cues were helpful for them, we observed that almost none of the participants replayed the audio cues. We assumed that the audio cues we provided were understandable enough for the participants that repeated playback was not necessary. Furthermore, we did not ask our participants about their personal preferences toward computer-generated audio read-aloud. For

verbal cues, half of the participants answered that they did not utilize it since they relied more heavily on the graphical cues. We did not have enough data to determine whether the verbal cues could be removed or presented in a different way to save more space, but that could be a potential future work. Three participants utilized the spatial cue, but mostly the position of the graphical cue within the portfolio, and not other information such as the neighboring graphical cues.

The user feedback showed a consensus that the system provides ease of registration and helps in memorizing the assigned password. However, they also agreed that the login process took longer than for traditional textual passwords. A surprising result is that most of the participants, even given the high login success rate, would write down the password. When we asked them about this, most of them simply stated that they did not trust their declining memory, regardless of how easy their passwords are. Some mentioned that keeping a hard-copy backup of their passwords would allow easy retrieval if needed by their family members in future. Most agreed that they were likely to use this system in real life. In fact, a few participants asked us when it would be deployed in real life.

V. INTERNET USAGE, SECURITY BELIEFS AND BEHAVIORS

In this section, we discuss the results of our surveys on the participants' internet usage, security beliefs and behaviors.

A. Internet Usage

The participants had varying experience in using the Internet. All had used online banking. Two participants reported that they had stopped using online banking due to its difficulties. They commented that using the teller or the ATM is more familiar. However, those who continued using online banking reported that they log in frequently (from once every two to three days up to a few times daily). Other online financial services that they utilized regularly include investment, tax reporting, and automatic bill-pay.

All of the participants have made online purchases. Each of them have used email, with three participants reporting that they had multiple email accounts. Two of the participants did not have an account with any of the popular social networks (Facebook and Twitter). All of the participants voiced their concerns regarding their limited knowledge about social networks and difficulty in finding useful resources that can help them navigate the sites safely and effectively. All of the participants read news online through different websites, but none had a subscription to any news website. Only two participants had a subscription with Netflix, while all participants reported that they had also used YouTube for entertainment.

B. Security Beliefs and Behaviors

The participants were more aware and interested in security than we had anticipated. Many of them knew about the FBI's attempt to access an encrypted iPhone used by the alleged San Bernardino attackers and a ransomware attack that happened to a hospital, both of which had occurred around the time of the study. One participant even used a password manager on her devices.

The computer security knowledge of the participants was not very deep, however. All eight participants knew that some sites have secure connections (i.e., HTTPS), but they all indicated that they do not look for the lock icon or the string "https" in the URL bar. In follow-up questions, several participants indicated the belief that if the connection is secure, then the site should be legitimate.

Regarding authentication, four participants indicated that a password is secure as long as it does not contain personal information, like a birthday, name, or telephone number. Most participants believe that it is safe to use a common string as the password as long as it contains multiple character types. The participants also had some typical security behaviors. Most of them owned more than one online account, but they did not use different passwords for them. A few used minor variations in their passwords, such as modifying the endings of their passwords. Furthermore, they also did not change their passwords regularly, unless required by the system.

A key finding of this survey is that all of the users had their passwords written down and stored physically, some in a secure place such as a safe and some out in the open in their living space. They also mentioned that they would write down their passwords regardless of the effectiveness of an authentication scheme. As we asked them if they had written down the password assigned for this study, all of the participants except one reported that they did not write down the CuedR password. However, most of them noted that they would write down the CuedR password if they require to use this scheme in real-life. This means that, for older users, the memorability of passwords may actually be *less* important than for other age groups.

Overall, our study has shed some lights onto the security behaviors and internet usage of older users. However, our sample size was too small to make generalizations from the results. On the other hand, we believe that we have gathered useful experience for working with older users that we would like to share as the recommendation for future studies with this population.

VI. RECOMMENDATIONS

In this study, we spent a large amount of time with each participant, which helped us to gather valuable insights. While we are mindful that this is a preliminary result with a small sample size study, our experience gained from this study informs the following recommendations.

1) Guidelines for User Studies: We have several recommendations that we believe will make a study with older users more pleasant for both the researchers and the participants. First, it is important to establish trust and a connection with the participants. Unlike a typical user study, this study had a more intimate atmosphere. Therefore, the researchers shall put in effort to establish a friendly relationship during the study. Our participants enjoyed spending their time and sharing their stories with us. They also appreciated that they were contributing to society in some form. This was a more motivating factor for them than monetary compensation. Therefore, we suggest that researchers stress the importance and the impacts of their participation in the study.

Surveys with open-ended questions were helpful for the study, as participants often had more details and thoughts that went beyond our anticipated questions. We recommend that researchers set aside extra time between each appointment, since the interviews in our study tended to be longer than we had planned due to the flow of conversation. Also, participants may take longer to process information and execute tasks, especially on a new system. Therefore, the typical 10 - 15 minutes break between two appointments may not suffice.

Researchers need to be encouraging and extra patient with the participants throughout the study.Despite our best efforts, two of our participants did not complete the registration process due to their frustration with the learning curve of a new system. We found it to be helpful to have multiple researchers and equipment at the study. Some participants may require additional assistance in learning the system. However, researchers need to be mindful that their assistance is not patronizing. We suggest asking before offering them help. Furthermore, it is important to speak clearly, loudly, and slowly if needed. We also found it helpful to familiarize the users with the system by tailoring our vocabulary to match their word choices.

Finally, to help the participation rate, older users should be met in a place where they live, preferably in the participants' rooms if they are comfortable.

2) Guidelines for System Design: While designing the system with the first set of modifications, we believed that we had covered most of the obstacles our participants would face. Nonetheless, we still encountered more along the way. Some of our recommendations are common design principles and non-novel. However, these principles are not being implemented in most of the current systems, which inclines us to include them in our guidelines. From the user feedback and our observations, it is clear that the items shown on the screen, especially text, must be large and clear. San-Serif fonts work best for low-vision. Pictures need to have good contrast. As shown by their confusion in between steps 4 and 5 of the incremental learning process, older users could not detect subtle changes on the screen. Therefore, it is important to signal the users to the items that have been modified, or require their attention or interaction.

Furthermore, we learned that scrolling and mouse clicking should be minimized. We observed that some users had difficulty scrolling to view the portfolio, both on mouse and touchpad. They also faced problem re-positioning the cursor to click back on the input text field after scrolling. That's why auto focus is a useful technique to reduce both the time spent by the participants and their confusion with the user interface.

3) How to Improve Security Practices: As we found from our conversations with the participants, they were eager to learn more about security. Therefore, we believe that providing small-scale workshops to this population would be a great way to increase their awareness and improve their security practice and behavior.

One thing that we understand cannot be changed is older users writing down their passwords. Since they do not trust their cognitive ability, we anticipate that they will continue to write down their passwords, no matter how easy the system may be. Given this, providing senior users with random, system-assigned passwords may be beneficial for security overall, since they are writing down the passwords anyway.

4) How to Improve Authentication Performance and Experience: For a graphical password system, we believe that having a simple interface is the key. Mouse clicking and scrolling should be reduced if possible. It is very important to provide detailed instruction on how to use the system. Demos are very helpful in getting the users started. A one-on-one tutorial also helps the users as well. Furthermore, researchers should encourage repetitive practice so that older users can improve their performance with a new system.

VII. FUTURE WORK

For future work, we plan to conduct a study with a larger sample size and clearly defined age groups to get more generalizable results. To this end, we will increase the number of recruitment locations, as we recruited participants from just one location in this study. Since many of our participants expressed a high level of interest in learning about computer security, we will organize small workshops prior to future studies, which in turn, should increase the participation rate by advertising our presence and helping to create a sense of familiarity.

We are also looking into possible solutions to decrease the login time of graphical passwords for older users, where we are considering different ways of modifying the layout of a portfolio to reduce the time for searching a keyword while retaining the security level of the authentication system. Furthermore, we will look into secure and usable ways to leverage the prior knowledge of participants to help them learn the system-assigned keywords in a shorter period of time. Finally, since all participants reported writing down their passwords regardless of the strength and complexity of authentication secrets, we will examine usable ways to increase the security of system-assigned textual passwords, such as by applying pronounceable passwords and chunking.

VIII. CONCLUSION

In this paper, we reported the results of our preliminary user study with older users, through which we aimed to understand their performance with a graphical password scheme and their security perceptions. We leveraged the existing literature on the cognitive limitations of older users to tailor a recently proposed system-assigned graphical password scheme that had offered high memorability for young users in prior studies. We found that most of the older users in our study could remember the password. We used their feedback to identify and then tested several additional improvements to the scheme. This study is also an early step towards learning about the security perceptions and behaviors of older users through our survey and open-ended questions. Based on our experience of conducting a study with older users, we offered recommendations for the usable security research community as well as identified the potential directions for future work to improve upon the study.

REFERENCES

[1] M. N. Al-Ameen, K. Fatema, M. Wright, and S. Scielzo, "The impact of cues and user interaction on the memorability of system-assigned recognition-based graphical passwords," in *SOUPS*, 2015.

[2] M. N. Al-Ameen, M. Wright, and S. Scielzo, "Towards making random passwords memorable: Leveraging users' cognitive ability through multiple cues," in *CHI*, 2015.

[3] M. N. Al-Ameen, K. Fatema, M. Wright, and S. Scielzo, "Leveraging real-life facts to make random passwords more memorable," in *ES-ORICS*, 2015.

[4] C. R. Atinkson and M. R. Shiffrin, "Human memory: A proposed system and its control processes," *K.W. Spence and J.T. Spence (eds), Advances in the psychology of learning and motivation, New York academic press*, 1968.

[5] S. A. Becker, "E-government visual accessibility for older adult users," *Social Science Computer Reviews*, vol. 22 (1), pp. 11–23, 2004.

[6] D. Florêncio, C. Herley, and P. C. Van Oorschot, "An administrators guide to internet password research," in *USENIX LISA*, 2014.

[7] F. Huppert, "Designing for older users," in *Inclusive Design: Design for the Whole Population*, P. J. Clarkson, R. Coleman, S. Keates, and C. Lebbon, Eds. London: Springer-Verlag London, 2003, ch. 2, pp. 30–49.

[8] M. Mcmurtrey, S. M. Zeltmann, J. P. Downey, and R. Mcgaughey, "Seniors and technology: Result from a field study," *Journal of Computer Information Systems*, vol. 51 (4), pp. 22–30, 2011.

[9] J. Nicholson, L. Coventry, and P. Briggs, "Faces and Pictures: Understanding age differences in two types of graphical authentications," vol. 71, no. 10, Oct. 2013, pp. 958–966.

[10] A. Paivio, *Mind and Its Evolution: A Dual Coding Theoretical Approach*. Lawrence Erlbaum: Mahwah, N.J., 2006.

[11] M. Pattison and A. Stedmon, "Inclusive design and human factors: Designing mobile phones for older users," *PsychNology Journal*, vol. 4 (3), pp. 267–284, 2006.

[12] K. Renaud and J. Ramsay, "Now what was that password again? A more flexible way of identifying and authenticating our seniors," vol. 26, no. 4, Jul. 2007, pp. 309–322.

[13] R. Shepard, "Recognition memory for words, sentences, and pictures," *Journal of Verbal Learning and Verbal Behavior*, vol. 6, 1967.

[14] A. Smith, "Older adults and technology use," http://www.pewinternet.org/2014/04/03/older-adults-and-technology-use/, 2014.