# Learning System-assigned Passwords: A Preliminary Study on the People with Learning Disabilities

Sonali Tukaram Marne
University of Texas at Arlington
sonali.marne@mavs.uta.edu

Mahdi Nasrullah Al-Ameen
Clemson University
malamee@clemson.edu

Matthew Wright
Rochester Institute of Technology
matthew.wright@rit.edu

## ABSTRACT

With an increase in cyber attacks, including online password guessing attacks, system-assigned password schemes are studied as alternatives to traditional user-chosen textual passwords. While people with learning disabilities face difficulty in memorizing new information, it is not clear yet if system-assigned passwords would be usable for them. We begin to address this gap with this preliminary study, where we leveraged a recently-proposed graphical authentication scheme that offers multiple cues (visual, verbal, spatial, audio) to memorize system-assigned random passwords. In our single-session study with 14 participants having different types of learning disabilities, all of them could effectively learn system-assigned passwords, and were able to successfully log in using that authentication secret within just one attempt. Based on our findings, we outline the directions for future research in evaluating the authentication performance of people with learning disabilities.

## Keywords

Learning disabilities, user authentication, system-assigned password

## 1. INTRODUCTION

In traditional user-chosen textual passwords, users bear the responsibility of ensuring security of their account by creating a password that should be chosen with creativity and intelligence so that it achieves satisfactory security and memorability. Users, however, typically lack information about what is secure in the face of modern cracking and attacks tools, as well as how to construct memorable strings, memorize them quickly, and accurately recall them later.

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 [4]. As users face difficulties with memorizing information, this becomes more of a concern, making users with learning disabilities more vulnerable to attacks on their online accounts. While numerous studies have examined the efficacy and usability of password alternatives with people from different age and demographics, we still know a little on the usability of an authentication scheme for people with learning disabilities.

Our study aims to address this gap by evaluating the authentication performance of users with learning disabilities. We argue that the burden of password creation should be borne by the system, rather than the user. With system-assigned passwords, the user does not have to guess whether a password is secure, and the system can ensure that all passwords offer the desired level of security. So, in this study, we leveraged a recently-proposed graphical password scheme called CuedR [2, 12], which helps users memorize system-assigned random passwords by providing them with memory cues at both registration and login.

We chose to use CuedR due to its security level and its design based on theories from cognitive psychology [2, 12], 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], the use of verbal and spatial cues to leverage the *depth of processing effect* [3], and the use of incremental learning and audio cues at registration to satisfy the needs of people with special requirements (e.g., older users) [7, 11].These features, we believe, make CuedR interesting to explore for users with learning disabilities. Studies on CuedR showed 100% login success rate for both young (average age: 21) [2] and older users (average age: 81) [12]. In this paper, we are the first to examine how the scheme works for the people with learning disabilities.

## 2. BACKGROUND

In this section, we briefly discuss about different types of learning disabilities [1, 6, 8, 14] and give an overview of the CuedR authentication scheme that we used in our evaluation [2, 12].

### 2.1 Learning Disabilities

Learning disabilities (LD) refer to neurological disorders that alter the brain's ability to process information, which may involve difficulties with basic skills, like reading, writing, spelling, and recall [1, 6, 8, 14]. The most common types of learning disabilities include *Dyslexia*, *Dyscalculia*, *Dysphasia/Aphasia*, *Dysgraphia*, *Auditory Processing Disorder*, and *Visual Processing Disorder* [1, 6, 8, 14].

*Dyslexia*, also known as reading disorder, is a language-based disability in which a person faces difficulty in understanding alphabet, words, and spelling. People with *Dyscalculia*

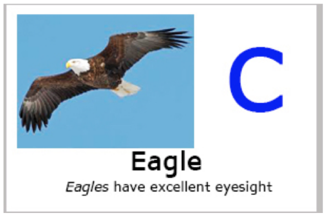


**Figure 1: One keyword with cues in CuedR.**

have poor comprehension of mathematical symbols and digits, and they face difficulty in memorizing numbers and patterns. *Dysphasia/Aphasia* refers to a disability in language, i.e. trouble in understanding language and communication. *Dysgraphia* is associated with impaired writing ability, resulting in difficulty to organize and memorize the letters in a word.

*Auditory Processing Disorder (APD)* makes it difficult for a person to analyze the auditory information, which is not caused due to deafness or difficulty in hearing; rather due to the way auditory information is processed by the brain. APD may affect sequencing the order in which information is heard and processed, e.g., storing "ephelant" for "elephant". *Visual Processing Disorder (VPD)* makes it difficult to process visual information, which is not related to the problem with eyes; rather due to the way visual information is processed by the brain. The examples of VPD include skipping lines while reading.

Any of these disorders might have an impact on learning and memorizing passwords, including both traditional textual passwords, in which letters, numbers, symbols, and ordering are all important, as well as graphical passwords, which require visual processing and can also involve language.

## 2.2 CuedR

CuedR is a system-assigned graphical password system proposed by Al-ameen et al. [2]. 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 [5].

Seng et al. introduced an updated version of CuedR [12] with incremental learning and audio cues in the registration process, where users learn each keyword in five steps: graphical cue with keyword (step 1), verbal cue (step 2), spatial cue (steps 3 and 4), and key (step 5). Audio and visual information are combined together by including audio cues in step 1 (reading the keyword aloud) and in step 2 (reading the verbal cue aloud). The audio is automatically played once the screen for the corresponding step is loaded. We used this updated version of CuedR in our study.

**Reasons for choosing CuedR.** To assist people with LDs with learning, researchers have recommended several strategies, including: pictures should presented with textual information [8]; learning should be multi-sensory [14]; incremental learning should be used [6]; and acronyms (e.g., using a picture or word to link new information with a familiar concepts) should be used in the learning process [8].

The design of CuedR scheme [2,12] is in line with these recommendations. For example, CuedR offers multiple cues, including graphical, verbal, spatial, and audio cues, which makes it a multi-sensory approach. As noted by Lee et al. [14], using a multi-sensory approach is an effective way to support the learning process of people with LDs. CuedR [12] also offers incremental learning, which is particularly helpful for people with LDs to learn new information [6]. In addition, CuedR implements several subtle but important techniques to assist learning for people with special needs, which include using color coding, highlighting text, and a fading effect in the user interface (see [12] for details).

# 3. USER STUDY

Our study examines if the users having learning disabilities could effectively learn system-assigned passwords with the help of memory cues, and remember that information after a period of time, while they were distracted with a separate task in between registration and login sessions.

The study was conducted in a lab setting at the University of Texas at Arlington (UTA). It took about 30-45 minutes for each participant to complete the study. Participants were compensated with a $10 Starbucks gift card for their participation. The study was approved by Institutional Review Board (IRB) at UTA.

To recruit participants, we posted fliers inside the university campus and sent emails to the pupils who are enrolled at the Office for Students with Disabilities (OSD). We had 14 participants in this study (6 male, 8 female, average age: 28, maximum age: 67, minimum age: 18), who came from diverse backgrounds, including Law, Business, Engineering, and Education. Out of the 14 participants in our study, seven had Dyslexia, two had Dyscalculia, one had both Dyslexia and Dyscalculia, two had Dysphasia/Aphasia, one had Dysgraphia, and one had VPD.

## 3.1 Procedure

After signing a consent form, the participants were given an overview of our study. Then the participants registered with CuedR. During registration, each participant was assigned a system-generated secret consisting of five keywords, where each keyword was associated with graphical, verbal, spatial, and audio cues. Then they took part in an interview, lasted for around 10 minutes. In this interview, participants gave their feedback on the experience of learning CuedR passwords at registration. Afterwards, participants were asked to log in using the authentication secret they were assigned during registration. Upon completing the login, participants answered a set of survey questions that asked about their demographics and overall experience of using CuedR. Then they were compensated and thanked for their time.

## 3.2 Results

The registration process with CuedR comprises two phases: learning and confirmation. If a participant fails to enter the authentication secret correctly in the confirmation phase, the system allows her to re-learn the password. In this study, three (21%) of our 14 participants had to re-learn their CuedR password during registration.

*Registration time* refers to the total time taken by a participant to complete both learning and confirmation phases, which also includes any additional time required by participants who had to re-learn their password. The mean registration time for CuedR was 217 seconds (median: 202 seconds), where the maximum registration time was 514 seconds and the minimum registration time was 112 seconds. During login, all 14 participants could log in successfully in one attempt. The mean login time for CuedR was 16 seconds (median: 14 seconds, maximum: 42 seconds, minimum: 9 seconds).

All of our participants reported graphical cues to be most helpful in learning system-assigned random passwords. They also mentioned that the font size was appropriate for them to read keywords and verbal cues. One of our 14 participants has Dysgraphia, and he found audio cues to be helpful in learning authentication secrets. One user mentioned that the use of yellow color to highlight the verbal cues and the keywords was very helpful in learning process.

# 4. DISCUSSION AND FUTURE WORK

The US Department of Education reports that 4-5% of American school-aged children have some kind of learning disability [9]. With the increasing threats of cyber attacks, including online password guessing attacks, it is important to understand if the people with LDs could learn system-assigned random passwords to better protect their online accounts.

We addressed this question through a preliminary study, in which we found that people with LDs could effectively learn system-assigned passwords and log in correctly with just one attempt. The registration time was high in our study, mostly due to the incremental learning process requiring multiple steps to complete the registration. Registration, however, is an one-time process, and incremental learning is considered important for people with LDs [14], so this may be a reasonable trade-off.

Our findings are encouraging to conduct further studies on people with LDs, where a multi-session user study should be conducted in future research to evaluate the long-term memorability of multiple system-assigned passwords.

Although the participants for our user study came from diverse majors and had various types of learning disabilities, they may not generalize to the entire population of Internet users having LDs. In future work, we may conduct a study with larger population, including not only students but also professionals from varying age-groups. With a larger group of participants, we will be able to compare the authentication performance of users in terms of the type of learning disabilities they have. We will also evaluate the individual impact of each type of memory cue (namely, graphical, verbal, spatial, or audio) in aiding users with a certain type of LD to learn system-assigned random passwords.

# 5. REFERENCES


[1] The educator's guide to learning disabilities and ADHD. http://www.ldonline.org.

[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] 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.

[4] A. Das, J. Bonneau, M. Caesar, N. Borisov, and X. Wang. The tangled web of password reuse. In *Symposium on Network and Distributed System Security (NDSS)*. Internet Society, 2014.

[5] D. Florêncio, C. Herley, and P. C. Van Oorschot. An administrator's guide to internet password research. In *USENIX LISA*, 2014.

[6] P. Gregor, A. Dickinson, A. Macaffer, and P. Andreasen. Seeword - a personal word processing environment for dyslexic computer users. *British Journal of Educational Technology*, 34(3):341–355, 2003.

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

[8] Integra. A handbook on learning disabilities. https://www.childdevelop.ca/sites/default/files/files/WAM%20LD%20handbook.pdf.

[9] D. of Education. Twenty-ninth annual report to congress on the implementation of the Individuals with Disabilities Education Act, Parts B and C 2007. year = 2007, howpublished = http://www2.ed.gov/about/reports/annual/osep/2007/parts-b-c/.

[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*, 4 (3):267–284, 2006.

[12] S. Seng, S. Ahmed, M. N. Al-Ameen, and M. Wright. (work in progress) an insight into the authentication performance and security perception of older users. In *USEC*, 2017.

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

[14] L. L. Wah. Development of multimedia learning resources for children with learning disabilities in an undergraduate special education technology course. *Malaysian Education Dean's Council (MEDC)*, 1:29–36, 2007.