

A STUDY OF USING MULTIPLE CUES TO AID PEOPLE WITH LEARNING DISABILITIES IN  
LEARNING SYSTEM-ASSIGNED PASSWORDS

by

SONALI TUKARAM MARNE

Presented to the Faculty of the Graduate School of-  
The University of Texas at Arlington in Partial Fulfillment  
of the Requirements  
for the Degree of

Master of Science in Computer Science

THE UNIVERSITY OF TEXAS AT ARLINGTON

MAY 2017

Copyright © by SONALI TUKARAM MARNE 2017

All Rights Reserved



*To my parents, brother and to my advisor Dr. Matthew Wright.*

## ACKNOWLEDGEMENTS

I would like to extend my heartfelt thanks to Dr. Matthew Wright, my supervisor who guided and motivated me throughout my thesis. I got a lot of exposure to the latest and exciting technologies under his mentorship. Without his invaluable support and encouragement, this would not have been possible.

My heartfelt thanks to my committee members Dr. Zaruba and Mr. Levine, and the computer science department, UTA for their invaluable cooperation, and support. I would also like to thank Mr. Bito Irie for been an exemplary and visionary person, I really appreciate everything he has taught me.

I am grateful to my mother, my father, and my brother who were always there with me in my good and the bad times. Finally, I would like to thank all my friends who helped me through this journey.

April 24, 2017

## ABSTRACT

### A STUDY OF USING MULTIPLE CUES TO AID PEOPLE WITH LEARNING DISABILITIES IN LEARNING SYSTEM-ASSIGNED PASSWORDS

SONALI TUKARAM MARNE, MS

The University of Texas at Arlington, 2017

Supervising Professor: Matthew Wright

Traditional user-chosen passwords often offer weak password security and are prone to password reuse and password patterns whereas system-assigned passwords are secure but fail to provide sufficient memorability.

LDs are problems that affect the brain's ability to receive, process, analyze and store information, i.e. they are disorders of neurologically-based processing. These problems can make it difficult for an individual to learn as quickly and accurately as someone who isn't affected with learning disabilities. Learning disability cannot be cured or fixed but may make it hard to learn and use passwords. With right assistance and with unique learning strategies, we may hopefully produce an authentication system to compensate for the weakness.

CuedR, a graphical authentication scheme that provides multiple cues (audio, visual, verbal and spatial) to help users learn system-assigned passwords, showed promising memorability in prior studies, where 98% of users were able to log in successfully one week after learning their password [20]. In this thesis we explore how whether CuedR's multi-modal recognition-based approach would be helpful for people with LDs.

In particular, we conducted a single-session lab study, with 19 participants. The participants had a 100% success rate using CuedR. Seven (37%) of the participants had to re-learn their password during registration. Our analysis shows that verbal, visual and audio

cues helped the users with learning disabilities to overcome the difficulties to read, hear and interpret information as compared to traditional passwords.

This study is a preliminary work to understand features of a system which would help people with LDs. Also, the findings from this study show potential for future studies aimed at people with LDs.

## TABLE OF CONTENTS

ACKNOWLEDGEMENTS .....	iii
ABSTRACT .....	iv
LIST OF ILLUSTRATIONS.....	viii
LIST OF TABLES .....	ix
LIST OF ACRONYMS .....	x
CHAPTER 1 .....	11
INTRODUCTION.....	11
CHAPTER 2 .....	14
RELATED WORK.....	14
2.1 Password Schemes.....	14
2.1.1 Textual passwords .....	14
2.1.2 System-assigned passwords.....	15
2.1.3 Graphical passwords .....	15
2.2 Learning Disabilities .....	18
2.2.1 Needs of People with Learning Disabilities .....	21
2.3 CuedR .....	22
CHAPTER 3 .....	24
CONTROL CONDITION.....	24
3.1 System Design .....	24
CHAPTER 4 .....	28
SYSTEM DESIGN.....	28
4.1 System Design .....	28
4.2 The features of system design .....	30
4.2.1 Multiple Cues.....	30
4.2.2 Use of Upper Case Keys.....	32
4.2.3 Color Coding.....	33
4.2.4 Repetitive Learning .....	35
4.2.5 Fading Effect .....	35
CHAPTER 5 .....	36

USER STUDY .....	36
5.1 Participants.....	36
5.1.1 Recruitment of Participants .....	36
5.1.2 Demographics .....	36
5.2 Apparatus .....	37
5.3 Procedure .....	37
5.4 Ecological Validity .....	39
CHAPTER 6 .....	40
RESULTS AND ANALYSIS.....	40
6.1 Results of Study 1 (UTA).....	40
6.1.1 Memorability .....	40
6.1.2 Registration Time .....	41
6.1.2 Login Time.....	42
6.1.3 Number of Attempts .....	44
6.1.4 User Feedback & Suggestions.....	44
6.2 Results of Study 2 (RLC).....	47
6.2.1 Registration time.....	47
6.2.2 Login Time.....	51
6.2.3 Number of Attempts .....	56
6.2.4 User Feedback & Suggestions.....	57
6.3 Discussion .....	60
6.3.1 Memorability .....	60
6.3.2 Registration Time .....	61
6.3.3 Login Time.....	61
6.3.4 User Feedback .....	62
CHAPTER 7 .....	63
CONCLUSION .....	63
REFERENCES.....	64
BIOGRAPHICAL INFORMATION .....	72



## LIST OF ILLUSTRATIONS

Figure		Page
Fig 2.1	A Portfolio in CuedR.....	23
Fig 3.1	Control Condition 1: four-character system-assigned password .....	25
Fig 3.2	Control condition 2: six-character system-assigned password .....	26
Fig 3.3	Control condition 3: eight-character system-assigned password.....	27
Fig 4.1	Registration Screen 1: Visual, Verbal and audio cue offered by the system .....	29
Fig 4.2	Registration Screen 2: The system-assigned keyword is highlighted, thus providing spatial cues about the keyword's location and the other objects nearby. ....	29
Fig 4.3	Registration Screen 3: The user needs to enter the key letter (e.g. "N") associated with the assigned keyword (Panda). ....	30
Fig 4.4	CuedR vs Modified CuedR .....	33
Fig 4.5	Color-coding for highlighting Keyword .....	34
Fig 4.6	Color-coding for highlighting Verbal Cue .....	34
Fig 4.7	Fading effect.....	35

## LIST OF TABLES

Table	Page
Table 1 Registration time (seconds) for all 14 participants at UTA.....	41
Table 2 Registration time (seconds) for CuedR at UTA.....	42
Table 3 Login time (seconds) for all 14 participants at UTA .....	43
Table 4 Login time for CuedR at UTA .....	44
Table 5 User feedback for CuedR at UTA .....	44
Table 6 Likert scale feedback table for CuedR at UTA.....	45
Table 7 Notable Positive Feedback .....	46
Table 8 Notable Negative Feedback.....	46
Table 9 Registration time (seconds) for CuedR 1 for all 5 participants at RLC .....	48
Table 10 Registration time (seconds) for CuedR 2 for all 5 participants at RLC .....	48
Table 11 Registration time (seconds) for CuedR 1 at RLC.....	49
Table 12 Registration time (seconds) for CuedR 2 at RLC.....	50
Table 13 Registration time (seconds) for Control Condition 1 at RLC .....	50
Table 14 Registration time (seconds) for Control Condition 2 at RLC .....	51
Table 15 Registration time (seconds) for Control Condition 3 at RLC .....	51
Table 16 Login time (seconds) for CuedR 1 for all 5 participants at RLC.....	52
Table 17 Login time (seconds) for CuedR 2 for all 5 participants at RLC.....	52
Table 18 Login time (seconds) for all 5 participants during control condition 1 .....	53
Table 19 Login time (seconds) for all 5 participants during control condition 2 .....	53
Table 20 Login time (seconds) for all 5 participants during control condition 3 .....	53
Table 21 Login time for CuedR 1 at RLC .....	54
Table 22 Login time for CuedR 2 at RLC .....	55
Table 23 Login time for Control Condition 1.....	55
Table 24 Login time for Control Condition 2.....	56
Table 25 Login time for Control Condition 3.....	56
Table 26 Number of Attempts for Control conditions at RLC .....	57
Table 27 User feedback for study at RLC .....	58
Table 28 Likert scale feedback table for study at RLC .....	58
Table 29 Notable Positive Feedback .....	59
Table 30 Notable Negative Feedback.....	59

## LIST OF ACRONYMS

UTA – University of Texas at Arlington

RLC – Research & Learning Center at Fort Worth Museum of Science and History

FWMSH - Fort Worth Museum of Science and History

LD – Learning Disability

LDs – Learning Disabilities

## CHAPTER 1

### INTRODUCTION

For authentication of users, most systems use user-chosen textual passwords. Users typically select these passwords by using some common phrases or strategies that make them easy to remember. While users often think that such passwords are secure, they typically do not understand the requirements to make a secure password. Users also find it challenging to create unique and strong passwords for the many accounts they have, such as for email, online banking, social networks, credit cards, etc. Furthermore, the password restriction policies meant for creating a strong password do not necessarily lead to strong passwords, but they do harm memorability [40, 41]. Thus, user selected passwords are a poor choice of security.

A more secure approach is to use system-assigned passwords. System-assigned passwords have a guaranteed level of security against dictionary and guessing attacks, and the level of security is tunable by the system administrator. Random strings, however, are difficult to remember, thus affecting the memorability of the password [43]. Even when natural language words are used to generate a system-assigned password, they fail when it comes to memorability [7, 42].

The number of student aged 3-21 was 6.5 million in year 2013-14 as reported to IDEA (Individuals with Disabilities Education Act) which is about 13 % of all the public school students. Out of these, 35% had specific learning disabilities, which counts to be a considerably large number.

For people who have learning disabilities like dyslexia, visual processing disorders or difficulties in interpreting visual information, many existing authentication systems may be difficult

to use. Having a system with features designed to assist these individuals might be valuable for both security and usability.

Learning disabilities or learning disorders is not a problem with the intelligence. It's just that the brain is differently wired which can lead to difficulties in learning information and even processing the information. Common types of learning disabilities include difficulties in reading, hearing differences between sounds, interpreting visual information, speaking and writing. In order to make the authentication system more usable to the people with LDs, the system should provide the information in such a way that it makes it easy to read, hear and interpret the information.

This thesis addresses the learning difficulties faced by the people with LDs. We explore an existing CuedR system, whose features might be helpful for people with LDs to learn their password and be able to recall it in future. We seek to understand which features of CuedR are helpful and whether we need any modification that would cover the obstacles people with LDs would face. We reviewed the literature of human memory and various strategies that have been used to help in the learning process of people who have different types of LDs. Since people with LD have difficulties in reading, writing, in math, spelling, etc. and considering the fact that almost 80% of all people with LDs have dyslexia i.e reading disability, we developed a system that uses multiple cues to help people with LDs learn their password by considering the difficulties they face.

To understand the impact of CuedR, we conducted a single-session in-lab user study with 19 participants using two different procedures. For the first procedure with 14 participants, only three participants had to re-learn their password, whereas the remaining 11 participants learned it successfully on the first attempt. For the second procedure with five participants, four had to re-learn it, possibly because of the multiple password interference effect. This implies that

the system provided sufficient assistance to overcome LDs, but having a multiple passwords may be a concern for these users. This is a preliminary work to understand what design features might be helpful to overcome learning difficulties faced by people with LDs. The findings of this study could be a potential future work to studies aimed at people with LDs.

## CHAPTER 2

### RELATED WORK

Traditional user-chosen passwords offer uncertain and often weak security whereas system-assigned passwords provide considerable security but fail to provide memorability. To address these limitations, we argue that the system should assign secure passwords and also help users to memorize and recall them. Though the existing textual passwords have a good number of issues, we still use them for many systems. There has been a lot of research to address and improve the textual-passwords. In this section, we discuss key findings in textual passwords, system-assigned passwords and graphical passwords with their limitations and we discuss the differences between recognition-based and recall-based password mechanisms.

#### 2.1 Password Schemes

##### 2.1.1 Textual passwords

In this scheme, the user creates his own password. An ideal password would be a one which is easy to remember but difficult guessing attacks, making the system secure [44]. Users create passwords that are easy to recall, but these are often vulnerable to guessing, dictionary and brute-force search attacks. [1]. Users' propensity to handle alphanumeric passwords insecurely arises largely from limitations of long-term memory [2], as users face difficulty in remembering long and complex passwords. Recent surveys have shown that users often choose - short, alphabetic-only passwords consisting of the names of family or friends, pets, and even the word "password" [3, 4]. Users often write down their passwords, share passwords with others, and use the same password for multiple systems, sometimes with a single digit added on the end [4, 5]. In this process of creating and remembering a strong password, either the security of password is neglected or else the memorability is affected.

### 2.1.2 System-assigned passwords

In a system-assigned password scheme, the passwords are randomly generated. They can be random words, passphrases or even pronounceable passwords. A random password can be any random string, e.g. “hgsbrmk”, which does not make any sense making it difficult to remember. In an attempt to make system-assigned passwords memorable, the idea of *passphrases* was introduced. A passphrase is a set of natural-language words separated by spaces [42, 45]. In a system-assigned scheme, the words are randomly selected from a set English dictionary. In spite of having natural-language words in this kind of password, passphrases have been shown to offer similar memorability and usability as to system-assigned random strings [42]. Also, having a dictionary for these words was a major concern as the number of words in the dictionary made little difference in usability and security metrics. In a study to explore system-assigned passwords Shay et al. [42] found that user disliked system-assigned passwords and passphrases. But the users performed well in terms of accuracy and login time when they were assigned a pronounceable password. A pronounceable password consist of pronounceable natural-language words which are concatenated to form a password. However, early work by Gasser [68] has shown that the password generation process used by pronounceable password systems, uses frequencies with which syllables appear in English, which makes it vulnerable to guessing attacks [46].

### 2.1.3 Graphical passwords

Graphical passwords have been proposed as an alternative to traditional text based passwords. This was motivated by the psychological fact that human can remember images better than text [47, 48, 49]. Research [71, 72] has shown that cues aid memory retrieval and that



authentication systems should provide cues to the users to help them to remember their passwords. Some of the graphical password schemes are discussed below.

In general, graphical passwords are categorized into four main categories- recognition-based, recall-based, cued-recall and cued-recognition schemes [50]. In recognition-based schemes, to login successfully, the user has to recognize the image(s) that can be either assigned to him or selected by him during registration. In recall-based schemes, the user must recall and reproduce their password. This is a difficult memory task [22, 51] as the user has to recall the password from his memory without any help or cues. Comparison study between recognition and recall shows that recognition is easier as compared to recall [71]. In cued-recall, cue(s) that can help to remember and retrieve information are provided to the user. Cued-recall password schemes provide better memorability than recall-based password schemes, whereas recognition-based leads to more accuracy as compared to cued-recall based password schemes [69, 70]. Cued-recognition password scheme provides multiple cues – visual, verbal and spatial to help users in remembering their password. The users choose the cues, that they think are best for them to remember their password.

Draw-A-Secret (DAS) was the first recall-based graphical password scheme proposed by Jermyn et al. [52, 54]. In this scheme, users draw something on a 2D grid and the coordinates of the grid cells are stored as the DAS password. To authenticate, the user needs redraw the same picture or pattern. DAS offers the same memorability as textual passwords, but lack of user studies we have little information on its usability and effectiveness as a graphical password scheme [53, 55]. Also, J. Thorpe [56] found that users often choose predictable patterns and simple passwords.

In BDAS [57], which is similar to DAS, background images were added to encourage users to create complex passwords. A comparison study between DAS and BDAS showed that

adding background image reduced symmetry within the password and users created longer passwords. BDAS provides enhanced usability and security as compared to DAS [57, 58]. Research on various other recall-based password schemes show that these passwords are as difficult to remember as traditional textual passwords [59].

Passfaces [53, 61] is a recognition-based password scheme in which the selects human faces as their password. For authentication, the user recognizes the faces that selected by them during registration. A study conducted by Brostoff [62] showed that a Passfaces password is easier to remember as compared to a traditional textual password. Valentine [63] found that user could login successfully using Passface passwords at various intervals over a period of 5 months.

Cued-recall is a password scheme in which the user selects particular points on the image(s). PassPoints, Cued-Click Points (CCP) and Persuasive Cued-Click Points (PCCP) are few cued-recall based password schemes [53]. In PassPoints scheme, user selects five points on a system-assigned image. To authenticate the user needs to select these five points in the correct order. The main difficulty in PassPoints was identifying the ideal precision and system tolerance levels for re-entering the click-points [53, 65]. CCP is a click-based scheme in which the user selects five points, one from each of the five images shown during registration. The user then needs to recognize these points correctly during login. A study of CCP showed that confirmation and login success rates of 83% and 96% respectively [66]. PCCP was developed using CCP as base system [53, 67]. It encourages users to select a more secure password than CCP by providing randomly positioned viewports. Viewports avoid known hotspots [60, 67]. PCCP and CCP have showed favorable results in terms of usability and security though PCCP requires additional effort to learn the password during registration [67].

Taking advantage of the fact that humans can remember images better than text [49], use of graphical passwords has helped to prove that they are better in terms of memorization as

compared to traditional textual passwords and system-assigned passwords. Al- Ameen et al. [6] performed a study of the memorability of passwords using a cued-recognition based password scheme called CuedR that provides multiple cues (verbal, spatial and verbal). After one week of registration, it was found that 100% of the participants could log in. User feedback showed that 84% of the users preferred to use this scheme over traditional textual passwords in real life and were satisfied with usability of CuedR. [6]. CuedR will be discussed in detail in Section 2.3.

## 2.2 Learning Disabilities

A learning disability is a neurological disorder that alters brain's ability to process information. This has nothing to do with the intelligence of the person. These disorders affect the learning process and may involve difficulties with basic skills like reading, writing, spelling, recalling and/or math.

In this section, we discuss about some common types of learning disabilities [33-37]. Learning disabilities are usually categorized by school-area skill set [34].

### *Dyslexia: learning disabilities in reading:*

Dyslexia, also known as reading disorder, is a language-based disability in which a person has trouble understanding words, reading comprehension, spelling, alphabet and sometimes speech. This often results in an effortful and slow learning process. Dyslexia is a lifelong condition that cannot be cured, but with proper help and appropriate techniques, people who suffer from dyslexia can learn to read and write. Research indicates that reading disorders are not a vision issue but they are caused by impairment in phonological processing [26].

*Dyscalculia: learning disabilities in math:*

People with dyscalculia have poor comprehension of math symbols and digits. They also have difficulty in memorizing and organizing numbers and patterns, counting, solving math problems and learning tables. This reduces the speed of math problem solving and even playing strategical games [34].

*Dysphasia/Aphasia:*

This is a disability in language i.e. trouble in understanding language and communication. People with dysphasia may have difficulty in understanding language, listening or writing. This can affect basic functions like identifying words, comprehension and speech.

*Dysgraphia:*

Dysgraphia is a condition that is associated with impaired writing ability. This may result in difficulty in organizing, sequencing and storing letters of a word. People with dysgraphia might struggle with retrieving information from their brain and putting that information correctly on paper. Dysgraphia can cause trouble with reading maps, drawings or shapes, organizing words and shape-discrimination.

*Auditory and visual processing problems:*

This disorder occurs when either eyes or the ears are not working properly, which may result in learning difficulties [36].

Auditory processing disorder (APD), also known as Central auditory processing disorder (CAPD) is a condition that makes it difficult for a person to analyze the auditory information taken in through ears. The person cannot recognize even a subtle difference between sounds in words.

This condition is not caused due to deafness or difficulty in hearing but it is due to the way the auditory information is processed by the brain. This may affect the understanding and learning of any information heard by the individual. An individual with APD may not be able to understand instructions, hence resulting in trouble in recalling this information. APD may also affect in sequencing difficulty i.e. the order in which information is heard and processed. For e.g. storing “ephelant” for “elephant”.

Visual processing disorder is a condition that makes it difficult to process information taken in through eyes. This is not a problem with eyes; rather it is due to the way brain processes the information that is seen visually. The way the brain interprets this information makes it difficult to process it and store it for recall. This disorder is difficult to diagnose as it doesn't show up in vision tests. There are various types of visual processing disorders identified with a wide range of effects caused by them.

Problems with visual processing disorder includes reversing letters or numbers ( e.g. 'b' with 'd', 'p' with 'q', etc), trouble finding out specific information, skipping lines while reading, problems with coordinating eyes with movement of body parts, difficulty in identifying objects with missing parts or even difficulty in sequencing the information. These are the effects of the brain not processing the information seen accurately.

*Attention Deficit Hyperactivity Disorder (ADHD):*

ADHD is a condition in which there is difficulty in focusing and paying attention, hyperactivity and difficulty in controlling the behavior. Though this is not considered as a learning disability, previous research indicates that people who have ADHD might also have learning disabilities. ADHD plus learning disability can be extremely challenging. Three types of ADHD are recognized – inattention, hyperactivity and impulsivity.

There has been limited research on creating web interfaces, learning software and appropriate learning environment for people with LDs. As each LD type needs to be addressed differently, the existing authentication systems might not necessarily cope with the difficulties of LDs. Reading system-assigned textual passwords, can be challenging for people with reading disability because of the text formats and text and background color. For people with visual processing disorder, images size used by graphical password schemes might be large enough to process it efficiently. Also, with graphical password schemes like Passfaces, that have image portfolios, it can be confusing to focus on the correct image that forms the password. By developing an authentication system which reduces unnecessary complexities and has features that can help in learning and retaining the password, we might be able to help people with LDs to overcome their difficulties.

#### 2.2.1 Needs of People with Learning Disabilities

To select the most appropriate strategies to assist and support the learning to people with learning disabilities and to design an authentication system considering those strategies, we studied the needs of people with different types of LDs.

A Handbook on Learning Disabilities [26] helped us in understanding the needs of people with LDs. Almost 80% of all people with LDs have Dyslexia, i.e. reading disability. In order to assist people with LDs, the Handbook suggests that written material should be supplemented with pictures, illustrations, gestures and color coding to make it multi-sensory, new terms should be explained, instructions should be repeated, and acronyms (e.g. use of visual picture or letter/word to link unfamiliar information with familiar/already known information) should be used when helpful [26].

### 2.3 CuedR

In this section, we will discuss the CuedR authentication system.

CuedR is a recognition-based graphical authentication system proposed by Al-Ameen et al. [20] that helps the user to learn and memorize a random system-assigned password. Users are assigned a series of five random keywords. Each keyword is mapped to single-character key that forms a five-character password. A portfolio of 16 images is shown to the user together with the keyword and the key assigned by the system. This acts as a visual cue. CuedR also provides a verbal cue i.e. a phrase associated with the image. The location of the images on this portfolio is fixed across the registration and login, which creates a *spatial cue* that makes it easier for the user to recognize the keyword and identifying the correct key letter to type.

In Figure 2.1, for an example “Elephant” is shown with a picture of an elephant), a related fact which is “Elephants can get sunburned”, and the key letter (‘a’). Each portfolio has 16 keywords, all shown with these accompanying cues and randomly assigned key letters. These portfolios are same throughout the registration and login sessions. The user enters the key letter corresponding to the image into the password field to move to the next portfolio. For successful login, the user needs to enter all the keys correctly in the key field and in the same order that it was assigned during registration. Irrespective of any incorrect key entered during login, the user has to enter all five keys. CuedR offers 20 bits of entropy considering distinct 16 keys displayed on each of five portfolios.

Key: [ ] [Next>>]




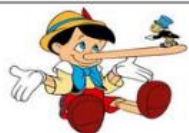





 <p><b>Elephant (a)</b> <i>Elephants can get sunburned.</i></p>	 <p><b>Radio City Music Hall (b)</b> The nickname of <i>Radio City Music Hall</i> is 'Showplace of the Nation'</p>	 <p><b>Hummingbird (c)</b> <i>Hummingbirds</i> are among the smallest of the birds</p>
 <p><b>Pinocchio (e)</b> The <i>Pinocchio</i> puppet built for the film was lost for over 50 years</p>	 <p><b>Sunflower (z)</b> Wild <i>Sunflower</i> typically does not turn toward the sun</p>	 <p><b>Rice (g)</b> <i>Rice</i> has been cultivated for eight thousand years</p>
 <p><b>Candle (k)</b> Scented <i>candles</i> help to eliminate odor from the room</p>	 <p><b>Clownfish (m)</b> Animation movie 'Finding Nemo' features a family of <i>clownfish</i></p>	 <p><b>Table Tennis (n)</b> Top players in <i>table tennis</i> often smash the ball at speeds exceeding 100 mph</p>

Fig 2.1 A Portfolio in CuedR

A number of user studies to study the impact of system-assigned graphical passwords have been conducted. A multi-session study conducted on seven different graphical passwords showed varying login success rate of 93-98% [20]. CuedR offers sufficient security and at the same time the use of multiple cues improves the memorability of random system-assigned passwords.



## CHAPTER 3

### CONTROL CONDITION

In this chapter, we will discuss the control condition, which uses a textual system-assigned password. This scheme is a recall-based password scheme. In 3.1 we describe the system and the design choices.

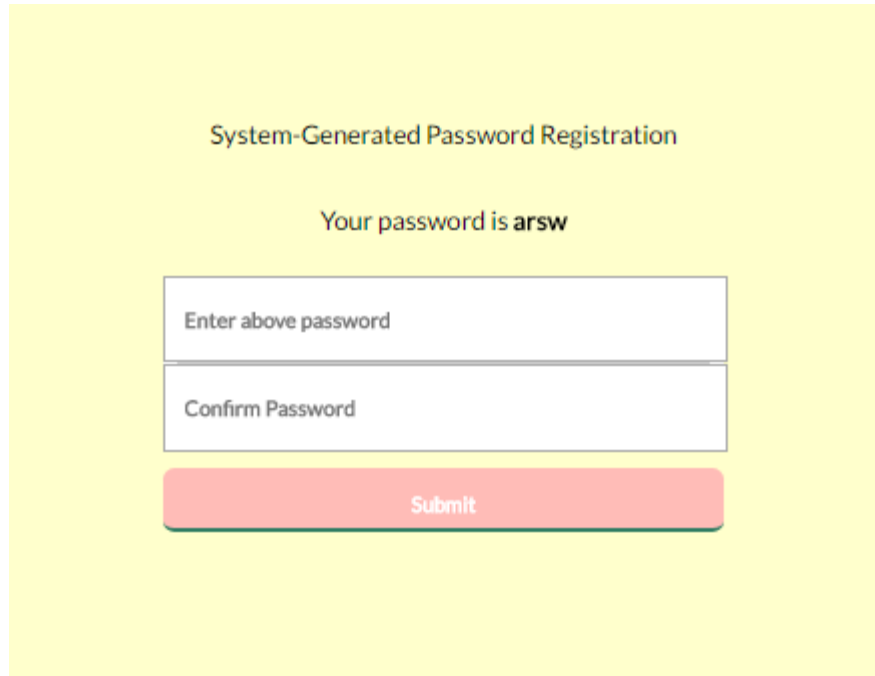
The system-assigned password scheme provides users with a random alphabetical password. It is the user's responsibility to learn that password for future logins. Users can have their own strategy to learn and memorize the password.

For our control condition, we designed three different system-assigned password schemes. Each scheme required the users to learn a similar text-based authentication mechanism to login to a website. The website of the first scheme provides a random four character system-assigned password. The site for the second scheme provides a six character system-assigned password. Finally, the third scheme provides an eight character system-assigned password. All the three conditions are pure recall based mechanism, meaning that the user recalls the passwords from the memory without any cues. Each condition has a different entropy level.

#### 3.1 System Design

We now discuss the designs for the three control conditions.

Condition 1: In first condition, we use a four-character system-assigned password. The password is generated using random four letters, all lowercase, from set {a-z}. The user needs to learn the password during registration and enter it twice in the password fields (Fig 3.1).



The image shows a registration form on a yellow background. At the top, it says "System-Generated Password Registration". Below that, it says "Your password is arsw". There are two input fields: the first is labeled "Enter above password" and the second is labeled "Confirm Password". Below the input fields is a red "Submit" button.

Fig 3.1 Control Condition 1: four-character system-assigned password

Control condition 1 provides entropy of

$4 * \log_2(26) \sim 19$  bits. Note that CuedR provides 20 bits of entropy, so it is slightly more secure than the first control condition.

Condition 2: In control condition 2, we use a six-character system-assigned password (Fig 3.2), but we do not sample from the alphabet completely uniformly.

System-Generated Password Registration

Your password is eqcpja

Enter above password

Confirm Password

Submit

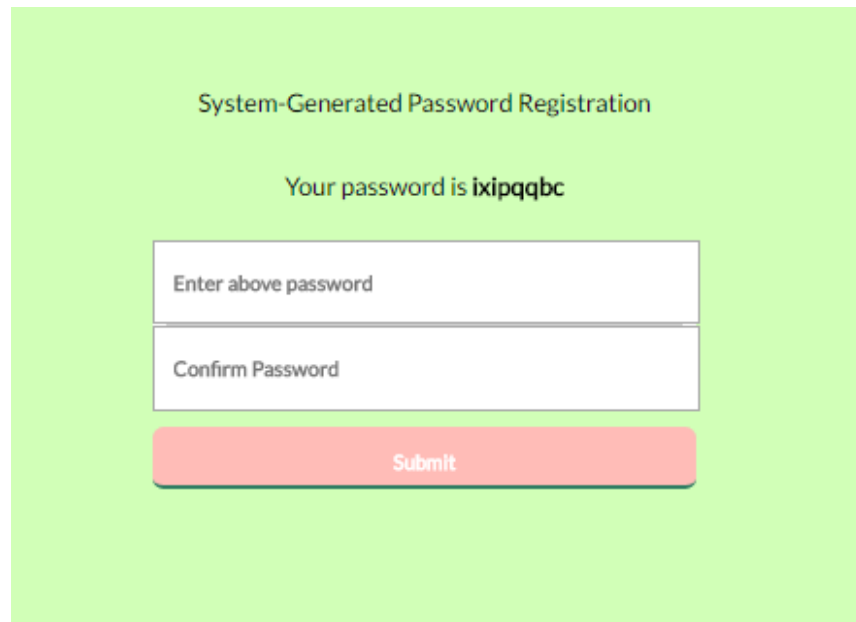
Fig 3.2 Control condition 2: six-character system-assigned password

From the findings based on LD types [34], we changed the choice of letters included in the password. People with LDs have difficulty in understanding letters, i.e. they might interpret letters backwards. The common letters that are often confused and reversely interpreted by people with LDs are p/q, b/d, o/a and i/l [34]. To understand the impact of this effect on password memorability, we modified letter selection in this control condition to ensure that some potentially confusing letters would appear. Specifically, we select two letters from the set {p, q, b, d, o, a, i, l} and then select the remaining four letters from set {c, e, f, g, h, j, k, m, n, r, s, t, u, v, w, x, y, z}. This password offers entropy of

$2 * \log_2 (8) + 4 * \log_2 (18) \sim 23$  bits, which is more than CuedR. Because of this, and the modified letter selection, we do not treat this as a fair condition for comparison with any other condition in the study.

Condition 3: This condition provides a random system-assigned password of eight characters uniformly selected from the full set of 26 letters (a-z) (Fig 3.3). This password scheme provides entropy of

$$8 * \log_2 (26) \sim 38 \text{ bits.}$$



The image shows a registration form with a light green background. The text 'System-Generated Password Registration' is centered at the top. Below it, the password 'ixipqqbc' is displayed in bold black text. There are two input fields: the first is labeled 'Enter above password' and the second is labeled 'Confirm Password'. Below the input fields is a red 'Submit' button.

Fig 3.3 Control condition 3: eight-character system-assigned password

For all three control conditions, we have some design choices in common. All are pure recall-based password mechanism, as we do not provide any cues to help the user to learn and memorize the password. Considering the fact that users with LDs have reduced reading ability [33-37], we used a font-size of 16px (medium) and font weight as “bold”, to display the password during registration. Each website has a different background color to help user avoid any confusion between the sites.

## CHAPTER 4

### SYSTEM DESIGN

In this chapter, we will discuss the design modifications that we made to the CuedR authentication system. A version of these modifications was previously presented by Seng et al [1]. We also discuss the reasons for modifying the features of original CuedR.

#### 4.1 System Design

The CuedR system has two functionalities: Registration and Login. Registration allows a new user to create an account. The user will be assigned randomly generated five keywords. The five keywords together form the password and will be displayed one after the other on the screen. To improve the memorability, each keyword will have corresponding visual, verbal, audio and spatial cues. For example the keyword “Panda” will have an audio file that will read out loud “Panda” and a picture of a panda. The phrase (verbal cue) will also be read out loud. See figure 4.1 for a screenshot of registration process where the user sees multiple cues. The audio for verbal cue can be replayed multiple times with “Play Audio” button. Then, a portfolio of 16 different images will be displayed where previously assigned image (Panda) will be highlighted, which also shows the spatial cue of where the panda is in the portfolio and what is around it. The image has an associated key letter. For e.g. for “Panda” we have “N” as key letter. The user then types “N” (non-case sensitive) in the key input box and proceeds. This is repeated until all five keywords are learnt by the user.

During login, the user will be shown five different portfolios of 16 different images each. The user has to recognize the system-assigned password and enters the corresponding key letters, one by one. Only if all five keywords are correct will the user be authenticated. If the user

enters even one incorrect keyword, an error is displayed and the user has to start the login process again. Since the user inputs the keywords by pressing the key on keyboard, this technique is resistant to shoulder-surfing [10].



Fig 4.1 Registration Screen 1: Visual, Verbal and audio cue offered by the system



Fig 4.2 Registration Screen 2: The system-assigned keyword is highlighted, thus providing spatial cues about the keyword's location and the other objects nearby.

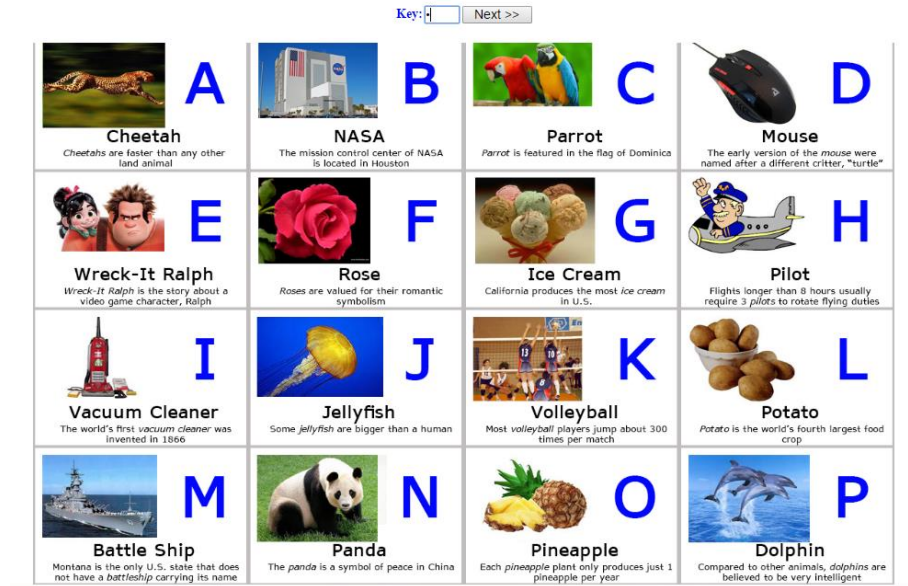


Fig 4.3 Registration Screen 3: The user needs to enter the key letter (e.g. "N") associated with the assigned keyword (Panda).

## 4.2 The features of system design

In this section, we will discuss the design features of the system and the reasoning behind choosing the design.

### 4.2.1 Multiple Cues

Multiple cues are provided by the system to aid the memorability of a system-assigned password. It is difficult to remember a random system-assigned password. This authentication system provides four different types of cues - visual, verbal and audio and spatial making it a multisensory approach to assist people with LDs. These cues together might help the user with the learning process, thus helping the memorability of the password. Lee et al. [73] find that using multimedia technology (e.g. text, images, audio, video, etc.) for instructing people with LDs is the

most promising way to support their learning process. We now discuss each of these cue types in turn.

#### Audio cue:

The system has audio clips associated with each keyword. The audio clips consist of a computer-generated reading of the keyword and the phrase (verbal cue). For the keyword “Panda” for example, the fact that “The *panda* is a peace symbol in China” is read out as a part of the audio cue. The phrase can be replayed multiple times. A study [11] to evaluate role of audio cues in student engagement and learning outcome in an educational setting, demonstrated that systematic use of audio cues improved the learnability by 38% relatively and also improved the relative memorability, i.e. long-term retention by 40%. Providing audio cues serve as one of the supplemental multisensory strategies to assist reading.

Humans have a very sensitive and well-developed auditory system. Experimental studies based on audio and visual recall [12, 13, 14] shows higher auditory recall compared to visual recall. In particular, visual recall was 88% with precision of 72% whereas auditory recall was 91% with precision of 100%. Audio cues can also be helpful to convey information to visually impaired people. Finally, people with Dyslexia might find audio helpful as the audio contains verbal cues which act as the explanation of the keywords.

#### Visual cue:

The images act as visual cues. Visual passwords have superior memorability as compared to traditional text based passwords [49, 59, 62]. The science behind this is explained by two different theories of how images are encoded and stored in the mind. One theory states that both the image and the verbal cue are encoded in distinct ways. [17], i.e. the image is



encoded in memory as image code and the text is encoded in memory as a textual code. The other theory [16, 18, 19] states that images are encoded in memory using dual-encoding technique i.e. image is encoded as image code as well as with the associated text code. Dual-encoding helps in increased recall rate. Providing visual cues (images) helps people with LD [26] especially with Dyslexia.

#### Verbal Cue:

Verbal cues are text phrases or facts associated with the keyword. They help in learning and memorizing the keyword. Use of color coding and highlighting for visual focus reduces the efforts required to focus for reading [26, 27]. A study of CuedR [20] in which spatial cues were studied together with verbal cues, found that the participants had 98% login success rate when both spatial and verbal cues were provided, whereas for schemes with only visual cues, the login success rate was 93-95%. Thus, when multiple cues (verbal and graphical) are combined, there are greater chances of successful login as compared to a single cue.

#### 4.2.2 Use of Upper Case Keys

People with LDs, especially the ones that cause trouble in reading letters might reflect specific problems in processing small case letters like p/q, i/l, o/a and b/d [27]. This might affect the ability to take the information and store it in mind in a correct way. To help to overcome this difficulty, we used upper case letters to display the key letters. A gray background behind the verbal cue was removed to enhance readability [31] and have high contrast of black and white. We used APHont font style, a sans-serif font recommended by Becker [32]. O'Brien [75] predicted that people with LDs, dyslexia in particular would require larger font size. To enhance the readability, we increased the font size of the key letters.

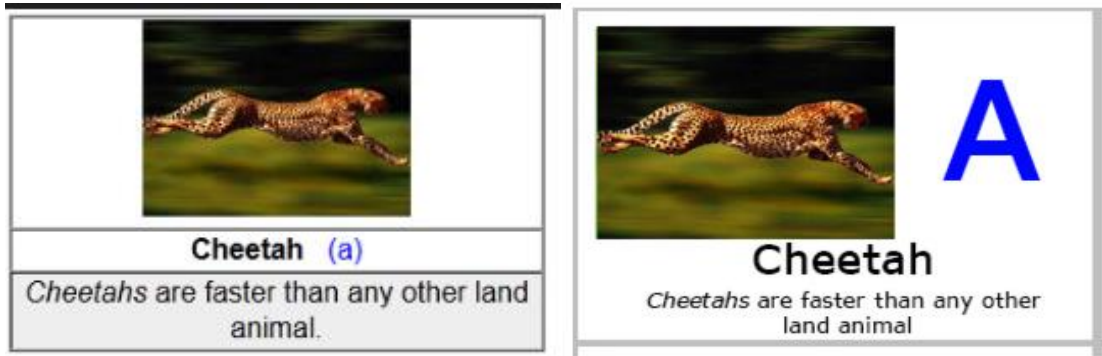


Fig 4.4 CuedR vs Modified CuedR

#### 4.2.3 Color Coding

Color coding i.e. use of colors in background to highlight important text, signs, symbols, etc. can be used to visualize and understand a problem in a better way [74]. Previous research on use of background colors showed that colors can be useful for reading on the screen [29]. Gregor [29, 30] used brown & dark green and blue & yellow as they were chosen by people with LDs. Almost 38% of total people with Dyslexia chose black and yellow [28] as the preferred color coding for highlighting text. Also, black and yellow have a high contrast value (19.6). We used yellow color to highlight the Keywords (Fig 4.5) and the verbal cues (Fig 4.6) to increase the visual focus.

Play Audio Continue

Cheetah



Fig 4.5 Color-coding for highlighting Keyword

Play Audio Continue

Cheetah



*Cheetahs* are faster than any other land animal.

Fig 4.6 Color-coding for highlighting Verbal Cue

#### 4.2.4 Repetitive Learning

Repetitive learning offers better chances to achieve higher productivity and improve the user's experience. Repetition can also increase familiarity with the system. From prior work studying strategies to assist people with learning disabilities [27, 29, 30], we found that using repetitive learning to present information visually can help people who have LDs. In CuedR, we used rote memorization as well as incremental learning for the learning phase. We incrementally displayed cues in sequence: graphical cues with keyword, verbal cue, spatial cue and key. To help with repetitive learning, we introduced one extra step for the learning phase, with image portfolio without keys.

#### 4.2.5 Fading Effect

We applied a fading effect to the image portfolios that are shown during registration phase. The image that is assigned by the system will be highlighted with a yellow box and the remaining images in the portfolio will be faded. This was added to bring focus to the assigned image. Fig 4.7 shows a part of portfolio that has the fading effect. Highlighting important concepts with colors [74] can be a potential support for people with LDs.

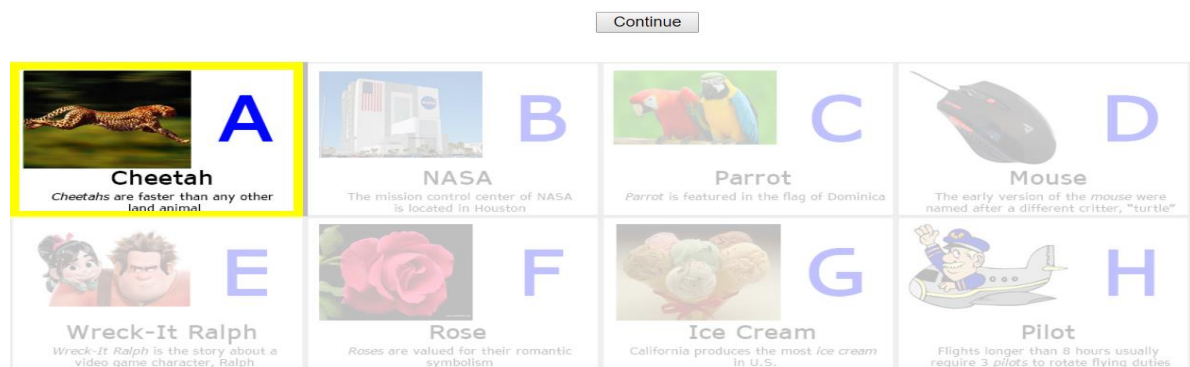


Fig 4.7 Fading effect

## CHAPTER 5

### USER STUDY

In this section, we will discuss the user study to explore the impact of multiple cues on learning process of people with LDs. The study was conducted first in our lab at University of Texas at Arlington (UTA) and then at the Research and Learning Center at Fort Worth Museum of Science and History. Both parts of the study were approved by Institutional Review Board (IRB) at UTA.

#### 5.1 Participants

##### 5.1.1 Recruitment of Participants

For our user study we recruited 19 participants: 14 students studying at UTA and five from volunteers at the Research and Learning Center (RLC) at the Fort Worth Museum of Science and History (FWMSH). These participants are people who have LDs like dyslexia, visual processing disorder or audio processing disorder. To recruit the participants at UTA, flyers were posted inside the university campus and emails were sent to people who are enrolled at Office for Students with Disabilities (OSD) as students with disabilities. These participants were compensated with \$10 Starbucks gift card. For RLC recruitment, we posted flyers on the FWMSH website and also around the research center. Visitors at FWMSH were given handouts of the flyer. There was no compensation given to the participants at RLC.

##### 5.1.2 Demographics

In the study conducted at UTA and RLC, we had 19 participants, where nine were men and ten were women. The average age of participants was 30.88, with the oldest participant being

67 years old and the youngest one being 18 years old. The participants came from different backgrounds including Law, Business School, Management, Engineering, Education, etc.

All the participants completed the study conditions included in one session.

## 5.2 Apparatus

To understand the impact of multiple cues on memorability, we used modified CuedR. Our CuedR implementation logs the time taken by the participant to register and to login as well as the number of login attempts. A control condition with three experimental conditions was developed, which has registration and login and logs the time for both.

## 5.3 Procedure

This study was a two-phase single-session study which takes approximately 30-45 minutes.

### Study 1 – User Study at UTA

#### First Session:

Before we began the user study, we showed each participant a five-minute-long demonstration of CuedR to introduce the system and to help them to understand what they will be doing during the study. We answered their questions about CuedR during this demonstration. After the demonstration, the participant was given a two-digit user ID. During registration, the participant was assigned a five-key system-generated password, where each key letter will have visual, verbal and audio cues to help her remember the key. During login, the participant had to recognize the system-assigned keyword from a portfolio of 16 images and enter the corresponding key. These five keys comprised her password. Lastly, the participant was asked to participate in a

survey to give feedback on the password scheme. The survey included demographic questions asking for gender, age, major and their overall experience of using the authentication system.

## Study 2 – User Study at RLC

### First Session:

As with the UTA study, we showed the participants CuedR. We then had each user has to register and login to all three control conditions and both CuedR conditions. The order of control conditions and CuedR was alternated.

In control condition, there will be three different applications to test three different control condition. First control condition will have a system-assigned password with four characters, second will have password with six characters and third will have a password with eight characters. Each participant will register and login to one application at a time. During registration, a system-generated password will be displayed on the screen. The participant will have to learn the password and enter it in the two password fields. Then the participant will login using this password and the user ID.

In CuedR, there will be two CuedR conditions, both with similar design. The only difference is that, both the CuedR will assign a different five-key system-assigned password to the participant. During registration, the participant will be assigned a five key system-generated password, where each key letter will have visual, audio and verbal cues to help him remember the key. During login, the participant will have to recognize the system-assigned keyword, from a portfolio of images (each portfolio has 16 images) and enter the corresponding key. These five keys will constitute his password. Lastly, participant will be asked to participate in a survey to give your feedback on the password scheme. The survey will also include demographic questions asking for your gender, age, major and your overall experience of using the authentication system.

#### 5.4 Ecological Validity

The participants for our user study came from diverse majors like Law, Engineering, Business, etc., were across a wide age range, educated and they had some type of LDs. They represent a significant real world Internet users with LDs, but do not necessarily generalize to the entire population of Internet users who have LDs. This was a lab study were we could gather data from 19 participants. We chose to have a lab study based on previous research which says that lab studies are preferred to test brain-powered memorability of passwords [38]. The lab study would help us determining if we could conduct a similar field study or even online study in the near future.



## CHAPTER 6

### RESULTS AND ANALYSIS

In this section, we present and discuss the results of the user studies described in Chapter 5. We have analyzed our results in terms of registration time, login time and user feedback. All the 14 participants at UTA have completed the CuedR registration, login and feedback survey and all the five participants from RLC have completed all three experimental control condition's registration and login, two CuedR condition's registration and login and also the user feedback. So we have included data collected for all the 19 participants.

#### 6.1 Results of Study 1 (UTA)

##### 6.1.1 Memorability

Considering the intended pool of participants who have LDs, it is important to understand the impact multiple cues on memorability of these participants.

To understand memorability, we have taken into account the registration process which involves initial registration and password confirmation phase. If the participant fails in password confirmation phase, the system allows to learn the same password again with the help of same multiple cues that were provided during initial registration.

Our results show that out of 14 participants in the user study at UTA, only three participants (21.42%) had to learn their password again. Of the three participants, who had to learn their password again, one participant learnt the password correctly in two attempts whereas the other two learnt it in just one attempt.

### 6.1.2 Registration Time

Registration time is the total time taken by the participant to finish initial registration and password confirmation. This also includes learning time if the participant had to learn the password again.

The mean registration time for CuedR was 217.4 seconds (3.62 minutes) and median was 201.5 seconds. The maximum registration time was 514 seconds and minimum was 112 seconds (Table 1).

Mean	Median	SD	Max	Min
217.4	201.5	106.87	514	112

Table 1 Registration time (seconds) for all 14 participants at UTA

In the feedback survey, we asked participants whether “It was difficult to sign up with this password scheme”. We used 10-point Likert scale (1 being Strongly Disagree and 10 being Strongly Agree). The feedback we received for this question was Mean 8.1 and Median 9.5. We also asked the participants whether “The sign-up process took too long to maintain focus” and received feedback with Mean 7.5 and Median 10.

We analyzed CuedR registration time for different types of Learning Disabilities (Table 2). The minimum registration time was 112 seconds (1.86 minutes) for a participant who has Dyscalculia (math learning disability) and the maximum time was 514 seconds (8.56 minutes) for a participant who has Dyslexia (difficulty in reading). The interesting result was the registration time of 198 seconds (3.3 minutes) for a participant with Visual processing disorder which hinders the visual information processing of the person.

Learning Disability	Number of Participants	Registration Time (secs)				
		Mean	Median	Standard Deviation	Maximum	Minimum
Dyslexia	7	243	209	131.77	514	131
Dyscalculia	2	227	227	161.92	341	112
Dyslexia and Dyscalculia (both)	1	206	206	-	206	206
Visual Processing disorder	1	198	198	-	198	198
Dysphasia/Aphasia	2	180	180	36	205	154
Dysgraphia	1	125	125	-	125	125
All Participants	N = 14	217.4	201.5	106.8	514	112

Table 2 Registration time (seconds) for CuedR at UTA

### 6.1.2 Login Time

In this study, we have considered the login time of all the 14 participants at UTA. The mean login time for CuedR was 16 seconds (0.26 minutes) and the median login time was 13.5 seconds (0.23 minutes). The minimum login time was 9 seconds (0.15 minutes) and maximum login time was 42 seconds (0.7 minutes) (Table 3).

Mean	Median	SD	Max	Min
16	13.5	8.81	42	9

Table 3 Login time (seconds) for all 14 participants at UTA

In the feedback survey, we asked participants whether “Logging in using this password scheme was too time-consuming”. We used 10-point Likert scale (1 being Strongly Disagree and 10 being Strongly Agree). The feedback we received for this question was Mean 7.1 and Median 8.5.

We analyzed CuedR login time for different types of Learning Disabilities (Table 4). The minimum login time was 9 seconds (0.15 minutes) for a participant who has Dyslexia (difficulty in reading) and the maximum time was 42 seconds (0.7 minutes) for a participant who has Dyscalculia (difficulty in math).

Learning Disability	Number of Participants	Login Time (seconds)				
		Mean	Median	Standard Deviation	Maximum	Minimum
Dyslexia	7	14	14	5.99	26	9
Dyscalculia	2	27	27	21.92	42	11
Dyslexia and Dyscalculia (both)	1	13	13	-	13	13
Visual Processing disorder	1	13	13	-	13	13

Dysphasia/ Aphasia	2	12	12	3	14	10
Dysgraphia	1	20	20	-	20	20
All Participants	14	16	13.5	8.8	42	9

Table 4 Login time for CuedR at UTA

### 6.1.3 Number of Attempts

In our user study at UTA, all the 14 participants could login successfully in 1 attempt.

### 6.1.4 User Feedback & Suggestions

To analyze the feedback of participants we used Likert scale with scores ranging from 1 for Strongly Disagree and 10 for Strongly Agree. Table 5 shows the user feedback results.

Statement	Mean	Median	SD
The images helped me to recognize the password	7.79	9	3.29
The verbal cues helped me to recognize the password	6.79	8	3.56
The images were big enough	9.21	10	1.63
Verbal cues were easily readable	7.36	9	2.82
The audio cues were helpful for learning the passwords	8.64	9.5	2.47
Password key letters being written in upper case ('A') was helpful	7.14	8	3.08

Table 5 User feedback for CuedR at UTA

Table 6 shows the Likert scale scores of user feedback which are categorized based on the learning disability types.

Learning Disability	Number of Participants	Likert Scale Score (1: Strongly Disagree to 10: Strongly Agree)				
		Mean	Median	Standard Deviation	Maximum	Minimum
Dyslexia	7	7	6	0.79	8	6
Dyscalculia	2	7	7	1.98	8	5
Dyslexia and Dyscalculia (both)	1	5.2	5.2		5.2	5.2
Visual Processing disorder	1	5.1	5.1		5.1	5.1
Dysphasia/Aphasia	2	7	7		7	7
Dysgraphia	1	6.1	6.1		6.1	6.1
All Participants	14	6.47	6.3	0.99	8.2	5.06

Table 6 Likert scale feedback table for CuedR at UTA

During the study, we asked participants some additional questions to know more about their feedback and if they have any positive or negative remarks about the system. We found that all the participants found image cues to be helpful. All participants agreed that the use of upper case for keys helped them as it did not create confusion because of “reverse letter” as it is in case of letters like b/d, p/q, etc. They also mentioned that the font size was appropriate for them to read it. Only one participant who had Dysgraphia (problem with writing, spelling) found audio cues

helpful, especially the audio which reads out the verbal cue. Other participants found audio cues distracting. One user mentioned that the use of yellow color to highlight the verbal cue and the keyword really helped and that during her training sessions for Dyslexia, they used similar technique of using background colors like yellow and red to highlight the text. Table 7 shows some notable positive feedbacks from the participants.

During this feedback interview, we also received some concerns about the keywords and key. Four participants explicitly mentioned about the confusion caused due to disconnection between the key and keyword (“N” for “Panda confused). Table 8 shows some of the notable negative feedbacks from the participants.

Feedback	Type of LD
Images were the best cues in this scheme. In first attempt tried to remember the keys, but couldn't. But images helped.	Dyslexia
Use of “yellow” color as background color for Verbal cue and Keyword was helpful	Dyslexia
The font-size was appropriate and upper case really helped	Dyslexia
Audio was helpful.	Dysgraphia

Table 7 Notable Positive Feedback

Feedback	Type of LD
Audio did not help at all	Dyscalculia
There was no relation between the Keyword and the key which was distracting.	Dysgraphia
Too many words in verbal cue. Verbal cues were disconnected from the keys associated to them	Dyslexia

Table 8 Notable Negative Feedback

One participant suggested using lines or bordered blocks to highlight the word read out from the verbal cues. One participant who has Dyscalculia (difficulty with math) suggested adding numbers and symbols as a part of password so that it can be used to know its impact of people with Dyscalculia.

## 6.2 Results of Study 2 (RLC)

In this section, we show the results of user study at RLC. To understand the results of user study at RLC, we consider all the five participants that we recruited at RLC. All the five participants completed registration and login to three experimental control conditions and two CuedR conditions.

### 6.2.1 Registration time

We analyzed the registration to understand the impact of multiple cues provided by CuedR on the learning process. We also discuss the results of Control conditions.

Our results show that out of five participants in the user study at RLC, three participants (60%) had to learn their password again in CuedR condition 1 and only one participant (20%) had to learn the password again in CuedR condition 2. The participants who had to learn their password again in either CuedR condition 1 or 2 are different participants. All these four participants learnt their password in only one attempt.

Registration time is the total time taken by the participant to finish initial registration and password confirmation. This also includes learning time if the participant had to learn the password again. We show different results for both the CuedR conditions.



The mean registration time for CuedR condition 1 was 271 seconds (4.52 minutes) and median was 257 seconds. The maximum registration time was 393 seconds and minimum was 123 seconds (Table 9).

Mean	Median	SD	Max	Min
271	257	102.95	393	123

Table 9 Registration time (seconds) for CuedR 1 for all 5 participants at RLC

The mean registration time for CuedR condition 2 was 124 seconds (2.07 minutes) and median was 140 seconds. The maximum registration time was 148 seconds and minimum was 91 seconds (Table 10).

Mean	Median	SD	Max	Min
124	140	27.13	148	91

Table 10 Registration time (seconds) for CuedR 2 for all 5 participants at RLC

In the feedback survey, we asked participants whether “It was difficult to sign up with this password scheme”. We used 10-point Likert scale (1 being Strongly Disagree and 10 being Strongly Agree). The feedback we received for this question was Mean 8.8 and Median 10. We also asked the participants whether “The sign-up process took too long to maintain focus” and received feedback with Mean 2.6 and Median 1.

We analyzed CuedR registration time for different types of Learning Disabilities for both the CuedR conditions. Our results for CuedR 1 show that the maximum registration time was 393 seconds (6.55 minutes) for a participant who has Dyslexia (reading difficulty) and the minimum

time was 123 seconds (2.05 minutes) for a participant who has Dyslexia (difficulty in reading) (Table 11). For CuedR 2 the maximum registration time was 148 seconds (2.47 minutes) for a participant who has Dyslexia (reading difficulty) and the minimum time was 91 seconds (1.52 minutes) for a participant who has Dyslexia (difficulty in reading) (Table 12).

Learning Disability	Number of Participants	Registration Time (secs)				
		Mean	Median	Standard Deviation	Maximum	Minimum
Dyslexia	3	285	339	142.87	393	123
Dyslexia + ADHD	1	243	243	-	243	243
Audio Processing disorder	1	257	257	-	257	257
All Participants	5	271	257	102.95	393	123

Table 11 Registration time (seconds) for CuedR 1 at RLC

Learning Disability	Number of Participants	Registration Time (secs)				
		Mean	Median	Standard Deviation	Maximum	Minimum
Dyslexia	3	126	140	30.86	148	91
Dyslexia + ADHD	1	144	144	-	144	144

Audio Processing disorder	1	99	99	-	99	99
All Participants	5	124	140	27.13	148	91

Table 12 Registration time (seconds) for CuedR 2 at RLC

We considered registration time for three control conditions for three types of LDs (Table 13, Table 14 and Table 15) for all the five participants who took part in this user study at RLC. For the first control condition with four-character password, the minimum registration time was 12 seconds and the maximum time was 24 seconds, both for a person with Dyslexia. The minimum registration time for control condition 2 with six-character password was 12 seconds for a person with Dyslexia and maximum was 45 seconds for a person with ADHD and Dyslexia both. The third control condition showed a minimum registration time of 17 seconds which was for a person with Dyslexia and maximum of 53 seconds for a person with ADHD and Dyslexia both. This was the same person who took maximum time for registration in control condition 2.

Learning Disability	Number of Participants	Registration Time (secs)				
		Mean	Median	Standard Deviation	Maximum	Minimum
Dyslexia	3	17.67	17	6.02	24	12
Dyslexia + ADHD	1	16	16	-	16	16
Audio Processing disorder	1	12	12	-	12	12
All Participants	5	16.2	16	4.92	24	12

Table 13 Registration time (seconds) for Control Condition 1 at RLC

Learning Disability	Number of Participants	Registration Time (secs)				
		Mean	Median	Standard Deviation	Maximum	Minimum
Dyslexia	3	20	19	8.54	29	12
Dyslexia + ADHD	1	45	45	-	45	45
Audio Processing disorder	1	20	20	-	20	20
All Participants	N = 5	25	20	12.71	45	12

Table 14 Registration time (seconds) for Control Condition 2 at RLC

Learning Disability	Number of Participants	Registration Time (secs)				
		Mean	Median	Standard Deviation	Maximum	Minimum
Dyslexia	3	22.33	21	6.11	29	17
Dyslexia + ADHD	1	53	53	-	53	53
Audio Processing disorder	1	17	17	-	17	17
All Participants	5	27.4	21	15.13	53	17

Table 15 Registration time (seconds) for Control Condition 3 at RLC

### 6.2.2 Login Time

In this study, we have considered the login time of all the five participants at RLC. The mean login time for CuedR 1 was 10 seconds (0.16 minutes) and the median login time was 11

seconds (0.18 minutes). The minimum login time was 4 seconds (0.07 minutes) and maximum login time was 14 seconds (0.23 minutes) (Table 16). The login success rate was 100%.

Mean	Median	SD	Max	Min
10	11	4.06	14	4

Table 16 Login time (seconds) for CuedR 1 for all 5 participants at RLC

For CuedR 2 mean login time 13.6 seconds (0.23 minutes) and the median login time was 11 seconds (0.18 minutes). The minimum login time was 4 seconds (0.07 minutes) and maximum login time was 35 seconds (0.58 minutes) (Table 17).

Mean	Median	SD	Max	Min
13.6	11	12.32	35	4

Table 17 Login time (seconds) for CuedR 2 for all 5 participants at RLC

The login success rate for all the 5 participants was 100%.

In the feedback survey, we asked participants whether “Logging in using this password scheme was too time-consuming”. We used 10-point Likert scale (1 being Strongly Disagree and 10 being Strongly Agree). The feedback we received for this question was Mean 5.6 and Median 7. But out of five participants, two participants mentioned that the login for second CuedR was difficult due to the password interference with the first CuedR.

The three control condition login was also considered for this study. For Control condition 1 mean login time 7.2 seconds (0.12 minutes) and the median login time was 6 seconds (0.1 minutes). The minimum login time was 5 seconds (0.08 minutes) and maximum login time was 12 seconds (0.2 minutes) (Table 18).

Mean	Median	SD	Max	Min
7.2	6	2.77	12	5

Table 18 Login time (seconds) for all 5 participants during control condition 1

However, not all the participants could login successfully during the login session. The login success rate for this control condition was 80% i.e out of five, four participants could login successfully.

For Control condition 2 mean login time 12.75 seconds (0.21 minutes) and the median login time was 8 seconds (0.13 minutes). The minimum login time was 6 seconds (0.01 minutes) and maximum login time was 29 seconds (0.48 minutes) (Table 19).

Mean	Median	SD	Max	Min
12.75	8	10.87	29	6

Table 19 Login time (seconds) for all 5 participants during control condition 2

In this condition as well not all the participants could login successfully during the login session. The login success rate for this control condition was 60% i.e out of five, three participants could login successfully.

For Control condition 3 mean login time 9.8 seconds (0.16 minutes) and the median login time was 10 seconds (0.17 minutes). The minimum login time was 5 seconds (0.08 minutes) and maximum login time was 12 seconds (0.2 minutes) (Table 20).

Mean	Median	SD	Max	Min
9.8	10	2.86	12	5

Table 20 Login time (seconds) for all 5 participants during control condition 3

All the participants five could login successfully during the login session i.e. we had 100% login success rate.

We analyzed both CuedR conditions and all three control condition's login time for different types of Learning Disabilities. The minimum login time for both CuedR was 4 seconds (0.07 minutes) for a participant who has Dyslexia (difficulty in reading) and the maximum time was 14 seconds (0.23 minutes) for CuedR 1 for participant who has Dyslexia + ADHD and 35 seconds (0.58) for CuedR 2 for the same person who had maximum login time in CuedR 1. Table 21 and Table 22 shows the login time in seconds for CuedR 1 and CuedR 2.

Learning Disability	Number of Participants	Login Time (seconds)				
		Mean	Median	Standard Deviation	Maximum	Minimum
Dyslexia	3	7.67	8	3.51	11	4
Dyslexia + ADHD	1	14	14	-	14	14
Audio Processing disorder	1	13	13	-	13	13
All Participants	5	10	11	4.06	14	4

Table 21 Login time for CuedR 1 at RLC

Learning Disability	Number of Participants	Login Time (seconds)				
		Mean	Median	Standard Deviation	Maximum	Minimum
Dyslexia	3	7.33	7	3.51	11	4

Dyslexia + ADHD	1	35	35	-	35	35
Audio Processing disorder	1	11	11	-	11	11
All Participants	5	13.6	11	12.32	35	4

Table 22 Login time for CuedR 2 at RLC

We have also considered the login time for all three control condition based of LD types. Table 23, Table 24 and Table 25 show the login time (in seconds). The maximum login time recorded was 29 seconds (0.48 minutes) which was for Control condition 2 for a participant who has Dyslexia. While the minimum time was 5 seconds (0.08 minutes) for Control Condition 1 for a participant with Dyslexia + ADHD and also for Control Condition 3 for a participant with Dyslexia.

Learning Disability	Number of Participants	Login Time (seconds)				
		Mean	Median	Standard Deviation	Maximum	Minimum
Dyslexia	3	6.33	6	0.58	7	6
Dyslexia + ADHD	1	5	5	-	5	5
Audio Processing disorder	1	12	12	-	12	12
All Participants	5	7.2	6	2.77	12	5

Table 23 Login time for Control Condition 1



Learning Disability	Number of Participants	Login Time (seconds)				
		Mean	Median	Standard Deviation	Maximum	Minimum
Dyslexia	3	14.33	8	12.74	29	6
Dyslexia + ADHD	1	8	8	-	8	8
Audio Processing disorder	1	-	-	-	-	-
All Participants	5	12.75	8	10.87	29	6

Table 24 Login time for Control Condition 2

Learning Disability	Number of Participants	Login Time (seconds)				
		Mean	Median	Standard Deviation	Maximum	Minimum
Dyslexia	3	9	10	3.61	12	5
Dyslexia + ADHD	1	10	10	-	10	10
Audio Processing disorder	1	12	12	-	12	12
All Participants	5	9.8	10	2.86	12	5

Table 25 Login time for Control Condition 3

### 6.2.3 Number of Attempts

In our user study at RLC, all the five participants could login successfully in one attempt for both CuedR conditions.

For Control Condition 1, out of five participants only one could not login successfully and did not try to attempt it again. Remaining four participants could were able to login successfully in one attempt. For Control condition 2, out of five participants, one did not even try to login saying that he cannot remember the password. Three participants were able to login successfully in first attempt and one participant failed to login and did not try further. For control condition 3, all five participants were able to successfully login in first attempt.

		Mean	Median	Standard Deviation	Maximum	Minimum
No. Of Attempts	Control Condition 1 & Control Condition 3	1	1	0	1	1
	Control Condition 2	0.8	1	0.45	1	0

Table 26 Number of Attempts for Control conditions at RLC

#### 6.2.4 User Feedback & Suggestions

To analyze the feedback of participants we used Likert scale with scores ranging from 1 for Strongly Disagree and 10 for Strongly Agree. Table 27 shows the user feedback results of all the 5 participants that took part in the user study and completed 2 CuedR and 3 Control Conditions.

Statement	Mean	Median	SD
The images helped me to recognize the password	6.4	8	3.78
The verbal cues helped me to recognize the password	6	8	3.08
The images were big enough	8.2	9	2.49
Verbal cues were easily readable	7	9	2.83
The audio cues were helpful for learning the passwords	8	9	3.39
Password key letters being written in upper case ('A') was helpful	5.4	6	2.70

Table 27 User feedback for study at RLC

Table 28 shows the Likert scale scores of user feedback which are categorized based on the learning disability types.

Learning Disability	Number of Participants	Likert Scale Score (1: Strongly Disagree to 10: Strongly Agree)				
		Mean	Median	Standard Deviation	Maximum	Minimum
Dyslexia	3	5	6	1.55	6	4
Dyslexia + ADHD	1	7.53	7.53	-	7.53	7.53
Audio Processing disorder	1	5.1	5.1	-	5.1	5.1
All Participants	5	6	6	1.49	8	4

Table 28 Likert scale feedback table for study at RLC

During the study at RLC, we interviewed the participants to know more about their opinion about CuedR. All the participants agreed that the image cues helped them during login session. One participant with Dyslexia also mentioned that the verbal cues and audio cues together were helpful. This participant has some reading problems and cannot read and interpret the information properly when in silence and that the audio cues acted as a sound source. One participant mentioned that the audio cues were distracting because of which the participant had to pay more attention during registration. Out of five participants, four participants mentioned that having two CuedR conditions confused them as both had same portfolios.

Feedback	Type of LD
It is awesome idea. Will start using sticky notes to have images and corresponding keys to remember my password.	Dyslexia
Audio was helpful which added to the verbal cues.	Dyslexia

Table 29 Notable Positive Feedback

Feedback	Type of LD
Audio was distracting	Dyslexia

Table 30 Notable Negative Feedback

One participant suggested adding numbers and other symbols as a part of password to create a stronger password. Another participant suggested having multifactor login so that a similar scheme with graphical passwords can be used for financial accounts as well.

### 6.3 Discussion

In this study, we explored the impact of multiple cues on memorability of people who have LDs. Based on human memory model by Atkinson and Shiffrin [9] and also by studying various strategies to assist people who have LDs [26], we designed our system to provide a recognition-based authentication system, which uses the learning strategies to improve the memorability of system-assigned passwords.

We conducted a user study with total 19 participants who have some type of LDs, to understand the impact of multiple cues on their learning process. Considering the fact that almost 2.4 million students are diagnosed with specific LDs [33], we agree that having a sample size of 19 participants is not a large set to generalize our findings.

#### 6.3.1 Memorability

We had two different procedures for user study conducted at UTA and RLC. Out of 14 participants at UTA, only three i.e. 21.43% had to re-learn their password again during the registration phase. And one of these three participants learnt it after two attempts whereas the other two learnt in one attempt. Considering the learning difficulties faced by these participants, the success rate of registration is quite significant. This also suggests that, the multiple cues that were provided after considering various learning strategies for people with learning disability actually helped the participants to overcome their difficulties to certain extent and thus aided to their learning process.

The study conducted at RLC with five participants where three participants i.e. 60% had to re-learn their password in first registration whereas only one participant out of five re-learned the password in registration 2. Having 2 CuedRs had some multiple password interference effect, where the users found it difficult to recognize their password for one CuedR due to similar

portfolios that were used in CuedR 2 as well. As described in the cognitive psychology literature [39], memory interference is “the impaired ability to remember an item when it is similar to other items stored in memory”. The control condition comparison show login success rate of 80%, 60% and 100% for random system-assigned password of length four characters, six characters and eight characters respectively. Whereas for both CuedRs we had 100% login success rate. We can infer that though the participants had to re-learn their passwords, re-learning helped them to login successfully.

However, this was a single-session study so we cannot conclude anything about long term memorability of this authentication system.

### 6.3.2 Registration Time

We found the average registration time to be maximum of 271 seconds (4.52 minutes) from both the studies (UTA and RLC) which is considerably higher than the highest average registration time for control condition which was 22.33 seconds (0.37 minutes). However, the registration and learning of password aids participants with faster recognition during login thus, reducing the login time.

### 6.3.3 Login Time

We found that the average login time to be minimum of 7.33 seconds which is (0.12 minutes) from both the studies (UTA and RLC). There are no significance difference between the minimum average login time of control condition which was 7.2 seconds (0.12 minutes).

#### 6.3.4 User Feedback

One important part of our study was the user feedback from the participants. Based on the user feedback that we received, majority of the participants enjoyed learning their password in a different way with the help of cues. They found it easier to remember the password with the help of images that we provided. Though not more than two participants liked the audio cues, others found them distracting. This suggests that our system has potential to be used even by people who have learning disabilities provided modify the system based on user feedback and adding more strategies to assist the people who have learning disabilities.

## CHAPTER 7

### CONCLUSION

In our study, we aimed to understand the impact of using multi-sensory cues to aid people with LDs in learning system-assigned passwords. We designed two different study procedures to understand this. In an attempt to assist the learning process of people having learning disability, we chose CuedR authentication system as a base system and made some modification considering the needs of people with different types of learning disabilities.

Our study showed that the proposed system offered a good learning platform with 78.57% of participants at UTA learning their password in first attempt in spite of having learning disabilities which hinder their reading, writing, spelling, visual and audio processing abilities. The finding at RLC show that all the five participants logged in successfully i.e. 100% success rate as compared to the average login success rate of 80% of all three control conditions.

From the user feedback that we received during our study, we believe that majority of the participants we had were comfortable using this system and it helped them in the learning process even though they have some LDs which hinders their learning otherwise.

The current work is the first to see the impact of cues on learning process, where we considered very few, though really important needs of people with LDs. In the future, we are interested to consider more strategies to help individual LD types like Dyscalculia, Dysgraphia, etc. We also plan to make UI modifications based on user feedback to study the impact of these changes and how it affects people with different types of LDs.



## REFERENCES

- [1] C. Shoba Bindu "Secure Usable Authentication Using Strong Pass text Passwords." I. J. Computer Network and Information Security, 2015, 3, 57-64 Published Online February 2015 in MECS.
- [2] Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, Nasir Memon "Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice" Symposium On Usable Privacy and Security (SOUPS) 2005, July 6-8, 2005, Pittsburgh, PA, USA.
- [3] Brown, A.S., Bracken, E., Zoccoli, S. and Douglas, K. "Generating and remembering passwords." Applied Cognitive Psychology 18 (2004), 641-651.
- [4] Sasse, M.A., Brostoff, S. and Weirich, D. "Transforming the 'weakest link' – a human/computer interaction approach to usable and effective security." BT Technical Journal 19 (2001), 122-131.
- [5] Adams, A. and Sasse, M.A. Users are not the enemy. CACM 42, 12 (1999), 41-46.
- [6] Mahdi Nasrullah Al-Ameen Matthew Wright Shannon Scielzo "Towards Making Random Passwords Memorable: Leveraging Users' Cognitive Ability Through Multiple Cues" CHI 2015, April 18 - 23 2015, Seoul, Republic of Korea
- [7] Wright, N., Patrick, A. S., and Biddle, R. Do you see your password? Applying recognition to textual passwords. In SOUPS (2012).
- [8] P. G. Kelley, S. Komanduri, M. L. Mazurek, R. Shay, T. Vidas, L. Bauer, N. Christin, and L. F. Cranor. "The impact of length and mathematical operators on the usability and security of system-assigned one-time PINs, 2012.
- [9] R. C. Atkinson and R. M. Shiffrin "Human Memory: A Proposed System And Its Control

Processes”

- [10] M Sreelatha, M Shashi, M Roop Teja, M Rajashekar And K Sasank " Intrusion prevention by image based authentication techniques" IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011.
- [11] Jatin Bajaj, Akash Harlalka, Ankit Kumar, Ravi Mokashi Punekar, Keyur Sorathia, Om Deshmukh and Kuldeep Yadav "Audio Cues: Can Sound Be Worth a Hundred Words?" Springer International Publishing Switzerland 2015 P. Zaphiris and A. Ioannou (Eds.): LCT 2015, LNCS 9192, pp. 14–23, 2015
- [12] Hari Sundaram, Shih-Fu Chang "Determining computable scenes in films and their structures using audio-visual memory models" MULTIMEDIA '00 Proceedings of the eighth ACM international conference on Multimedia Pages 95-104
- [13] Dan G. Drew Thomas Grimes "Audio-Visual Redundancy and TV News Recall" Volume: 14 issue: 4, page(s): 452-461 Issue published: August 1, 1987 DOI: <https://doi.org/10.1177/009365087014004005>
- [14] Elizabeth T. Davis, Kevin Scott, Jarrell Pair, Larry F. Hodges, James Oliverio "Can Audio Enhance Visual Perception and Performance in a Virtual Environment?" Volume: 43 issue: 22, page(s): 1197-1201 Issue published: September 1, 1999
- [15] Karen Renaud, Peter Mayer, Melanie Volkamer and Joseph Maguire "Are Graphical Authentication Mechanisms As Strong As Passwords?" Proceedings of the 2013 Federated Conference on Computer Science and Information Systems pp. 837–844
- [16] LiPing Mi, Xiangyang Liu, Fuji Ren "The Picture Superiority Effect in Encoding and Retrieval Processes during Japanese Learning for Chinese Bilinguals" 978-1-4244-4538-7/09 ©2009 IEEE
- [17] A. Paivio, Imagery and Verbal Processes. Holt, Rinehart, and Winston, New York. 1971.

- [18] A. Paivio, *Mental representations: a dual coding approach*. Oxford University Press, England, 1986.
- [19] A. Paivio, Dual coding theory: retrospect and current status. *Canadian Journal of Psychology* 45, 1991, pp.255–287.
- [20] Mahdi Nasrullah Al-Ameen, Kanis Fatema, Matthew Wright, Shannon Scielzo “The Impact of Cues and User Interaction on the Memorability of System-Assigned Recognition-Based Graphical Passwords” Symposium on Usable Privacy and Security (SOUPS) 2015, July 22–24, 2015, Ottawa, Canada
- [22] Tulving, E., & Pearlstone, Z. 1966. Availability vs. accessibility of information in memory for words. *Journal of Verbal Learning and Verbal Behavior*. 5, 381 – 391.
- [23] Michelsen, C. D., Dominick, W. D. and Urban, J. E. (1980). A methodology for the objective evaluation of the user/system interfaces of the MADAM system using software engineering principles. *ACM Southeast Regional Conference*. 103-109.
- [24] Nielsen, J. (1994). *Usability Engineering*. Morgan Kaufmann
- [25] A Survey of Software Learnability: Metrics, Methodologies and Guidelines Tovi Grossman, George Fitzmaurice, Ramtin Attar Autodesk Research, CHI 2009, April 4–9, 2009, Boston, Massachusetts, USA.
- [26] A Handbook on Learning Disabilities Designed by Integra® Staff to Complement our “Walk a Mile in My Shoes” Workshop
- [27] The Colorado Department of Education’s Twice-Exceptional Students Gifted Students with Disabilities, Level 1: An Introductory Resource Book
- [28] OPTIMAL COLORS TO IMPROVE READABILITY FOR PEOPLE WITH DYSLEXIA Luz Rello. Universitat Pompeu Fabra, Ricardo Baeza-Yates. Yahoo! Research & Universitat Pompeu Fabra, rbaeza@acm. Available at <https://www.w3.org/WAI/RD/2012/text->

[customization/r11](#)

- [29] Gregor, P. & Newell, A. F. (2000), An empirical investigation of ways in which some of the problems encountered by some dyslexics may be alleviated using computer techniques, in Proceedings of the fourth international ACM conference on Assistive technologies, ASSETS 2000, ACM, New York, NY, USA, pp. 85–91.
- [30] Gregor, P., Dickinson, A., Macaffer, A. & Andreasen, P. (2003), 'Seeword a personal word processing environment for dyslexic computer users', British Journal of Educational Technology 34(3), 341–355.
- [31] M. Pattison and A. Stedmon, "Inclusive design and human factors: Designing mobile phones for older users," Psychology Journal, vol. 4(3), pp. 267–284, 2006.
- [32] S. A. Becker, "E-government visual accessibility for older adult users," Social Science Computer Reviews, vol. 22 (1), pp. 11–23, 2004.
- [33] <https://ldaamerica.org/>
- [34] <http://www.ldonline.org>
- [35] <https://www.papermasters.com>
- [36] <https://www.helpguide.org/>
- [37] <https://www.understood.org/>
- [38] S. Fahl, M. Harbach, Y. Acar, and M. Smith. On the ecological validity of a password study. In SOUPS, 2013.
- [39] M. Anderson and J. Neely. Memory. Handbook of Perception and Cognition, chapter 8: Interference and inhibition in memory retrieval, pages 237–313. Academic Press, 2<sup>nd</sup> edition, 1996.

- [40] R. W. Proctor, M.-C. Lien, K.-P. L. Vu, E. E. Schultz, and G. Salvendy. Improving computer security for authentication of users: Influence of proactive password restrictions. *Behavior Research Methods, Instruments, and Computers*, 34(2), 2002.
- [41] R. Shay, S. Komanduri, P. G. Kelley, P. G. Leon, M. L. Mazurek, L. Bauer, N. Christin, and L. F. Cranor. Encountering stronger password requirements: User attitudes and behaviors. In *SOUPS*, 2010.
- [42] R. Shay, P. G. Kelley, S. Komanduri, M. L. Mazurek, B. Ur, T. Vidas, L. Bauer, . Christin, and L. F. Cranor. Correct horse battery staple: Exploring the usability of system-assigned passphrases. In *SOUPS*, 2012.
- [43] Learning System-assigned Passwords (up to 56 Bits) in a Single Registration Session with the Methods of Cognitive Psychology USEC '17, 26 February 2017, San Diego, CA, USA
- [44] Yan, J., Blackwell, A., Anderson, R., Grant, A. 2005. The Memorability and Security of Passwords. In L. F. Cranor & S. Garfinkel (Eds.), *Security and Usability: designing secure systems that people can use* (pp. 129 -142). Sebastopol, CA: O'Reilly.
- [45] Effect of Grammar on Security of Long Passwords- Ashwini Rao, Birendra Jha, Gananand Kini - CODASPY'13, February 18–20, 2013, San Antonio, Texas, USA.
- [46] M. Leonhard and V. Venkatakrisnan. A new attack on random pronounceable password generators. In *Proc. IEEE EIT*, 2007.
- [47] D. L. Nelson, V. S. Reed, and C. L. McEvoy. Learning to order pictures and words: A model of sensory and semantic encoding. *Journal of Experimental Psychology: Human Learning and Memory*, 3(5), 1977.
- [48] A. Paivio. *Mind and Its Evolution: A Dual Coding Theoretical Approach*. Lawrence Erlbaum: Mahwah, N.J., 2006.
- [49] [Antonella De Angeli, Lynne Coventry, Graham Johnson, and Karen Renaud. Is a picture](#)

[really worth a thousand words? exploring the feasibility of graphical authentication systems. International Journal of Human-Computer Studies, 63:128–152, July 2005.](#)

- [50] Xiaoyuan Suo, Ying Zhu, and G. Scott Owen. Graphical passwords: A survey. In Proceedings of Annual Computer Security Applications Conference, pages 463–472, 2005.
- [51] F. Craik and J. McDowd Age Differences in recall and recognition. *Journal of Experimental Psychology: Learning, Memory, and Cognition*, 13(3):474{479, July 1987.
- [52] I. Jermyn, A. Mayer, F. Monroe. M. K. Reiter and A. D. Rubin, “The Design and Analysis of Graphical Passwords”, In Proceedings of the 8th USENIX Security Symposium, 1999.
- [53] Graphical Passwords: Learning from the First Twelve Years Robert Biddle, Sonia Chiasson, P.C. van Oorschot School of Computer Science Carleton University, Ottawa, Canada Version: January 4, 2011. Technical Report TR-11-01, School of Computer Science, Carleton University, 2011
- [54] Secure Usable Authentication Using Strong Pass text Passwords C. Shoba Bindu I.J. *Computer Network and Information Security*, 2015, 3, 57-64
- [55] D. Nali and J. Thorpe, \Analyzing user choice in graphical passwords," School of Computer Science, Carleton University, Tech. Rep. TR-04-01, 2004.
- [56] J. Thorpe, P.C. van Oorschot, “Towards secure design choices for implementing graphical passwords”, *Computer Security Applications Conference* (2004)
- [57] P. Dunphy and J. Yan. Do background images improve "Draw a Secret" graphical passwords? In 14th ACM Conference on Computer and Communications Security (CCS), October 2007.
- [58] MEMORABILITY FEATURES OF DRAW -BASED GRAPHICAL PASSWORDS *Journal of Theoretical and Applied Information Technology* 10th August 2013. Vol. 54 No.1

- [59] Modeling user choice in the PassPoints graphical password scheme - Ahmet Emir Dirik, Nasir Memon and Jean-Camille Birget Symposium On Usable Privacy and Security (SOUPS) 2007, July 18-20, 2007, Pittsburgh, PA, USA.
- [60] Secure User Authentication & Graphical Password using Cued Click-Points - Miss.Saraswati B.Sahu, International Journal of Computer Trends and Technology (IJCTT) – Volume 18 Number 4 – Dec 2014
- [61] Passfaces Corporation. The science behind Passfaces. White paper, [http://www.passfaces.com/enterprise/resources/white\\_papers.htm](http://www.passfaces.com/enterprise/resources/white_papers.htm), accessed July 2009.
- [62] S. Brostoff and M. A. Sasse, "Are Passfaces more usable than passwords: A Field Trial Investigation", In People and Computers XIV – Usability or Else: Proceedings of HCI. Sunderland, U.K.: Springer –Verlag, 2000.
- [63] T. Valentine. An evaluation of the Passface personal authentication system. Technical report, Goldsmiths College Univ. of London, 1999.
- [64] A. De Angeli, L. Coventry, G. Johnson, and K. Renaud. Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems. International Journal of Human-Computer Studies, 63(1-2):128{152, 2005.
- [65] PassPoints: Design and longitudinal evaluation of a graphical password system Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, Nasir Memon - S. Wiedenbeck et al. / Int. J. Human-Computer Studies 63 (2005) 102–127.
- [66] Chiasson, S., van Oorschot, P.C., Biddle, R. Graphical Password Authentication Using Cued Click-points. ESORICS 2007.
- [67] Influencing Users Towards Better Passwords: Persuasive Cued Click-Points Sonia Chiasson, Alain Forget, Robert Biddle, P.C. van Oorschot- Chiasson, Forget, Biddle, van Oorschot 2008, Published by the British Computer Society.

- [68] M. Gasser. A random word generator for pronounceable passwords. Technical Report ESD-TR- 5-97, The MITRE Corporation, 1975.
- [69] Baddeley, A. (1997), Human Memory: Theory and Practice, Revised edition, Psychology Press.
- [70] Parkin, A. J. (1993), Memory: Phenomena, Experiment and Theory, Blackwell.
- [71] 46. Tulving, E., and Watkins, M. Continuity between recall and recognition. American Journal of Psych 86(4) (1973).
- [72] Anderson, J. R., and Bower, G. H. Recognition and recall processes in free recall. Psychological Review 79(2) (1972).
- [73] Lee Lay Wah. (2003). An introduction to assistive technology: Meeting the needs of students with disabilities. Diges Pendidik. 3(2), 31-37.
- [74] Supporting Students with Learning Disabilities: A Guide for Teachers: Ministry of Education and the British Columbia School Superintendent's Association September 2011.
- [75] B. A. O'Brien, J. S. Mansfield, and G. E. Legge. "The Effect of Print Size on Reading Speed in Dyslexia." Journal of Research in Reading 28.3 (2005): 332-49.
- [76] (Work in Progress) An Insight into the Authentication Performance and Security Perception of Older Users. Sovanharith Seng, Sadia Ahmed, Mahdi Nasrullah Al-Ameen and Matthew Wright available at <http://www.dcs.gla.ac.uk/~karen/usec/programme.html>



## BIOGRAPHICAL INFORMATION

Sonali Marne was born in Pune, India in 1989. She received her Bachelor of Engineering (B.E) degree in Information Technology from University of Pune in May 2011. She worked with Capgemini, Pune as an Associate Consultant until December 2014. She decided to pursue her Master's degree in Computer Science from University of Texas at Arlington from January 2015. She interned with IBM as a Software Developer at Littleton, Massachusetts. Her research interest cover a range of topics including but not limited to Information Security, Database Systems, Usability and Cryptography.