The Impact of Cues and User Interaction on the Memorability of System-Assigned Recognition-Based Graphical Passwords

Mahdi Nasrullah Al-Ameen, Kanis Fatema, Matthew Wright, Shannon Scielzo
The University of Texas at Arlington
Arlington, TX, USA
{mahdi.al-ameen, kanis.fatema}@mavs.uta.edu, mwright@cse.uta.edu, scielzo@uta.edu

ABSTRACT

User-chosen passwords reflecting common strategies and patterns ease memorization, but offer uncertain and often weak security. System-assigned passwords provide higher security, and thus in commercially deployed graphical-password systems (e.g., Passfaces), images are randomly assigned by the system. It is difficult, however, for many users to remember system-assigned passwords. We argue that this is because existing password schemes do not fully leverage humans' cognitive strengths, and we thus examine techniques to enhance password memorability that incorporate scientific understanding of long-term memory. In our study, we examine the efficacy of *spatial cues* (fixed position of images), *verbal cues* (phrases/facts related to the images), and employing *user interaction* (learning images through writing a short description at registration) to improve the memorability of passwords based on face images and object images. We conducted a multi-session in-lab user study with 56 participants, where each participant was assigned seven different graphical passwords, each representing one study condition. One week after registration, participants had a 98% login success rate for a scheme offering spatial and verbal cues, while the scheme based on user interaction had a 95% login success rate for face images and a 93% login success rate for object images. All of these were significantly higher than the control conditions representing existing graphical password schemes. These findings contribute to our understanding of the impact of cues and user interaction on graphical passwords, and they show a promising direction for future research to gain high memorability for system-assigned random passwords.

Keywords

System-assigned graphical password, memorability, cued-recognition, user interaction

Symposium on Usable Privacy and Security (SOUPS) 2015, July 22–24, 2015, Ottawa, Canada.

1. INTRODUCTION

Traditional user-chosen textual passwords suffer from security problems because of password reuse and predictable patterns [13, 42]. Users bear the responsibility of ensuring security of their account by creating a password that should be chosen with creativity and intelligence so that it achieves satisfactory security and memorability. For many users, this is a lot of work, and in many cases they compromise on security and create a weak but memorable password.

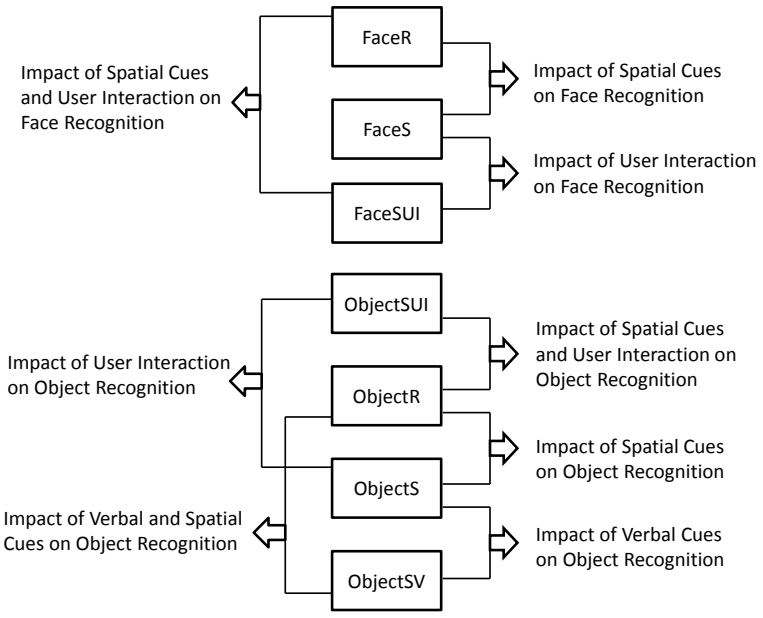
A recent study [40] reveals that with the advancement of digital technology and widespread use of the Internet, users now more than ever realize the importance of strong passwords, and many of them intend to create secure passwords but still fail to achieve a good balance between security and memorability. Policies requiring users to create longer passwords with different character types do not necessarily lead to more secure passwords, but they do adversely affect memorability in some cases [36, 42].

A number of important cognitive propensities have been considered by researchers to explore better alternatives to traditional textual passwords. For example, recognition is an easier memory task than recall [6, 46, 47], and due to the *picture superiority effect*, the human brain is better at memorizing graphical information as compared to textual information [33, 35]. These are the core ideas behind the design of recognition-based graphical passwords, such as Passfaces [1], which is now commercially available and deployed by a number of large websites.[1]

In recognition-based graphical passwords, such as Passfaces [1], users are shown several portfolios of faces (e.g., four portfolios of nine faces each), and one face per portfolio serves as the authentication secret that they have to recognize during login. Previously, users in Passfaces could select images from the portfolio for their authentication secret. Davis et al. [14], however, found that users select predictable images. As a result, the commercial Passfaces [1] product now assigns a random image for each portfolio instead of allowing users to choose.

With system-assigned passwords, the user does not have to guess whether a password is secure, and the system can ensure that all passwords offer the desired level of security. Additionally, while password reuse could pose a serious security threat [13], using system-assigned passwords ensures that users do not reuse a password (or modification thereof) already used on another account. Unfortunately, it is dif-

[1] http://www.realuser.com/ shows testimonials about Passfaces from customers, such as banks.



Study Condition	Image Type	Cues		User Interaction
		Spatial	Verbal	
FaceR	Human Face	x	x	x
FaceS	Human Face	√	x	x
FaceSUI	Human Face	√	x	√
ObjectR	Object	x	x	x
ObjectS	Object	√	x	x
ObjectSV	Object	√	√	x
ObjectSUI	Object	√	x	√

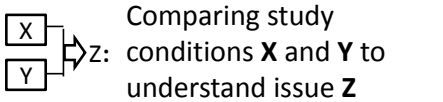


Figure 1: The Study Model to Understand the Impact of Cues and User Interaction on Recognition-based Graphical Authentication

ficult for most people to memorize system-assigned passwords [17, 41, 49]. Thus, it still remains a critical challenge to design an authentication scheme that offers satisfactory memorability for system-assigned random passwords.

The commercial deployment of recognition-based graphical passwords (e.g., Passfaces [1]) and its demonstrated potential mean that improvements to such schemes would be very valuable contributions. In this paper, we aim to incorporate the scientific understanding of long-term memory to advance the memorability of system-assigned recognition-based graphical passwords.

1.1 Contributions

To this end, we draw upon several prominent theories of cognitive psychology to enhance the memorability of system-assigned recognition-based graphical passwords. In particular, we examine the impact of using memory cues, including *spatial cues* in which images in a portfolio are shown in the same position each time and *verbal cues* in which each image is presented with a phrase or fact related to the image. The use of cues facilitates a detailed encoding that helps to transfer the authentication information (e.g., assigned images) from the working memory to long-term memory at registration [7], helping users recognize their images when logging in later. We call this approach *cued-recognition* [5].

We also explore the efficacy of requiring user interaction at registration, in which we have users apply their observation and imagination to type a short description about assigned images. In the course of such observations and thinking on the assigned images, users get more familiar with them and consequently succeed to recognize those images from the set of decoys during login. This process engages users' action-event memory [29], in addition to their visual memory [33, 35], and aids in the elaborate encoding of the authentication secret in long-term memory [7]. We provide a detailed discussion on these memorization processes in §3.

Considering both human faces and objects as images, along with cues and interaction, we design seven different study conditions (see Figure 1). In our within-group study with 56 participants, every participant was assigned seven different graphical passwords, each representing one study condition. The major findings from our study include:

- Verbal cues make a significant contribution in improving the memorability for object-recognition-based graphical passwords.
- Spatial cues do not contribute significantly to improve memorability for either face or object recognition.
- User interaction is an effective approach to enhance memorability for both face and object recognition.

We organize this paper as follows: In §2, we give an overview of the notable authentication schemes with a discussion on their limitations and the scope for possible improvements. In §3, we explain from the perspective of cognitive psychology how the design choices for our study conditions are set up. We then describe our study procedure in §4 and present the results in §5. In §6, we discuss the findings from our study and highlight the possible directions for future research, followed by a conclusion in §7.

2. RELATED WORK

In this section, we give a brief overview of notable textual and graphical password schemes in which we highlight why existing schemes are insufficient. A possible exception is

the CuedR scheme of Al-Ameen et al. [5], which inspires the deeper investigation that we undertake in this paper. We end this section by describing our distinct contributions from their work.

2.1 Textual Password Schemes

2.1.1 Traditional passwords

Traditional user-chosen textual passwords are fraught with security problems because of password reuse and predictable patterns [13,42]. Different password restriction policies (e.g., increasing the minimum password length, requiring a combination of different types of characters, and using password strength meters) have been deployed to get users to create stronger passwords [19, 42]. However, in separate studies, Proctor et al. [36] and Shay et al. [42] report that such policies do not necessarily lead to more secure passwords but do adversely affect memorability in some cases.

2.1.2 Mnemonic Passwords

Kuo et al. [30] studied passwords based on mnemonic phrases, in which the user chooses a memorable phrase and uses a character (often the first letter) to represent each word in the phrase. Their results show that user-selected mnemonic passwords are slightly more resistant to brute-force attacks than traditional passwords. However, mnemonic passwords are found to be more predictable when users choose common phrases to create their passwords. A properly chosen dictionary may further increase the success rate in guessing mnemonic passwords [30].

2.1.3 System-assigned passwords

System-assigned random textual password schemes are more secure but fail to provide sufficient memorability, even when natural-language words are used [41, 49]. Wright et al. [49] compared the usability of three different system-assigned textual password schemes: Word Recall, Word Recognition, and Letter Recall. None of these schemes had sufficient memorability rates.

2.1.4 PTP

Forget et al. [20, 21] proposed the Persuasive Text Passwords (PTP) scheme, in which the user first creates a password, and PTP improves its security by placing randomly-chosen characters at random positions into the password. PTP is resilient against attacks exploiting password reuse and predictable patterns. Unfortunately, the memorability for PTP is just 25% when two random characters are inserted at random positions [20].

2.1.5 Cognitive questions

Furnell et al. [23] revealed the potential of cognitive questions and reported a high level of user satisfaction in using them for primary authentication. However, Just and Aspinall [28] showed the usability and security problems of using cognitive questions for authentication, and several other studies [37, 39] point out the vulnerability of this approach to targeted guessing attacks.

2.2 Graphical Password Schemes

Graphical password schemes can be divided into three categories [8], based on the kind of memory leveraged by the systems: i) Drawmetric (recall-based), ii) Locimetric (cued-recall-based), and iii) Cognometric (recognition-based).

2.2.1 Drawmetric

The user is asked to reproduce a drawing in this category of graphical passwords. In *Draw-a-Secret (DAS)* [27], a user draws on top of a grid, and the password is represented as the sequence of grid squares. Nali and Thorpe [32] have shown that users choose predictable patterns in DAS that include drawing symmetric images with 1-3 pen strokes, using grid cell corners and lines (presumably as points of reference) and placing their drawing approximately in the center of the grid.

BDAS [16] intends to reduce the amount of symmetry in the user's drawing by adding background images, but this may introduce other predictable behaviors such as targeting similar areas of the images or image-specific patterns [8]. DAS and BDAS have recall rates of no higher than 80%.

2.2.2 Locimetric

The password schemes in this category present users with one or more images as a memory cue to assist them selecting their particular points on the image(s). In the *Passpoints* [9] scheme, users select a sequence of click-points on a single image as their password. *Cued Click-Points (CCP)* [12] is a modified version of Passpoints, where users sequentially choose one click-point on each of five images. Dirik et al. [15] developed a model that can predict 70-80% of users' click positions in Passpoints. To address this issue, Chiasson et al. proposed *Persuasive Cued Click-Points (PCCP)* [11, 22], in which a randomly-positioned viewport is shown on top of the image during password creation, and users select their click-point within this viewport. The memorability for PCCP was found to be 83-94%.

In a follow-up study, Chiasson et al. [10] found predictability in users' click points, showing that in Passpoints, the click points are roughly evenly spaced across the image, in straight lines starting from left to right, and either completely horizontal or sloping from top to bottom. The authors [10] indicate that predictability is still a security concern for PCCP.

2.2.3 Cognometric

In this recognition-based category of graphical passwords, the user is asked to recognize and identify their password images from a set of distractor images. *Passfaces* [1] is the most studied cognometric scheme as it is commercially deployed by a number of large websites. The commercial Passfaces [1] product assigns a random set of faces instead of allowing users to choose, since the research [14] has found that users select predictable faces, biased by race, gender, and attractiveness of faces. However, Everitt et al. [17] show that users have difficulty in remembering system-assigned Passfaces.

Davis et al. [14] proposed the *Story* scheme, in which users select a sequence of images as their password and, to aid memorability, are encouraged to mentally construct a story to connect those images. During login, users have to identify their images in accurate order from a panel of decoy images. Though the user choices in Story are found to be more varied than the face-recognition-based scheme, the results still display some exploitable patterns, and the user study showed a memorability rate of about 85% [14].

2.3 Cued-recognition

All prior graphical password schemes show either deficit in memorability, security, or both. A cognometric scheme called Cued-recognition (CuedR) was recently proposed by Al-Ameen et al. [5]. CuedR includes spatial and verbal cues designed to aid recognition of the images of objects, and in a lab study with 37 participants, it had 100% memorability one week after registration. This suggests that the use of cues is very promising and motivates further study. In particular, their study relied on user feedback to discern the relative importance of different cues. They did not actually study the impact of different cues in an experiment. Our deeper investigation on this issue, through direct comparisons between schemes offering different combinations of cues, indicates that relying solely on user feedback might not be reliable in this context (see §6 for detailed discussion). Further, the commercially deployed Passfaces scheme uses face images instead of object images, and it is unclear which should be used. We also examine this issue in our study.

3. SYSTEM DESIGN

Passfaces [1] provides *PIN-level* security (13 bits of entropy), while an authentication scheme should offer at least 20 bits of entropy to attain *password-level* security [8]. Hlywa et al. [26] provide a guideline to design recognition-based graphical authentication schemes with password-level security, where the user is assigned five images at registration and has to recognize each of the assigned images from a distinct portfolio of 16 images during login. We follow this guideline to design our study conditions, where a successful authentication requires the user to recognize all five images correctly. For an unsuccessful login, the user is shown an error message at the end of the login attempt but not informed on which portfolio the mistake was made.

In this section, we explain from the perspective of cognitive psychology how our study design is set up to understand the impact of cues and user interaction (at registration) in improving memorability for system-assigned recognition-based (i.e., cognometric) graphical password schemes. We illustrate our study model in Figure 1.

3.1 Visual Memory

In our study, we leverage the *picture superiority effect* [35], which points out that the human brain is better at memorizing graphical information as compared to textual information [33, 35]. Several explanations for this effect have been proposed in psychology research, where *dual-coding theory* [35] is the most widely accepted. According to this theory [35], images are encoded not only visually and remembered as images, but they are also translated into a verbal form (as in a description) and remembered semantically in human memory. Another explanation for the picture superiority effect is *sensory-semantic model* [33], which postulates that images are accessed more easily than the textual information because they are accompanied by more distinct sensory codes.

3.2 Memory Retrieval

Users are required to perform a recognition task in our study, since it is easier to identify the correct item among a set of distractors (i.e., recognition) than reproducing the item from memory (i.e., recall) [46]. This ease in recognition is explained through *Strength theory* [47] and *Generate-recognize theory* [6]. Strength theory [47] simply states that although the same memory tasks are involved in both recall and recognition, recognition requires less effort. According to generate-recognize theory [6], recall consists of two phases:

Generate phase: A list of candidate words is formed by searching long-term memory.

Recognize phase: The list of words (formed in generate phase) is evaluated to see if they can be recognized as the sought-out memory.

Generate-recognize theory postulates that recognition tasks are faster and easier to perform since they do not utilize the generate phase. This can be illustrated by considering exam questions—having the correct answer available for recognition makes multiple-choice questions easier than short-answer questions.

3.3 Face Recognition

In our study, we consider face and object images separately, to understand the impact of cues and user interaction on each image type for recognition-based graphical authentication. Passfaces [1] uses face images, and prior research [24,31] has shown evidence that there may be regions of the human brain dedicated to processing facial information and recognizing faces. Minnebusch et al. [31] demonstrate that three important regions of human brain, *fusiform face area (FFA)*, *superior temporal sulcus (STS)*, and *occipital face area (OFA)*, are activated (recruited) bilaterally (with some right hemisphere bias) while processing facial information. The results of functional MRI show that FFA in the brain gets activated more strongly while viewing faces as compared to other visual objects. STS is sensitive to dynamic aspects of face stimuli, such as gaze or expression. OFA is another important area of human brain, and it deals with the physical features of faces. The findings of Minnebusch et al. [31] are in agreement with the evidence shown by Haxby et al. [24] that suggest that face recognition is functionally different than recognizing other visual objects.

3.4 Long-Term Memory

We incorporate the scientific understanding of long-term memory to advance the usability properties of recognition-based authentication. The cognitive memory model proposed by Atkinson and Shiffrin [7] postulates that users learn new information through the sensory organs, which is then transmitted to their short-term memory (STM). The elaborate processing and encoding of the information, which is held in STM as *memory codes*—mental representations of selected parts of the information, contributes to transferring that information from STM to long-term memory (LTM). This encoding helps people to remember and retrieve the processed information efficiently over an extended period of time. To motivate this encoding, we examine two different approaches in our study:

Cued-recognition: Providing memory cues (e.g., spatial, verbal) with the images, which would be shown both at registration and login.

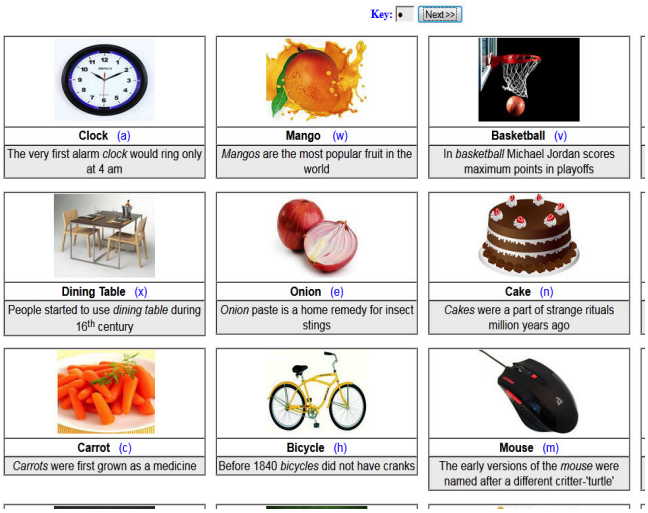


Figure 2: A partial screen shot of ObjectSV scheme during login. The facts corresponding to each image appear below that image. Users enter the key, a lowercase letter shown in parentheses, in the password field (on top) to select the corresponding image. The keys are randomly assigned to images each time the portfolio is loaded, where no two images share the same key. During login, users are shown five such portfolios, where each presents a distinct set of 16 images including one of the five assigned images.

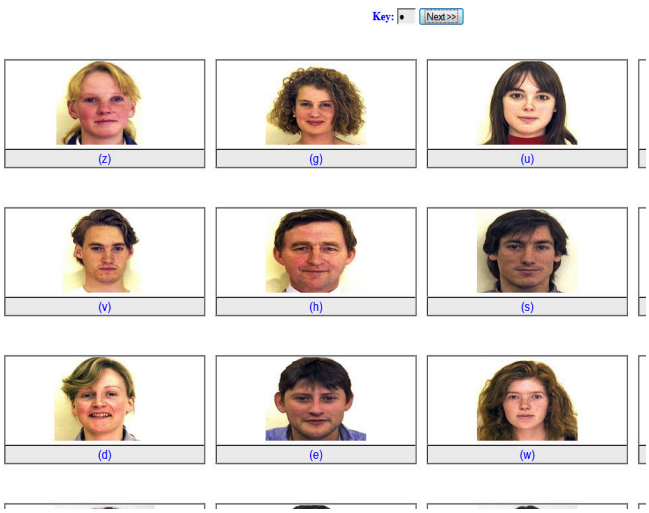


Figure 3: A partial screen shot of FaceSUI during login. Users are shown five such portfolios, and each presents a distinct set of 16 images including one of the five assigned images.

User interaction: Asking users to write a short description about the assigned images during registration. These descriptions would not be shown at login nor stored by the system.

To explore the impact of cues and user interaction on graphical recognition, we design a control condition for face recognition, in which the images in a portfolio remain the same but randomly positioned each time that portfolio is loaded, as in Passfaces [1]. In this paper, we term this control condition *FaceR* (**Face** images with **R**andom positioning). We design a similar control condition for object recognition that we call *ObjectR*.

3.4.1 Cued-Recognition

Based on psychology research [6, 46], we argue that password schemes should ease the memory retrieval of authentication information through providing users with cues, since it is difficult to remember information spontaneously without memory cues. In this regard, the most effective cues are those that are present at the time of remembering [45]. In this paper, we aim to understand the impact of spatial and verbal cues in improving the memorability of cognometric graphical passwords.

Spatial Cues. *Semantic priming* refers to recognizing an object through its relationship with other objects around it [1]. Semantic priming thus eases the recognition task [1], which is augmented by having a fixed set of objects in a certain place. In a graphical password scheme offering spatial cues, the images in a portfolio remain the same and are presented at a fixed position whenever that a portfolio is loaded. For example, in Figure 2, the clock is not only in the upper-left-hand corner each time, but it is always next to the mango and above the dining table. This establishes a relationship between the objects and reinforces semantic priming. Thus, the schemes (except control conditions: FaceR and ObjectR) in our study offer spatial cues, while we design *FaceS* (**Face** Images with **S**patial cues) and *ObjectS* (**Object** Images with **S**patial cues) schemes to understand the precise impact of spatial cues on graphical recognition.

In FaceS and ObjectS, the images in a portfolio remain at the same position each time that portfolio is loaded. We compare FaceS with FaceR and ObjectS with ObjectR to show the impact of spatial cues on face recognition and object recognition, respectively.

Verbal Cues. If the system provides verbal cues, i.e., phrases/facts related to the images, then users may focus their attention on associating the images with the corresponding cues, which should help to process and encode the information to store them in long-term memory. The cues would also assist users to recognize the images in the future and thus enhance their memorability.

In our study, the *ObjectSV* (**Object** images with **S**patial and **V**erbal cues) scheme provides users with verbal cues. For example, the image of a 'Dining Table' is provided with the name of this object ('Dining Table'), and a corresponding phrase/fact ("People started to use dining table during 16th century."). Yan et. al. [50] examined the influence of phrases in increasing the memorability of passwords, which inspires us to accommodate a common phrase or fact for each image as a verbal cue. See Figure 2 showing a partial screen shot of the login screen for ObjectSV.

We typically do not provide a physical description of an image (e.g., "A dining table has four legs.") as a phrase or fact, since it is already visible in the image. Rather, ObjectSV offers an additional fact corresponding to the object (in image) as a verbal cue for helping users to better remember the image through correlating it with the given cues. Thus, we did not accommodate verbal cues for face

recognition, since it is not possible to provide users with facts about the anonymous face images.

We compare ObjectSV with ObjectR to examine the memorability gain of combining spatial and verbal cues, and we compare ObjectSV with ObjectS to examine the more precise impact of verbal cues.

3.4.2 User Interaction

In our study, we implement user interaction through the schemes FaceSUI (**Face** images with **S**patial cues and **U**ser **I**nteraction) and ObjectSUI (**Object** images with **S**patial cues and **U**ser **I**nteraction)), in which the system asks users to describe each assigned image during registration. The user interface includes a text field for users to type a short description about the assigned image. The descriptions, provided by the users during registration, are not stored by the system nor shown in any form at login. The sole purpose of this approach is to make random images more familiar to the users through motivating their deeper observations. See Figure 3 showing a partial screen shot of the login screen for FaceSUI scheme.

Unlike existing graphical password schemes, such as Passfaces [1], where users just use their visual memory to memorize the given images, FaceSUI and ObjectSUI schemes leverage both visual memory and action-event memory [29] for a more elaborate encoding of authentication information (e.g., assigned images), which help users to remember and retrieve the processed information efficiently over an extended period of time.

We compare FaceSUI with FaceR and ObjectSUI with ObjectR to examine the memorability gain through combining spatial cues with user interaction, while the comparisons of FaceSUI with FaceS and ObjectSUI with ObjectS reveal the more precise impact of user interaction on face recognition and object recognition, respectively.

3.5 Variant Response

In existing cognometric graphical password schemes [1, 26], mouse input is used to select an image, where the images in a portfolio remain the same but are positioned randomly each time that a portfolio is loaded to compensate for shoulder surfing risk during login. Since the existing recognition-based schemes [26] are presented through our control conditions, FaceR and ObjectR schemes also use mouse input to select images. In fixed-position schemes, i.e., schemes offering spatial cues, mouse input is badly susceptible to shoulder surfing and should not be used. Instead, we use keyboard input, where each time a portfolio is loaded, a distinct lowercase letter `a-z` is assigned randomly as a *key* to one image on the page, and the user inputs the key letter corresponding to her assigned image into a single-character password field to move on to the next portfolio (see Figure 2 and Figure 3). The user-entered letter in the password field is shown as an asterisk to reduce the risk of shoulder surfing.

Keyboard input offers the ability to use *variant response*, in which the user's responses (typed characters) vary for each login session [8]. Tari et al. performed a shoulder-surfing study that showed that cognometric schemes with keyboard input and variant response provide higher resilience to shoulder surfing than schemes with mouse input [43]. Thus, we used keyboard input with variant response for a fair test of reasonably secure conditions compared with the control conditions.

4. USER STUDY

We now present the design of our user study to explore the impact of cues and user interaction on the memorability of recognition-based graphical authentication. In this study, we used a within-subjects design consisting of seven experimental conditions (see Figure 1). Using a within-subjects design controls for individual differences and permits the use of statistically stronger hypothesis tests. The Institutional Review Board (IRB) at the University of Texas at Arlington (UT Arlington) approved the procedures of our user study.

4.1 Participants, Apparatus and Environment

For this experiment, we recruited 56 students (40 women, 16 men) through our university's Psychology Research Pool. Participants came from diverse backgrounds, including majors from Nursing, Psychology, Business, Environmental Science, Biochemistry, and Spanish Language. The age of the participants varied between 18 to 51 with a mean age of 21. Participants received course credit as a compensation for participating in our study. They were aware that the amount of compensation would not be affected by their performance or feedback in this study.

We conducted lab studies in an isolated room on campus, free from outside distractions. The studies were conducted with one participant at a time to allow the researchers to observe the users' interactions with the system, where the participants did not perceive any real risk. We used mock sites, each with distinct look-and-feel to distinguish between multiple schemes. In particular, we created seven realistic and distinct websites, including sites for banking, social networking, email, movie streaming, and shopping. The sites used the images and layouts from familiar commercial sites, and each of them was equipped with one of our seven graphical password schemes.

In our study, each of the five portfolios in a scheme consists of unique set of images that are not repeated in any other portfolio nor in any other scheme. In other words, we did not reuse any images. Users were shown the same set of images for a given portfolio in a scheme, where the passwords were randomly assigned by the system. We collected the images and phrases/facts (verbal cues) from free online resources.

4.2 Procedure

In password studies with multiple sessions, a one-week delay is a common interval (e.g., [2,4,5,16,34,49]), and Hayashi and Hong [25] showed that a one-week delay is larger than the maximum average interval for a user between subsequent logins to any of her important online accounts. So to test users' memorization of the assigned passwords in our study, each participant sat in two sessions, each lasting around 30 minutes, with the second session one week after the first one.

Session 1. After signing a consent form, the participants were given an overview of our study. Then they performed registration for each of the seven sites, each outfitted with a distinct scheme. The sites were shown to the participants in a random order during registration. After registering with each scheme, participants performed a practice login with that scheme. They performed another practice login with each scheme after completing registration for all of the seven sites. We did not collect data for these practice trials. They were asked to not record (e.g., write down or take a picture of) their authentication secrets.

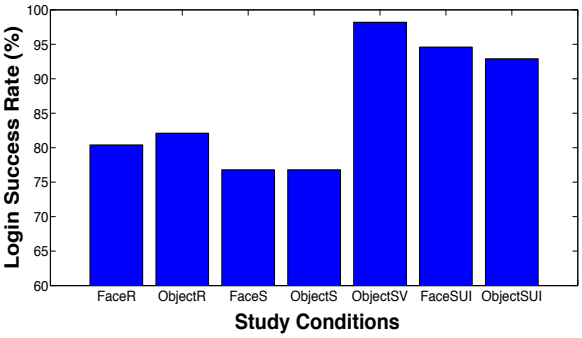


Figure 4: Login success rates for the study conditions [Number of participants=56]

Session 2. The participants returned one week after registration and logged into each of the seven sites using the assigned graphical passwords. The sites were shown to the participants in random order, and they could make a maximum of five attempts for a successful login. After the participants had finished, they were compensated and thanked for their time.

4.3 Ecological Validity

In our study, most of the participants were young and all of them were university educated. This participant pool may not generalize to the entire population. However, they are still representative of a large number of frequent Web users. They also came from diverse majors. As the study was performed in a lab setting, we were only able to gather data from 56 participants. However, lab studies have been preferred to examine brain-powered memorability of passwords [18]. Since lab studies take place in a controlled setting, it helps to establish performance bounds and figure out whether field tests are worthwhile in future research. We believe that 56 provides a suitable sample size for a lab study as compared to the prior studies on password memorability [2, 4, 5, 11, 12, 44, 48].

5. RESULTS

We now discuss the results of our user study. To analyze our results, we use statistical tests and consider results comparing two conditions to be significantly different when we find $p < 0.05$. When comparing two conditions where the variable is at least ordinal, we use a Wilcoxon signed-rank test for the matched pairs of subjects and a Wilcoxon-Mann-Whitney test for unpaired results. Wilcoxon tests are similar to t-tests, but make no assumption about the distributions of the compared samples, which is appropriate to the datasets in our conditions. Whether or not a participant successfully authenticated is a binary measure, and so we use either a McNemar's test (for matched pairs of subjects) or a chi-squared test (for unpaired results) to compare login success rates between two conditions. Here, we tested the following hypotheses:

Hypothesis 1

$H1_a$: *The login success rate for FaceS would be significantly higher than that for FaceR.*

$H1_b$: *The login success rate for ObjectS would be significantly higher than that for ObjectR.*

In a graphical password scheme offering spatial cues, the images in a portfolio remain the same and presented at a fixed position whenever that portfolio is loaded, which establishes a relationship between them and reinforces semantic priming (see §3 for details). Thus, we hypothesized that FaceS and ObjectS, offering spatial cues, would have significantly higher login success rates than FaceR and ObjectR, respectively, in which the position of images in a portfolio are randomly changed each time that a portfolio is loaded.

Our results show that out of 56 participants in our study, 45 participants (80%) succeeded to log in using FaceR, while 43 participants (77%) logged in successfully with FaceS. For ObjectR and ObjectS schemes, 46 participants (82%) and 43 participants (77%) succeeded to log in, respectively (see Figure 4). Thus, $H1_a$ and $H1_b$ are not supported by these results.

Whether or not a participant successfully authenticated is a binary measure, so we compare login success rates between conditions using McNemar's test. We did not find a significant difference in login success rate between FaceS and FaceR, $\mathcal{X}^2(1, N = 56) = 0.08$, $p = 0.77$, nor between ObjectS and ObjectR, $\mathcal{X}^2(1, N = 56) = 0.36$, $p = 0.55$.

Hypothesis 2

$H2_a$: *The login success rate for ObjectSV would be significantly higher than that for ObjectS.*

$H2_b$: *The login success rate for ObjectSV would be significantly higher than that for ObjectR.*

The ObjectSV scheme offers spatial and verbal cues (i.e., phrase or facts related to the images), where cues are shown both at registration and login. So, the users could memorize their graphical passwords through associating them with the corresponding cues, which should help to process and encode the information to store them in long-term memory (see §3 for detailed discussion). Moreover, the cues would assist users to recognize the images in the future, which should enhance their memorability. Thus, we hypothesized that ObjectSV scheme would have significantly higher login success rate than ObjectS and ObjectR schemes.

We observed a 98% login success rate for ObjectSV scheme, while 55 out of 56 participants could log in successfully one week after registration. As we compare the login success rate for ObjectSV scheme with that for ObjectS (77%) and ObjectR (82%), the results for McNemar's test show that ObjectSV had a significantly higher login success rate than ObjectS, $\mathcal{X}^2(1, N = 56) = 10.08$, $p < 0.05$ and ObjectR, $\mathcal{X}^2(1, N = 56) = 7.11$, $p < 0.05$. Hence, $H2_a$ and $H2_b$ are supported by these results.

Hypothesis 3

$H3_a$: *The login success rate for FaceSUI would be significantly higher than that for FaceS.*

$H3_b$: *The login success rate for FaceSUI would be significantly higher than that for FaceR.*

$H3_c$: *The login success rate for ObjectSUI would be significantly higher than that for ObjectS.*

$H3_d$: *The login success rate for ObjectSUI would be significantly higher than that for ObjectR.*

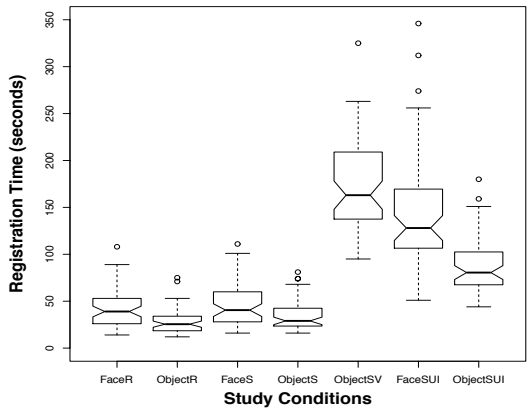


Figure 5: Registration time for the study conditions

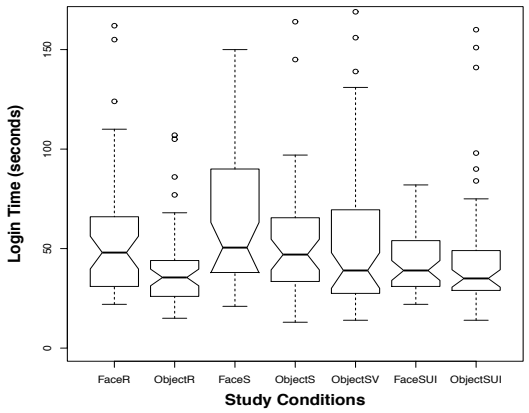


Figure 6: Login time for the study conditions

FaceR and ObjectR schemes represent existing graphical password schemes that use just the visual memory of users [1, 26]. FaceSUI and ObjectSUI schemes leverage both visual memory and action-event memory [29], which contributes to an elaborative encoding of the assigned images and thus assists users with memorizing the processed information. In addition, FaceSUI and ObjectSUI schemes offer spatial cues. So, we hypothesized that the login success rate for FaceSUI would be significantly higher than that for FaceS and FaceR schemes, while ObjectSUI would have a significantly higher login success rate than ObjectS and ObjectR schemes.

Our results show that 53 participants (95%) in FaceSUI and 52 participants (93%) in ObjectSUI scheme logged in successfully one week after registration. As we compare the login success rate for FaceSUI with that for FaceS (77%) and FaceR (80%), the results for McNemar's tests show that FaceSUI had a significantly higher login success rate than FaceS, $\mathcal{X}^2(1, N = 56) = 8.1$, $p < 0.05$ and FaceR, $\mathcal{X}^2(1, N = 56) = 4.9$, $p < 0.05$.

We also found that the login success rate for ObjectSUI was significantly higher than that for ObjectS, $\mathcal{X}^2(1, N = 56) = 7.11$, $p < 0.05$ and ObjectR, $\mathcal{X}^2(1, N = 56) = 4.17$, $p < 0.05$. Thus, $H3_a$, $H3_b$, $H3_c$, and $H3_d$ are supported by these results.

5.1 Registration Time

We illustrate the results for registration time in Figure 5. We found that the median registration times for FaceR and FaceS were 39 seconds and 41 seconds, respectively, while FaceSUI scheme had a median registration time of 128 seconds. We use a Wilcoxon signed-rank test (appropriate for matched pairs of subjects) to evaluate two schemes in terms of registration time. The results show that the registration time for FaceR ($V = 1596$, $p < 0.05$) and FaceS ($V = 1596$, $p < 0.05$) were significantly less than that for FaceSUI scheme. We did not find a significant difference in registration time between FaceR and FaceS ($V = 789.5$, $p = 0.69$).

Our results show that the median registration time for ObjectSUI scheme was 81 seconds, while ObjectR and ObjectS schemes had median registration time of 26 seconds and 29 seconds, respectively. The results for Wilcoxon signed-rank tests show that the registration time for ObjectR ($V = 1595$, $p < 0.05$) and ObjectS ($V = 1582.5$, $p < 0.05$) were significantly less than that for ObjectSUI. We also found that the registration time for ObjectR was significantly less than that for ObjectS ($V = 1074.5$, $p < 0.05$). In our study, ObjectSV scheme had a median registration time of 163 seconds, while the registration time for ObjectR ($V = 1596$, $p < 0.05$), ObjectS ($V = 1596$, $p < 0.05$), and ObjectSUI ($V = 1566.5$, $p < 0.05$) were significantly less than that for ObjectSV scheme.

We intend to see if the image type had any impact on the required time for learning system-assigned images (i.e., registration time). Our results show that the registration time for ObjectR was significantly less than that for FaceR ($V = 147.5$, $p < 0.05$). We also found that the registration time for ObjectS was significantly less than that for FaceS scheme ($V = 249$, $p < 0.05$), while the registration time for ObjectSUI was significantly less than that for FaceSUI ($V = 39$, $p < 0.05$).

5.2 Login Time and Number of Attempts

In this paper, *number of attempts* and *login time* respectively refer to the required attempts and time for successful logins only, unless otherwise specified. We do not get matched pairs of subjects while comparing two schemes in terms of login time or number of attempts for successful logins, since some participants who logged in successfully for one scheme failed in the other scheme. So, we use a Wilcoxon-Mann-Whitney test (appropriate for unpaired results) to evaluate two schemes in terms of login time and the number of attempts for successful logins.

5.2.1 Login Time

We illustrate our results for login time in Figure 6. We found that the median login time for FaceR and FaceS were 48 and 51 seconds, respectively, while FaceSUI had a median login time of 39 seconds. The results for Wilcoxon-Mann-Whitney tests show that the login time for FaceSUI scheme was significantly less than that for FaceS ($W = 746.5$, $p < 0.05$). We did not find a significant difference in login time between FaceSUI and FaceR ($W = 1017$, $p = 0.21$), nor between FaceR and FaceS ($W = 1096$, $p = 0.20$).

Our results show that the median login time for ObjectSUI scheme was 35 seconds, while ObjectR and ObjectS schemes had median login times of 36 and 47 seconds, respectively.

The results for Wilcoxon-Mann-Whitney tests show that the login time for ObjectSUI ($W = 814$, $p < 0.05$) and ObjectR ($W = 1310.5$, $p < 0.05$) were significantly less than that for ObjectS. We did not find a significant difference in login time between ObjectSUI and ObjectR ($W = 1285$, $p = 0.53$).

We found a median login time of 39 seconds for ObjectSV. No significant difference was found in terms of login times when we compared ObjectSV with ObjectR ($W = 1489$, $p = 0.13$), ObjectS ($W = 1020.5$, $p = 0.25$), and ObjectSUI ($W = 1560.5$, $p = 0.42$).

We compared ObjectR and FaceR to see if image type had any impact on login time given random image positioning. The results for Wilcoxon-Mann-Whitney tests show that the login time for ObjectR was significantly less than that for FaceR ($W = 1312.5$, $p < 0.05$). However, we did not find a significant difference in login time between ObjectS and FaceS ($W = 1033$, $p = 0.26$), nor between ObjectSUI and FaceSUI ($W = 1498.5$, $p = 0.44$).

5.2.2 Number of Attempts

The mean number of attempts for a successful login was less than two for each of the seven schemes, while the median was one in each case (see Table 1). The results for Wilcoxon-Mann-Whitney tests found no significant difference between any pair of study conditions in terms of the number of attempts for a successful login.

6. DISCUSSION

Cognometric graphical passwords (e.g., Passfaces [1]) are now commercially available and deployed by a number of large websites, in which the images are assigned by the system to provide reasonable security guarantees. They fail, however, to gain satisfactory memorability [17], since it is difficult for most people to memorize system-assigned passwords. Our study explores a promising new direction to improve memorability for these passwords by leveraging humans' cognitive abilities through cues and interaction.

6.1 Cued-Recognition

We accommodate the scientific understanding of long-term memory to improve the memorability of system-assigned cognometric passwords. As noted by Atkinson and Shiffrin [7], any new information is transferred from short-term memory to long-term memory, when it is duly processed and encoded. In our study, we explored the impact of spatial and verbal cues for an elaborate encoding of authentication information to ease recognition during login.

Table 1: Number of Attempts for Successful Logins [SD: Standard Deviation]

Study Conditions	Mean	Median	SD
FaceR	1.3	1	0.7
ObjectR	1.2	1	0.5
FaceS	1.3	1	0.6
ObjectS	1.3	1	0.7
ObjectSV	1.4	1	0.9
FaceSUI	1.1	1	0.3
ObjectSUI	1.1	1	0.4

Al-Ameen et al. [5] show the potential of combining multiple cues to aid recognition, where the participants were asked to rate the efficacy of each type of cue. The participants rated spatial cues to be more effective than verbal cues to aid recognition. In our study, however, we made a deeper investigation of this issue through a direct comparison between schemes offering different combinations of cues, and we found that spatial cues did not significantly contribute to enhance memorability, while verbal cues made a significant contribution in this regard. Thus, the findings from our study make an important contribution to understand the effectiveness of memory cues (e.g., spatial and verbal cues) and indicate that relying solely on user feedback might not be a reliable approach to understand the impact of cues on password memorability.

6.1.1 Spatial Cues

To understand the efficacy of spatial cues, we compared FaceS and ObjectS schemes with fixed positions of all images in a portfolio with FaceR and ObjectR schemes with random repositioning of the images. Our results show that spatial cues did not contribute to improve the login success rate for either face recognition or object recognition.

In theory, spatial cues reinforce semantic priming and thus ease the recognition task [1]. Further, the survey results from Al-Ameen et al. [5] suggest that users found them important. It is possible that spatial cues are less effective when remembering multiple images, in which case it might create confusion when a user attempts to recognize the images using spatial cues. In our future work, we would perform a field study to explore if a higher login frequency could lead to training effects that could help users to benefit from spatial cues.

6.1.2 Verbal Cues

We compared ObjectSV, which has spatial and verbal cues, with both the object-based control condition (ObjectR) and ObjectS, which has spatial cues but not verbal ones. We found a 98% login success rate for ObjectSV, which was significantly higher than those for ObjectS and ObjectR. Given that we also found no benefit in spatial cues alone, we conclude that providing verbal cues with the images played a significant role in improving memorability.

During registration with ObjectSV, the participants may have learned the assigned images by correlating them with the verbal cues. This then assisted them with a more elaborate processing of the authentication information, but it also contributed to the higher registration time compared to ObjectR and ObjectS. No significant difference was found in terms of login time or number of attempts for successful logins between ObjectSV and either ObjectR or ObjectS.

We observed an interesting anecdotal case from one participant. In the first session, he told us that he used to struggle in memorizing new information because of a severe injury on his head. At this point, we were interested to see his login performances in the second session, and we found that he could log in successfully only with the schemes offering verbal cues (e.g., ObjectSV) and leveraging user interaction (e.g., FaceSUI). At the end of second session, he said, "It is much too difficult to manage with just images. The fact [verbal cue] attached with an image help to encode the images." Indeed, the benefit of verbal cues may not be important to all users, but may instead help users who struggle with

graphical information alone, like the approximately 20% of participants who failed to login with ObjectS and ObjectR. If so, it may be good to individually tailor a scheme with different types of information for different users.

6.2 User Interaction

We tested user interaction with the FaceSUI and ObjectSUI schemes, in which we have users describe their assigned images at registration so as to deepen users' processing of authentication information. For clarity, we again note that the descriptions would be immediately destroyed and need not even be transferred to the server. In our study, we stored the user-written descriptions for the purpose of analysis. Our manual inspection shows that users made meaningful descriptions. If deployed, systems could use automated checks to partially enforce this.

We compare FaceSUI with FaceR and ObjectSUI with ObjectR to examine the memorability gain from combining spatial cues with user interaction, while comparisons of FaceSUI with FaceS and ObjectSUI with ObjectS reveal the more precise impact of user interaction on face recognition and object recognition, respectively. Our results show that the login success rate for FaceSUI (95%) was significantly higher than that for FaceS and FaceR and the login success rate for ObjectSUI (93%) was significantly higher than for ObjectS and ObjectR. It appears that user interaction played the major role to improve the success rates, since spatial cues by themselves did not help.

During registration with user interaction based schemes (e.g., FaceSUI and ObjectSUI), the participants wrote descriptions about the assigned images, which required significantly higher registration time for FaceSUI (in comparison to FaceS and FaceR) and ObjectSUI (in comparison to ObjectS and ObjectR).

6.3 Cued-Recognition vs. User Interaction

In our study, we found a significant improvement in login success rate through cued-recognition (ObjectSV) and user interaction (FaceSUI, ObjectSUI). The login success rate in ObjectSV was higher than the ObjectSUI and FaceSUI schemes, but no significant difference was found in this regard. We did not find a significant difference in login time or number of attempts for successful logins, when comparing ObjectSV with ObjectSUI and FaceSUI schemes. However, the registration times for ObjectSUI and FaceSUI were significantly less than that for ObjectSV scheme, indicating that the participants required less time to learn the assigned images through writing a description as compared to memorizing images through correlating them with the given verbal cues.

The deployment of ObjectSV scheme may require more effort as compared to other cognometric graphical password schemes that present users with images only, since ObjectSV requires writing verbal cues in addition to the images.

The success of the user-interaction-based schemes depends on the involvement of users in describing the assigned images. Our observations during the study reveal that all of the participants in ObjectSUI and FaceSUI schemes put in effort to describe the assigned images. Users in a lab study, however, are naturally open to take on requested tasks, while users in real life may get lazy. We plan to explore this issue deeper through a field study in a real-life setting and identify more ways for actively compelling users to engage with the interaction activity.

6.4 Face recognition vs. Object Recognition

Hlywa et al. [26] conducted a study to examine the effect of image type on the usability of recognition-based graphical passwords, in which they focused on exploring that impact for randomly-positioned images (similar to FaceR and ObjectR in our study).[2] In this paper, we provide a deeper understanding on this issue, while our investigation about the efficacy of cues and user interaction for face and object images lets us compare the face and object recognition in terms of registration time, login success rate, and login time for three different conditions: i) The images in a portfolio are randomly positioned each time that a portfolio is loaded (FaceR, ObjectR), ii) The images in a portfolio remain at the same position each time that a portfolio is loaded (FaceS, ObjectS), iii) The images in a portfolio are placed at the same position each time that a portfolio is loaded, and users learn the graphical passwords through interaction, e.g., writing a description about the assigned images at registration (FaceSUI, ObjectSUI).

The registration time for ObjectSUI scheme was found to be significantly less than that for FaceSUI scheme, which indicates that it was less time consuming for the participants to describe object images in comparison to face images. We also found that the registration time for ObjectR and ObjectS were significantly less than for FaceR and FaceS, respectively. Thus, users seem to need less time for object images. We speculate that since object images can be selected to be rather distinct from each other within a portfolio both visually and semantically (see Fig. 2), it takes less time to memorize a particular assigned object than for faces, which have distinct details but a basic similarity.

In login performance, we found no significant difference in login success rates as we compared ObjectR with FaceR, ObjectS with FaceS, and ObjectSUI with FaceSUI. ObjectR had a significantly lower login time than FaceR, but no significant difference was found in login time as we compared ObjectS with FaceS and ObjectSUI with FaceSUI. Random positioning may make visually distinctiveness more important to quick login times.

6.5 Input Type

We note that we used mouse input for our control conditions and keyboard input for the other conditions. As explained in Sec. 3.5, this was done to keep the control conditions the same as existing cognometric schemes while ensuring reasonable protection from shoulder surfing in the spatial-cue conditions. The input type, however, could affect memorability and login time. For example, the additional effort of selecting the key letter for typing may help with memorization at registration. On the other hand, using the mouse may provide greater focus on the visual elements, perhaps including cues. Further exploration of input options may be of interest if spatial cues are abandoned in favor of random image placement; in spatially fixed schemes, mouse input is likely too vulnerable to shoulder surfing for practical use.

[2] For randomly-positioned images, our findings about the impact of image type in terms of login time and login success rate are similar to those of Hlywa et al. [26]. Their study did not evaluate the effect of image type on registration time.

6.6 Future Work

Now that lab-study results show promise for implementing verbal cues and user interaction, it would be interesting to evaluate the approaches through a long-term field study with larger and more diverse populations, where we would explore the training effects on login performances over time. A recent field study [3] reveals that login time significantly decreases with the frequent use of a scheme due to training effects.

Although graphical passwords leverage the picture superiority effect, not all users may have a strong visual memory. Additionally, many graphical password schemes require good vision and motor skills, which elderly users [38] may lack. Thus, providing verbal cues for the images could assist users with memorizing their graphical passwords. We would further explore this issue in our future work through a user study with participants from different age groups. We would also make a deeper investigation to understand the impact of cues and user interaction in improving the memorability of passwords for the people with different cognitive limitations.

7. CONCLUSION

In our study, we aimed to better understand the impact of cues and user interaction on system-assigned recognition-based graphical passwords, and designed seven different study conditions to achieve this goal. In a study with 56 participants, we had a 98% login success rate for a scheme offering spatial and verbal cues (ObjectSV), while a scheme based on user interaction had a 95% login success rate for face images (FaceSUI) and a 93% login success rate for object images (ObjectSUI). Our analysis show that verbal cues and user interaction made an important contribution to gain significantly higher login success rate as compared to the control conditions representing existing graphical password schemes. Contrary to the suggestions of user feedback from a prior study [5], we found that spatial cues were not effective. These findings shed light on a promising research direction to leverage humans' cognitive ability through cues and interaction in gaining high memorability for system-assigned random passwords.

8. ACKNOWLEDGEMENT

This material is based upon work supported by the National Science Foundation under Grant No. CNS-1423163 and CAREER Grant No. CNS-0954133.

9. REFERENCES

[1] Passfaces corporation. The science behind Passfaces. White paper, `http://www.passfaces.com/enterprise/resources/white_papers.htm`.

[2] M. N. Al-Ameen, S. M. T. Haque, and M. Wright. Q-A: Towards the solution of usability-security tension in user authentication. Technical report, arXiv:1407.7277 [cs.HC], 2014.

[3] M. N. Al-Ameen and M. Wright. A comprehensive study of the GeoPass user authentication scheme. Technical report, arXiv:1408.2852 [cs.HC], 2014.

[4] M. N. Al-Ameen and M. Wright. Multiple-password interference in the geopass user authentication scheme. In *USEC*, 2015.

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

[6] J. R. Anderson and G. H. Bower. Recognition and recall processes in free recall. *Psychological Review*, 79(2), 1972.

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

[8] R. Biddle, S. Chiasson, and P. van Oorschot. Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys*, 44(4), 2012.

[9] S. Chiasson, R. Biddle, and P. C. van Oorschot. A second look at the usability of click-based graphical passwords. In *SOUPS*, 2007.

[10] S. Chiasson, A. Forget, R. Biddle, and P. van Oorschot. User interface design affects security: Patterns in click-based graphical passwords. *International Journal of Information Security*, 8(6), 2009.

[11] S. Chiasson, E. Stobert, R. Biddle, and P. van Oorschot. Persuasive cued click-points: design, implementation, and evaluation of a knowledge- based authentication mechanism. *IEEE TDSC*, 9, 2012.

[12] S. Chiasson, P. C. van Oorschot, and R. Biddle. Graphical password authentication using cued click points. In *ESORICS*, 2007.

[13] A. Das, J. Bonneau, M. Caesar, N. Borisov, and X. Wangz. The tangled web of password reuse. In *NDSS*, 2014.

[14] D. Davis, F. Monrose, and M. Reiter. On user choice in graphical password schemes. In *USENIX Security*, 2004.

[15] A. E. Dirik, N. Memon, and J.-C. Birget. Modeling user choice in the passpoints graphical password scheme. In *SOUPS*, 2007.

[16] P. Dunphy and J. Yan. Do background images improve "Draw a Secret" graphical passwords? In *CCS*, 2007.

[17] K. Everitt, T. Bragin, J. Fogarty, and T. Kohno. A comprehensive study of frequency, interference, and training of multiple graphical passwords. In *CHI*, 2009.

[18] S. Fahl, M. Harbach, Y. Acar, and M. Smith. On the ecological validity of a password study. In *SOUPS*, 2013.

[19] D. Florencio and C. Herley. Where do security policies come from? In *SOUPS*, 2010.

[20] A. Forget. *A World with Many Authentication Schemes*. PhD thesis, Carleton University, 2012.

[21] A. Forget, S. Chiasson, P. van Oorschot, and R. Biddle. Improving text passwords through persuasion. In *SOUPS*, 2008.

[22] A. Forget, S. Chiasson, P. C. van Oorschot, and R. Biddle. Persuasion for stronger passwords: Motivation and pilot study. In *PT*, 2008.

[23] S. Furnell, I. Papadopoulos, and P. Dowland. A long-term trial of alternative user authentication technologies. *Information Management and Computer Security*, 12(2), 2004.

[24] J. V. Haxby, E. A. Hoffman, and M. I. Gobbini. The distributed human neural system for face perception. *Trends in Cognitive Science*, 4:223, 2000.

[25] E. Hayashi and J. I. Hong. A diary study of password usage in daily life. In *CHI*, 2011.

[26] M. Hlywa, R. Biddle, and A. S. Patrick. Facing the facts about image type in recognition-based graphical passwords. In *ACSAC*, 2011.

[27] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin. The design and analysis of graphical passwords. In *USENIX Security*, 1999.

[28] M. Just and D. Aspinall. Personal choice and challenge questions a security and usability assessment. In *SOUPS*, 2009.

[29] M. Knopf, A. Mack, S. Lenel, and S. Ferrante. Memory for action events: Findings in neurological patients. *Scandinavian Journal of Psychology*, 46, 2005.

[30] C. Kuo, S. Romanosky, and L. F. Cranor. Human selection of mnemonic phrase-based passwords. In *SOUPS*, 2006.

[31] D. A. Minnebusch, B. Suchan, O. Koster, and I. Daum. A bilateral occipitotemporal network mediates face perception. *Behavioural Brain Research*, 198 (1):179, 2009.

[32] D. Nali and J. Thorpe. Analyzing user choice in graphical passwords. Technical Report TR-04-01, School of Computer Science, Carleton University, 2004.

[33] 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.

[34] J. Nicholson, L. Coventry, and P. Briggs. Age-related performance issues for PIN and face-based authentication systems. In *CHI*, 2013.

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

[36] 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.

[37] A. Rabkin. Personal knowledge questions for fallback authentication: Security questions in the era of Facebook. In *SOUPS*, 2008.

[38] K. Renaud. A visuo-biometric authentication mechanism for older users. In *British HCI*, 2005.

[39] S. Schechter, A. J. B. Brush, and S. Egelman. It's no secret: Measuring the security and reliability of authentication via 'secret' questions. In *IEEE S&P*, 2009.

[40] R. Shay, I. Ion, R. W. Reeder, and S. Consolvo. "my religious aunt asked why i was trying to sell her Viagra": Experiences with account hijacking. In *CHI*, 2014.

[41] R. Shay, P. G. Kelley, S. Komanduri, M. L. Mazurek, B. Ur, T. Vidas, L. Bauer, N. Christin, and L. F. Cranor. Correct horse battery staple: Exploring the usability of system-assigned passphrases. In *SOUPS*, 2012.

[42] 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.

[43] F. Tari, A. Ozok, and S. Holden. A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords. In *SOUPS*, 2006.

[44] J. Thorpe, B. MacRae, and A. Salehi-Abari. Usability and security evaluation of GeoPass: A geographic location-password scheme. In *SOUPS*, 2013.

[45] E. Tulving and D. M. Thompson. Encoding specificity and retrieval processes in episodic memory. *Psychological Review*, 80(5), 1973.

[46] E. Tulving and M. Watkins. Continuity between recall and recognition. *American Journal of Psych*, 86(4), 1973.

[47] W. A. Wickelgren and D. A. Norman. Strength models and serial position in short-term recognition memory. *Journal of Mathematical Psychology*, 3, 1966.

[48] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon. Authentication using graphical passwords: Effects of tolerance and image choice. In *SOUPS*, 2005.

[49] N. Wright, A. S. Patrick, and R. Biddle. Do you see your password? Applying recognition to textual passwords. In *SOUPS*, 2012.

[50] J. Yan, A. Blackwell, R. Anderson, and A. Grant. Password memorability and security: Empirical results. *IEEE Security and Privacy*, 2 (5):25, 2004.