Learning System-assigned Passwords (up to 56 Bits) in a Single Registration Session with the Methods of Cognitive Psychology

S M Taiabul Haque*, Mahdi Nasrullah Al-Ameen†, Matthew Wright‡ and Shannon Scielzo§
*University of Central Missouri
haque@ucmo.edu
†Clemson University
malamee@clemson.edu
‡Rochester Institute of Technology
matthew.wright@rit.edu
§UT Southwestern Medical Center
shannon.scielzo@utsouthwestern.edu

***Abstract*—System-assigned random passwords offer security guarantees against guessing attacks but suffer from poor memorability. In this work, we review the cognitive psychology literature and identify two training methods appropriate to aid users in memorizing system-assigned passwords. The *method of loci* exploits users' spatial and visual memory, while the *link method* helps users by creating a chain of memory cues. We developed techniques to automatically take a given random password and generate training aids (videos) based on each of these methods. The results of a memorability study showed that both methods were significantly better than a control condition (no training) and that the *method of loci* had a login success rate of 86%, a high value for any recall-based study with system-assigned passwords. With a registration time of 160 seconds and a median login time of 9 seconds, this method holds promise as a direction to addressing the usability-security trade-off in user authentication. We further extend this idea to help users memorize long system-assigned random passwords that offer almost crypto-level security and conduct a second memorability study. The results of this study demonstrated that with the help of a password hint, 81% of participants were able to recall the password after a week. This indicates that the *method of loci* can be leveraged to help users memorize cryptographically-strong secret in just one session, and thus offers a more viable alternative to the *spaced repetition* technique, which involves dozens of sessions of user training.**

I. Introduction

Due to its simplicity and cost effectiveness, textual password-based authentication still remains the most common method of user authentication on the Web, and there is little chance this will change in the near future [25]. Unfortunately, traditional user-selected passwords have both usability and security problems. As formulated by Wiedenbeck et al., a good password needs to satisfy two conflicting requirements at the same time: being easy to remember and hard to guess [52]. It is a clear violation of designing for usability to expect users to manage this dilemma without specialized training in either password security or memorization techniques. In the end, users often select weak passwords [57], [8] and attempt to satisfy password strength requirements in predictable ways [48]. Passwords are also frequently reused, creating further vulnerabilities [20], [57], [47].

One approach to addressing these issues is to employ system-assigned random passwords. By removing the burden of password creation from the user, the system eliminates dictionary and targeted guessing attacks. Indeed, every user's password has a guaranteed level of security. Furthermore, it helps to limit password reuse. The major limitation of this approach, however, is memorability. For a user, a random sequence of characters or words is hard to recall without help [46], [54], [58], [53].

Our work aims to address this critical issue of memorability for system-assigned random passwords. After reviewing the literature on cognitive psychology and memorization techniques, we picked two scientifically proven methods that would be pertinent to password memorization. Our system design involves implementing novel training interfaces for both of these methods in the context of memorizing system-assigned random passwords.

We conducted a within-group memorability study with 52 participants in order to assess the effectiveness of these methods. The first method, known as the *method of loci*, achieved a recall success rate of 86%, a very high value for any recall-based memorability study with system-assigned random passwords. The second method, known as the *link method*, achieved a moderate recall success rate of 64%. Both of these methods achieved a statistically significant higher recall rate than the control condition (48%). The training interfaces for both of the methods were no longer than three minutes, and the median login times were 9 seconds and 6 seconds, respectively. These results suggest that the *method of loci* could be effective

USEC '17, 26 February 2017, San Diego, CA, USA

http://dx.doi.org/10.14722/usec.2017.23034

to help users memorize system-assigned random passwords in a reasonable period of time.

We carefully analyzed the mistakes made by the participants in this study and considered their feedbacks to further improve and extend the *method of loci* to help users memorize long system-assigned random passwords that offer 56 bits of entropy (random passwords with twelve lowercase letters). Although the spaced repetition technique has been demonstrated to be quite effective in this regard [10], it involves dozens of sessions of user training. We leveraged the *method of loci* to develop an extended training interface that would help users memorize a 56-bit password in just one session.

We conducted a second memorability study to test the effectiveness of our extended training interface. We found that 21 out of 26 participants (81%) successfully recalled the 56-bit password with the help of a password hint after just one session of training (the median training duration was 736 seconds). When the spaced repetition technique was used to achieve the same goal, 46 out of 56 participants (82%) succeeded in recalling the 56-bit password, but it required them logging into a system 90 times over up to 15 days [10]. We thus believe that in regard to feasibility, the *method of loci* offers a more viable alternative to the spaced repetition technique to help users memorize a cryptographically-strong secret.

II. Prior Work and Constraints

In this section, we first give a brief overview of the studies that have been conducted to assess various aspects of user-chosen and system-assigned password schemes. The results of these studies demonstrate that user-chosen password schemes are fraught with security problems, while system-assigned password schemes are prone to memorability issues. We then examine the constraints and goals on our proposed approach based on prior findings.

A. User-chosen Passwords

Study results have verified that when users are given the freedom of choosing their own passwords, they create weak passwords that are easy to remember and contain predictable patterns [1], [57], [8]. This, in turn, makes the passwords vulnerable to dictionary attacks. Although strict password composition policies prevent users from creating weak passwords, these policies might lead to user frustration at times without providing significant security benefits [47], [30]. Shay et al. confirm that a strict password composition policy has an adverse effect on memorability [47]

User-chosen passwords also allow users to reuse the same password for multiple sites, which eventually leads to a "domino effect" of password reuse [27]. Das et al. reported that 43% of users use the identical password for multiple sites [14], while Haque et al. found that users frequently reuse their important banking or email passwords, with little or no modifications, to create their passwords for less important accounts such as online news or weather sites [21].

B. System-assigned Random Passwords

System-assigned random passwords guard against the attacks and the usability issues described above. Since users have no input to the process of selecting the password, the effective guessing space is equal to the theoretical entropy, which can be set to the desired level of security. Multiple studies, however, report poor memorability for system-assigned random passwords, even when natural-language words are used [46], [53].

C. Constraints and Objectives

We now describe the constraints and objectives that define the design requirements of our system. In a system-assigned random password scheme, the system generates a sequence of random characters to be used as a password. The total number of characters depends on the desired entropy of the random password.

Entropy. We calculate entropy[1] by using the formula entropy $H = L \times \log_2 N$, an approximation of plain Shannon entropy [45], where L is the length of the password and N is the size of the alphabet. Although a larger N could be obtained by including digits, special characters, and/or uppercase letters, we consider lowercase letters only. This makes it easier to design our automatic training interfaces without risking confusion between symbols, plus it ensures that passwords are easy to enter on mobile devices [23], [22].

As we fix the size of the domain for N to 26 (lowercase letters only), we obtain the value of L by selecting our desired entropy level. With $L = 6$ letters, we get 28 bits of entropy, which provides password-level security [7] and has been used in prior studies on system-assigned random passwords [53]. To get cryptographic-strength security [10], using $L = 12$ gives us 56 bits of entropy.

Time. We note that unlike logging in, registering an account is a one-time activity. Our training methods are used once during the registration period only, not during logging in. While long registration tasks would likely hamper adoption by typical websites, single-sign-on systems in work environments and financial service sites (e.g. where a user may already have a real account) are systems with strong security needs and the leverage to require more time and effort at registration. Still, the training activity should not be so long as to unduly annoy users. We select 180 seconds (3 minutes) as the maximum duration of the training activity for password-level security (28 bits). All of the participants in our pilot study (N=8) expressed their satisfaction with this time duration and reported that they would be willing to spend this amount of time for memorizing a password for one of their important accounts. We allow a significantly longer period of up to 15 minutes for learning the passwords with cryptographic-level security (56 bits). Given that this compares with the spaced repetition approach, which requires dozens of sessions before the password can be used reliably [10], [44], we think that this is a reasonable amount of time at registration.

Automation. We do not attempt to involve the users in doing something on their own to facilitate the memorization process, such as imagining images to map to letters on their own or creating their own stories. Davis et al. found that users largely ignored their suggestion to construct a story to help memorize

[1] Although the term entropy has been rightly criticized when used to discuss user-generated passwords [51], it serves as an effective shorthand for guessing space in system-assigned passwords.

a graphical password [15]. Rather, we plan to generate the training content automatically based on the assigned random passwords. In this way, we seek to aid the users as much as possible, limiting their mental effort to following through with the memorization process being given to them.

Several researchers have examined ways to increase the memorability of system-assigned random passwords. Huh et al. propose a scheme called "Surpass" [26], which allows users to replace few characters in a random password to make it more memorable. They conducted a large-scale online study to evaluate different Surpass policies and confirmed that with the increase of number of allowed character replacement, the memorability improves. However, allowing users to replace letters in a password might result in predictable weak passwords.

Blocki et al. use a variant of the *Person-Action-Object* (PAO) method in the context of password memorization [9], which requires the users imagining something on their own (for example, a story in which a selected person would perform a randomly selected action-object pair in a given scene). Our scheme is different in three major ways. First, we do not require the participants to imagine anything on their own. The PAO method, as implemented by them, requires them imagining a story. Second, their scheme shows the images of the person and the scene as cues during authentication, and these need to be added to the login interface. For our scheme, authentication can be done using typical existing password interfaces, including in an ssh session, with little to no changes. Finally, unlike their scheme, we do not leverage spaced repetition since our focus is to help users memorize a random password in a single training session.

III. Memory Techniques

We extensively reviewed the literature on memorization techniques to identify techniques with greatest potential for helping users memorize system-assigned random passwords. Specifically, the requirements defined in the previous section helped us to narrow down the list of potential techniques.

A good number of techniques focus on memorizing digits, such as the *phonetic system* and *phonetic recoding* [16]. We excluded them, since we focus on memorizing letters. Other popular methods like *peg* or *hook* systems require users to first learn a series of memory pegs [38], which is not compatible with our time and automation requirements. All such techniques that require learning something in advance were excluded. Some techniques were excluded since they are not very effective, such as the *imagery method* [43].

After this filtering step, we pinpointed two potential techniques that are compatible with our requirements: the ancient *method of loci*, and the *link* or *story* method.

A. The Science Behind the Proposed Techniques

As proposed by Atkinson and Shiffrin, any new information first enters the sensory registers, where it retains for a very brief period of time, before eventually getting decayed and lost [5]. The short-term memory, which also acts as the human working memory, receives selected inputs from the sensory register. Information transfer from short-term memory to long-term memory depends upon further processing and encoding.

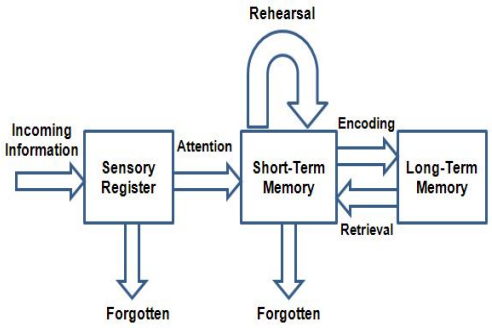

Fig. 1: Atkinson-Shiffrin Memory Model

In this regard, if the information could be associated with something meaningful, the encoding process would be more elaborative. The memorization techniques assist for elaborative encoding by providing meaningful cues. Tulving theorizes that memories are not truly lost or forgotten; forgetting something essentially means that the necessary cues needed to retrieve them are unavailable [50]. Thus, cues are considered to be fundamental source of information during a retrieval process.

B. The Method of Loci or the Memory Palace Method

The *method of loci* (also known as the *memory palace* or *mind palace* technique) is one of the oldest mnemonic techniques, and it has been used extensively to facilitate memory recall [55]. The method has also been broadly used in memory research [41], [6], [56]. Li et al. even proposed a graphical password scheme that was inspired by the *method of loci* [32].

For using this technique, one first needs to identify a few landmarks (also known as *loci*) in some familiar place, such as her home or office building. When needing to remember a set of items, she mentally walks through these landmarks and associates each item with a particular landmark. This association can be made by forming a vivid visual image of the item and placing it on the landmark. For recalling the items later, she re-imagines walking through the landmarks, and retrieving the items in order[2].

This technique leverages spatial memory, the part of memory that helps in recording information about one's surrounding environment and the associated spatial orientation [11]. More specifically, using this technique activates portions of the brain that are concerned with spatial awareness, such as the medial parietal cortex and the retrospenial cortex [34], [39]. Both of these regions play an important role in enhancing spatial learning abilities. The *method of loci* also activates the right

[2]The utilization of this method has been exemplified in TV series "Sherlock", a BBC-produced crime drama series that portrays a contemporary adaptation of Sir Arthur Conan Doyle's famous Sherlock Holmes detective stories [17]. During an episode in Season 3, titled "His Last Vow" [35], Sherlock can be seen using his *mind palace* for discovering the best path to survival. Although Sherlock's *mind palace* does not resemble the typical type of storage place for the *method of loci*, it gives an idea of organizing information in a certain way to facilitate the information retrieval from memory.

posterior hippocampus [34], [39], an important component of the brain that assists in finding one's way around an environment and remembering the associated events which occur within it [11].

Research results have revealed that memory champions do not necessarily have extraordinary brains; rather they use their normal spatial abilities to great effect [40], [34]. This makes us think that regular users can also take advantage of these abilities, if they have guidance to facilitate quick adoption of the *method of loci* via our training interfaces.

C. The Link (or Story) Method

The *Link method* is another mnemonic technique that is simple to use and requires no materials to learn in advance [33]. The basic concept of the *link* or *story* method has been applied in a graphical password scheme called Story [15], but has not been automated for the user in prior work.

Applying the *link method* involves converting each item to be remembered into a pictorial representation and creating a link or association between each successive pair of representations in a vivid way. This, in turn, creates a chain of interacting images (items) where the first image acts as the cue to recall the second one, the second image acts as the cue to recall the third one, and so on.

Morris and Stevens found that, while subjects asked to form images of objects did no better at recall than uninstructed control subjects, subjects who were told to link the images together had significantly better recall performance [36]. Research results have shown that such linking of images of items together improves recall performance relative to forming images of each item individually [36]. In fact, subjects that simply formed images of the items individually performed no better than uninstructed control subjects in recalling the items. This highlights that imagery instructions work best when they are linked together to form a sort of story. Since this linking of images ultimately lead to a cohesive story, the technique is also known as the *story method*.

IV. System Design

Our system has two parts: registration and login. During registration, we first assign each user a random password consisting of six lowercase letters. Next, we dynamically generate a video clip based on the assigned letters and show the clip to the user. The video clip employs either the *method of loci* or the *link method*, which assists the user in memorization. Once the clip ends, the user is asked to type the password to complete the registration. During login, users just recall and type the correct password to authenticate, just as they do in any recall-based textual password scheme.

This simple and straightforward recall-based authentication scheme has two major advantages. First, it avoids a longer login time, which is a major usability issue for any recognition-based authentication scheme [4]. The second major advantage is that it makes the deployment procedure very simple; nothing extra needs to be done during the login period.

Our work also differs from the related works in cognitive psychology in a major way [36], [43], [31]. We do not require the users to do anything on their own, such as imagining some pictures of their own preferences or creating their own stories for facilitating the memorization process. This essentially removes the susceptibility associated with any kind of poor user action or selection.

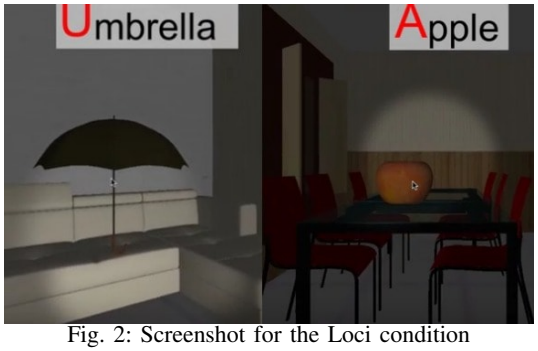

Fig. 2: Screenshot for the Loci condition

We now give a detailed description of our video clips for the *method of loci* and the *link method*.

A. Method of Loci

Legge et al. show that navigating a virtual environment is as effective as a familiar environment for *the method of loci* [31], and we thus generate a virtual environment. This environment was modeled after an apartment consisting of a living room, a kitchen, a dining room, a bedroom, and a bathroom. These five rooms, along with a mailbox at the entrance of the apartment, serve as the six loci. We then selected 26 distinct objects to pictorially represent the 26 letters (apple for 'a', ball for 'b', and so on). Depending on the generated random password, six of these 26 objects would appear at the six loci of our virtual apartment.

The video navigates through these rooms in a fixed order once with just arrows pointing to the loci and twice with the objects in those locations. To help a viewer to better recognize the objects, the camera zooms in whenever an object is shown. The navigation pauses for a few seconds and the object name appears on top, with the first letter highlighted. The entire duration of the video clip, including these pauses, is 160 seconds.

For example, if the randomly generated password is 'pcgbhr', then the video clip would show a pencil (for 'p', the first letter of the password) above the mail box at the entrance, a cat (for 'c') above a sofa at the living room, a guitar beside the sink in the kitchen, a ball above the dining table, a helicopter above the bed in the bedroom, and a rocket inside the washroom cabinet.

At first, the video clip would show the layout of the virtual apartment, with arrows instead of objects in the specified loci. This is meant to familiarize a viewer with the apartment and show her the order of different loci in the layout, starting from the mail box at the entrance and ending at the bathroom cabinet. Once this is done, the camera would return to the mail box at the entrance and navigation would re-start. This time, the objects would appear in the specified loci. The apartment with the objects would be repeated one more time, making for a total of three navigations of the entire apartment (one without and two with the objects).

B. Link Method

As with the training interface for the *method of loci*, this method also involves showing a video clip to the users. In this case, we show a small story that would be associated with the six letters of the randomly assigned password.

For this method also, we used 26 distinct objects to represent 26 different letters. In addition, for the sake of creating an interesting story, we used 26 different animals for representing the last two letters of the password.

Suppose that the randomly generated password is 'pcgbhr'. The story begins with a magician performing in front of an audience. The magician starts with a pencil (for 'p', the first letter of the password) and magically transforms it into a cat (for 'c'). The pencil acts as a cue for remembering the cat, since the former object would be transformed into the latter one. The magic act evolves to incorporate the other objects, ending with a boy being saved from a scary horse (for 'h') by a giant rabbit (for 'r').

The video is accompanied by captions describing the sequence of the incidents. As with the *method of loci*, the camera zooms in and the navigation pauses whenever the objects are shown. The entire duration of the clip is 180 seconds for this method. We note that the basic organization of the story remains the same for each password, where only the objects and animals would change to match the assigned letters.

C. Pilot Study

We conducted a pilot study with eight participants to primarily evaluate the effectiveness of our video clips. Their feedbacks helped us to finalize certain design issues such as the amount of light inside the virtual apartment, the duration of zooming and pausing, the size and placement of the captions/texts etc. For both of the methods, seven out of the eight participants were able to recall the memorized password after a week.

D. Development Platform and Tools

To develop our virtual apartment model and use it in custom way, we used two software packages: Max3D and Unity3D. First we developed the apartment model by using Max3D. The 3D objects representing the password letters were also modeled by using Max3D. We imported the resulting model file into Unity3D game engine, which we used to implement the camera navigation, create wall textures, and set up point light sources to make the objects clearly visible inside the apartment.

For showing the story of the magician, we basically used a series of image frames. These frames were designed by using Adobe Photoshop CS5. Later we merged all these frames by using Unity3D.

For both of the video clips, we dynamically placed different objects in different locations/frames, depending on the letters of the randomly assigned password. This logic was implemented by writing scripts in C Sharp.

V. Study 1

We used a within-subjects design consisting of three study conditions: Loci, Link, and Control. The study procedures were approved by the local Institutional Review Board (IRB) for human subjects research.

A. Participants, Apparatus and Environment

For this study, we recruited 52 students (34 women, 18 men). Participants came from diverse majors, including majors from Psychology, Business, Nursing, Biology, and Music. The age of the participants varied between 18 to 31 with a mean age of 20. Each participant was compensated with course credit for participation and was aware that her performance or feedback in this study would not affect the amount of compensation.

For assessing the effectiveness of our training methods and performing a better comparison, we administered a control condition in which participants were asked to memorize their system-assigned random textual password in any way they preferred. The guessing space for this condition was also 28 bits and the time limit for memorizing the password was 180 seconds (consistent with the other two methods).

We created three realistic and distinct websites using the images and layouts from familiar commercial sites, where each of them was equipped with one of our three password schemes: Loci, Link, and Control.

B. Procedure

Our experiment consisted of two sessions. To test users' memorization of the assigned passwords, the second session took place one week after the first one. This one-week delay is larger than the maximum average interval for a user between subsequent logins to any of her important accounts [24] and is also a common interval used in authentication studies (e.g., [37], [53], [18], [3], [4]).

1) Session 1: Participants were given an overview of our study after signing a consent form. Then they performed registration for each of the three sites, each outfitted with a distinct scheme. We described the registration process for the *method of loci* and the *link method* in the previous section. After registering with each scheme, participants performed a practice login with that scheme for which we did not collect data. During registration, the sites were shown to the participants in random order to compensate for ordering effects. They were asked to not write down the assigned passwords.

2) Session 2: After a week, when the participants returned for the second session, they were asked to log into each of the three sites using the assigned passwords. The sites were shown to the participants in random order. They were allowed to make a maximum of three attempts for a successful login. After they had finished, we conducted an anonymous paper-based survey. Participants were then compensated and thanked for their time.

C. Ecological Validity

Our participants came from diverse majors. They were young and educated, which represents a large number of frequent Web users, but may not generalize to the entire

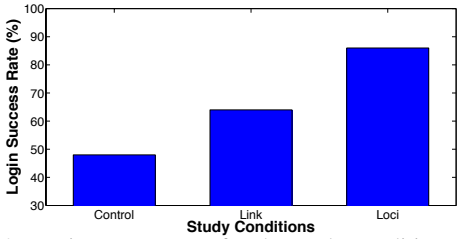

Fig. 3: Login success rate for the study conditions (n=44)

population. We were only able to gather data from 52 participants since the study was performed in a lab setting. However, lab studies have been preferred to examine password memorability [19]. Moreover, since lab studies are conducted in a controlled experimental setting, it helps to better assess the initial prototype of an authentication scheme by observing the participants and collecting their feedback. We believe that 52 provides a suitable sample size for a lab study as compared to the prior studies on password memorability [49], [12], [13], [2], [52], [3], [4].

D. Results

We evaluated our study conditions via metrics suggested in the literature: memorability, registration time, number of attempts, and login time. Since eight of the participants did not show up for the second session, we exclude their data and present results for 44 participants.

We use statistical tests to analyze our results, where the results comparing two conditions are considered to be significantly different when we find $p < 0.05$. When comparing two study conditions where the variable is at least ordinal, we use either a Wilcoxon signed-rank test (for matched pairs of subjects) or 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, so we use a McNemar's test for matched pairs of subjects and a chi-squared test for unpaired results to compare login success rates between two conditions.

1) Memorability: Our results show that out of 44 participants, 38 (86%) succeeded to log in using Loci method, while 28 participants (64%) and 21 participants (48%), respectively, logged in successfully with the Link method and the Control condition. We compare login success rates between our study conditions using McNemar's test. Our analysis shows that the login success rates for Loci method, $\chi^2(1, N = 44) = 13.47$, $p < 0.01$, and Link method, $\chi^2(1, N = 44) = 2.77$, $p < 0.05$, were significantly higher than that for the Control condition. We also found that the Loci method had a significantly higher login success rate in comparison to the Link method, $\chi^2(1, N = 44) = 5.79$, $p < 0.05$.

For the Control condition, participants were given the opportunity to memorize the password in their own way. We observed that most of them tried to follow a basic repetition technique. In the Loci and Link methods, however, some of this cognitive effort was reduced. The letters were all mapped to objects, e.g. "apple" for 'a', making memorization more visual and concrete. Further, the training aids in our system offered users a ready-made mnemonic.

The Loci method also had a significantly higher recall rate than the Link method. This result is consistent with the experimental results of a prior study that was conducted to assess the effectiveness of these methods in the context of memorizing a list of words [43].

At the end of second session, we asked participants to answer 5-point Likert-scale questions (1: *strong disagreement*, 5: *strong agreement*) regarding the efficacy of the Loci and Link methods in providing satisfactory memorability (e.g., "The passwords were easier to remember because of watching the clip."). The results for Wilcoxon signed-rank test (appropriate for matched pairs of subjects) show that user feedback was significantly better for the Loci method (Median: 4, Mode: 5) as compared to the Link method (Median: 3, Mode: 2) ($V = 398$, $p < 0.05$) [3].

We explicitly asked the participants at the end of the first session to not write down their assigned passwords. At the end of the second session we asked them about it, where we reversed this question (e.g., "I would need to write down the password to better remember it, even after seeing the clip") to avoid bias. The scores were reversed before calculating the modes and medians, so that a higher score always indicates a more positive result for a scheme. We found significantly better user feedback for the Loci method (Median: 4, Mode: 5) compared to the Link method (Median: 4, Mode: 4) in terms of the need to write down passwords for memorability ($V = 182$, $p < 0.05$).

2) Registration Time: The registration time was constant for the Loci (160 seconds) and Link methods (180 seconds). For performing a fair comparison, we allowed the participants to spend the same amount of time (180 seconds) in the Control condition to memorize their passwords.

At the end of second session, we asked for the perception of participants on the registration time of Loci and Link methods through a 5-point Likert scale question (e.g., "The time spent for learning the password was worth it"). We found significantly better user feedback for the Loci method (Median: 4, Mode: 5) compared to the Link method (Median: 3, Mode: 2) in terms of registration time, i.e., the time for learning a system-assigned password ($V = 224$, $p < 0.05$).

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. Thus, we use a Wilcoxon-Mann-Whitney test (appropriate for unpaired results) to evaluate two schemes in terms of number of attempts and the time for successful logins.

The mean number of attempts for a successful login was less than two for each of the three study conditions, while the median was one in each case. 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: Link-Control ($W = 312$, $p = 0.88$),

[3] Since Likert scale data are ordinal, it is most appropriate to calculate mode and median for Likert-scale responses [42].

Loci-Control ($W = 434$, $p = 0.58$), and Loci-Link ($W = 544$, $p = 0.72$).

3) Login Time: The median login times for the Control, Link, and Loci conditions were 5, 6 and 9 seconds, respectively. The results for Wilcoxon-Mann-Whitney tests show that the login time for the Control condition was significantly less than that for the Loci method ($W = 180.5$, $p < 0.05$) and the Link method ($W = 218.5$, $p < 0.05$). We did not find a significant difference in login time between the Loci and Link conditions ($W = 695.5$, $p = 0.26$).

For the Loci and Link methods, participants were required to recall the series of events that took place in the video clips. They were also required to recall the objects representing the password letters. Thus, the login times were slightly longer. However, compared to the login time of other recognition-based schemes [4], [2], the additional time was nominal.

4) An Insight into the Results of Participants Who Failed to Log In: We analyzed the mistakes made by the participants who failed to log in successfully and carefully reviewed their feedback and suggestions to improve our training interfaces. Since the Loci method yielded a statistically significant higher recall success rate, we exclusively focused on this method to further improve it.

We observed that three out of the six participants who could not log in successfully failed to recall just one object. One of them provided a very interesting feedback and commented that some kind of password hint would have helped to recall the missing object which prompted us to think about a password hint for the Loci condition. We figured out that navigating the empty apartment and highlighting the loci without the objects (same as the first round of navigation during the training session) might provide a helpful hint to recall the missing letters/objects.

VI. Study 2

Based on theoretical password space, Biddle et al. classified passwords into three categories in terms of the offered security level: i) PIN-level security: less than 20 bits of entropy, ii) Password-level security: 20 to 60 bits of entropy, iii) Crypto-level security: above 60 bits of entropy [7]. Passwords offering crypto-level security are regarded as cryptographically-strong passwords, which have applications in systems with high security requirements, including enterprise account login, master password for password managers, and password for protecting private keys in cryptography. In a separate work [10], Bonneau et al. considered a 56-bit password to be cryptographically strong.

Since the results of Study 1 showed promise for the *method of loci* in offering password-level security, it seems reasonable to examine its efficacy for providing crypto-level security. We thus decided to leverage the *method of loci* to design an extended training interface that would help users to remember longer system-assigned passwords. In this extended version, we incorporated the password hint during login to assist users in recalling their password. To keep consistency with the study of Bonneau et al. [10], our scheme offers 56 bits of entropy, requiring users to remember twelve lowercase letters as their authentication secret.

While conventional wisdom suggests that users are not capable of remembering cryptographically-strong secrets [29], Bonneau et al. [10] challenged this notion through their study on 56-bit passwords, where they leveraged spaced repetition to aid password memorization [10]. In this study [10], each participant was assigned a random 56-bit password, which was represented as three chunks of four lowercase letters. For memorizing this password, a participant had to log into a website 90 times over a period of up to 15 days, where the first chunk was displayed directly during the first login. For each subsequent login, a 1/3 second delay was added before displaying a chunk, to encourage participants to type that chunk from memory. Once the participant was able to enter the first chunk before it was displayed, the same procedure was followed for the subsequent chunks. Three days after the last login, participants were asked to recall the password from their memory, and 82% of participants succeeded.

The study of Bonneau et al. showed promise in terms of memorability [10]. However, the time duration for learning a 56-bit password was quite long, and the requirement of logging into a website 90 times over two weeks does not reflect many real-life time constraints, even for learning an important authentication secret. For example, if users need 56-bit passwords to access a secure system, how do they successfully access the system their first day? In our study, we examined the efficacy of *method of loci* to achieve the same goal within a substantially shorter time period. In particular, our goal is to leverage the *method of loci* to help users memorize a 56-bit authentication secret in just a single registration session.

A. Extended Training Interface

In our first study, we used a virtual apartment model for the *method of loci*, consisting of a mail box, a living room, a kitchen, a dining room, a bedroom, and a bathroom. For our study on 56-bit passwords, we added an additional model of a virtual office consisting of six additional loci: a reception room, a file cabinet room, a copier room, a room of cubicles, a recreation room, and a conference room.

As cryptographically-strong passwords are used for high-value applications, users have much incentive to spend more time in memorizing these passwords. We, therefore, relaxed the time constraint for password memorization in this study, where the objects were displayed at the specified loci for a much longer period of time. The duration of the entire video clip for this study was 480 seconds (8 minutes).

B. Participants

We recruited 26 participants (21 men, 5 women) for this study, all college students with majors, including Engineering, Psychology, Pharmacy, Chemistry, Biology, and Management. The age of participants varied between 19 to 41 with a mean age of 24. Each participant was compensated with a restaurant gift voucher ($10). The study was approved by the local Institutional Review Board (IRB) for human subjects research.

C. Procedure

1) Session 1: In the first session, participants were given an overview of our study after they had signed the consent form. Then they were assigned a random password consisting

of twelve lowercase letters and shown the video clip, which was generated based on that password. Once the clip ended, they were asked to sequentially write down the name of those twelve objects shown in the clip. If they had forgot or missed the order of any object, the portion of video clip displaying that object was shown again. Finally, they were displayed the twelve objects in the specified loci for one last time.

After learning the password, participants logged into a site (we designed this site by using the images and layouts of a familiar commercial site) using the assigned password. We did not collect data for these practice trials. We explicitly asked them not to write down the password.

2) Session 2: Participants returned for the second session one week after the first session. We asked them to log into the site using the assigned password, where they were allowed to make a maximum of three attempts for a successful login. Participants who had failed to correctly recall the password within three attempts were provided a password hint, in which we showed them a video clip that navigated through the twelve loci without displaying any object. Thereafter, they were given another chance to recall the password and log in successfully.

After they had finished, we conducted an anonymous paper-based survey. They were then compensated and thanked for their time.

D. Results

Our results show that 15 (58%) out of 26 participants logged in successfully by correctly recalling the password within three attempts, where the median login time was 28 seconds. Of the remaining eleven participants, six were able to log in successfully after watching the password hint, and the median login time for these participants was 171 seconds (2 minutes and 51 seconds), including the duration of the password hint clip (90 seconds). Thus, incorporating the password hint contributes to increase the login success rate of the scheme from 58% to 81%.

The median registration time for the scheme was 736 seconds (12 minutes and 16 seconds), including the 480 seconds (8 minutes) duration of the extended training clip. This essentially means that the total training time for our scheme is similar to that of Bonneau et al. [10]. While our scheme requires a single long training session, their scheme involves dozens of training sessions of small durations.

We analyzed the survey responses of the five participants who had failed to correctly recall their password even after watching the password hint clip. We found that one of them who had just missed the last letter of the assigned password, liked our idea to aid password memorization and expressed confidence to log in successfully in future attempts. Two other participants felt that the clip would be more helpful if the displayed objects were more meaningful to them or pertinent to their interests. The other two participants claimed that their learning style is not visual, and thus, it would not be possible for them to memorize new information just by watching a video clip.

VII. Discussion

To the best of our knowledge, this is the first study to date that applies the *method of loci* to help users memorize a system-assigned textual password. Although both of the methods (*loci* and *link*) have been used before in other domains, the current study is the first of its kind to implement a training interface which does not require the users to do anything unaided, such as imagining some pictures of their own preferences or creating their own stories, to facilitate the memorization process. As a result, it is not susceptible to any kind of poor user action or selection.

Since our training method involves watching a video clip only, it is very simple to follow. We also offer sufficient password-level strength, the duration of our training method is reasonable, and no overhead is associated with designing the login interface. In addition, our scheme does not require the users to type any uppercase letters, digits, or special characters, and thus, it offers a potential solution to the usability issue associated with entering a textual password with multiple character-types on mobile devices [28]. Prior works have demonstrated the inconvenience of capitalizing letters and inserting digits or special characters when entering a password on a mobile device [22], [23]. We therefore would like to implement and test our lowercase letter-only scheme on mobile devices in future.

Our experimental results showed that both of our proposed methods outperformed the control condition with regard to login success rate. In fact, the *method of loci* had a login success rate of 86%, which is very high for any recall-based memorability study with system-assigned random passwords. Furthermore, the median login time was just 9 seconds for the method of loci.

With such encouraging results, we plan to further improve the training interface for the *method of loci* based on the feedback from our participants, which include showing meaningful objects pertinent to individual interests, and adding animations when displaying the objects. Since password hints have been demonstrated to be useful in our second study, in future work, we will examine the effectiveness of various types of password hints incorporated with the *method of loci*. We will also conduct a multiple-password study to observe the effect of memory interference on the *method of loci*.

We believe that the implications of our study with cryptographically-strong passwords are profound. In general, security researchers have been skeptic about the capability of human brain to remember cryptographically-strong secrets [29]. Bonneau et al. took an attempt to solve this problem and succeeded by leveraging the spaced repetition technique, which involved dozens of sessions of user training [10]. We further contributed in this direction and demonstrated that the same goal can be achieved in a single registration session with the *method of loci*. This suggests that the capability of human brain should not be undermined and future researchers should focus on utilizing its highest potential by leveraging the memorization techniques from cognitive psychology.

References

[1] A. Adams and M. A. Sasse, "Users are not the enemy," *Commun. ACM*, vol. 42, no. 12, pp. 40–46, 1999.

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

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

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

[5] R. C. Atkinson and R. M. Shiffrin, "Human memory: A proposed system and its control processes," in *The Psychology of Learning and Motivation*, K. W. Spence and J. T. Spence, Eds. New York: Acedemic Press, 1968.

[6] P. B. Baltes and U. Lindenberger, "On the range of cognitive plasticity in old age as a function of experience: 15 years of intervention research," *Behavior Therapy*, vol. 19, pp. 283–300, 1988.

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

[8] M. Bishop and D. V. Klein, "Improving system security via proactive password checking," *Computers & Security*, vol. 14, no. 3, pp. 233–249, 1995.

[9] J. Blocki, S. Komanduri, L. Cranor, and A. Datta, "Spaced repetition and mnemonics enable recall of multiple strong passwords," in *NDSS*, 2015.

[10] J. Bonneau and S. Schechter, "Towards reliable storage of 56-bit secrets in human memory," in *USENIX*, 2014.

[11] N. Burgess, E. A. Maguire, and J. O'Keefe, "The human hippocampus and spatial and episodic memory," *Neuron*, vol. 35, no. 4, pp. 625–641, 2002.

[12] 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*, vol. 9, 2012.

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

[14] A. Das, J. Bonneau, M. Caesar, N. Borisov, and X. Wang, "The tangled web of password reuse," in *NDSS*, 2014.

[15] D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes," in *USENIX*, 2004.

[16] M. J. Dickel, "Principles of encoding mnemonics," *Perceptual and motor skills*, vol. 57, pp. 111–118, 1983.

[17] A. C. Doyle, *The Complete Sherlock Holmes*. New York City: Barnes & Noble, 2009.

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

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

[20] D. Florêncio and C. Herley, "A large-scale study of web password habits," in *WWW*, 2007.

[21] S. M. T. Haque, M. Wright, and S. Scielzo, "Hierarchy of users' web passwords: Perceptions, practices, and susceptibilities," *International Journal of Human-Computer Studies*, vol. 72, no. 12, pp. 860–874, 2014.

[22] S. M. T. Haque, S. Scielzo, and M. Wright, "Applying psychometrics to measure user comfort when constructing a strong password," in *SOUPS*, 2014.

[23] S. M. T. Haque, M. Wright, and S. Scielzo, "Passwords and interfaces: Towards creating stronger passwords by using mobile phone handsets," in *SPSM*, 2013.

[24] E. Hayashi and J. I. Hong, "A diary study of password usage in daily life," in *Proceedings of the 2011 annual conference on Human factors in computing systems*, May 2011, pp. 2627–2630.

[25] C. Herley, P. C. Oorschot, and A. S. Patrick, "Passwords: If we're so smart, why are we still using them?" in *FC*, 2009.

[26] J. H. Huh, S. Oh, H. Kim, and K. Beznosov, "Surpass:system-initiated user-replaceable passwords," in *ACM CCS*, 2015.

[27] B. Ives, K. R. Walsh, and H. Schneider, "The domino effect of password reuse," *Commun. ACM*, vol. 47, no. 4, pp. 75–78, 2004.

[28] M. Jakobsson, E. Shi, P. Golle, and R. Chow., "Implicit authentication for mobile devices," in *HotSec*, 2009.

[29] C. Kaufman, R. Perlman, and M. Speciner, *Network security: Private communication in a public world*. New Jersey: Prentice Hall Press, 2002.

[30] S. Komanduri, R. Shay, P. G. Kelley, M. L. Mazurek, L. Bauer, N. Christin, L. F. Cranor, and S. Egelman, "Of passwords and people: Measuring the effect of password-composition policies," in *CHI*, 2011.

[31] E. L. G. Legge, C. R. Madan, E. T. Ng, and J. B. Caplan, "Building a memory palace in minutes: Equivalent memory performance using virtual versus conventional environments with the Method of Loci," *Acta Psychologica*, vol. 141, pp. 380–390, 2012.

[32] Z. Li, Q. Sun, Y. Lian, and D. D. Giusto, "An association-based graphical password design resistant to shoulder-surfing attack," in *ICME*, 2005.

[33] H. Lorayne and J. Lucas, *The memory book*. New York: Stein and Day, 1974.

[34] E. A. Maguire, E. R. Valentine, J. M. Wilding, and N. Kapur, "Routes to remembering: The brains behind superior memory," *Nature Neuroscience*, vol. 6, no. 1, pp. 90–95, 2003.

[35] S. Moffat and N. Hurran, *Sherlock*. BBC One, 2014.

[36] P. E. Morris and R. Stevens, "Linking images and free recall," *Journal of Verbal Learning and Verbal Behavior*, vol. 13, no. 3, pp. 310–315, 1974.

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

[38] A. Paivio, *Imagery and verbal processes*. New York: Holt, Rinehart and Winston, 1971.

[39] R. Parasuraman and M. Rizzo, *Neuroergonomics: The brain at work*. New York: Oxford University Press, 2008.

[40] A. Raz, M. G. Packard, G. M. Alexander, J. T. Buhle, H. Zhu, S. Yu, and B. S. Peterson, "A slice of pi : An exploratory neuroimaging study of digit encoding and retrieval in a superior memorist," *Neurocase*, vol. 15, no. 5, pp. 361–372, 2009.

[41] J. T. E. Richardson, "The efficacy of imagery mnemonics in memory remediation," *Neuropsychologia*, vol. 33, pp. 1345–1357, 1995.

[42] J. Robertson, "Stats: We're doing it wrong," http://cacm.acm.org/blogs/blog-cacm/107125-stats-were-doing-it-wrong/fulltext, April 2011.

[43] H. L. Roediger, "The effectiveness of four mnemonics in ordering recall," *Journal of Experimental Psychology: Human Learning and Memory*, vol. 6, no. 5, pp. 558–567, 1980.

[44] S. Schechter and J. Bonneau, "Learning assigned secrets for unlocking mobile devices," in *SOUPS*, 2015.

[45] C. E. Shannon, "A mathematical theory of communication," *Bell System Technical Journal*, vol. 27, pp. 379–423, 623–656, 1948.

[46] 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.

[47] 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.

[48] J. M. Stanton, K. R. Stam, P. Mastrangelo, and J. Jolton, "Analysis of end user security behaviors," *Computers & Security*, vol. 24, no. 2, pp. 124–133, 2005.

[49] J. Thorpe, B. MacRae, and A. Salehi-Abari, "Usability and security evaluation of geopass: A geographic location-password scheme," in *SOUPS*, 2013.

[50] E. Tulving, "Cue-dependent forgetting: When we forget something we once knew, it does not necessarily mean that the memory trace has been lost; it may only be inaccessible," *American Scientist*, vol. 62, no. 1, pp. 74–82, 1974.

[51] M. Weir, S. Aggarwal, M. Collins, and H. Stern, "Testing metrics for password creation policies by attacking large sets of revealed passwords," in *Proceedings of the 17th ACM Conference on Computer and Communications Security (CCS)*, 2010.

[52] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Effects of tolerance and image choice," in *SOUPS*, 2005.

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

[54] J. Yan, A. Blackwell, R. Anderson, and A. Grant, "Password memorability and security: Empirical results," *IEEE Security & Privacy*, vol. 2, no. 5, pp. 25–31, 2004.

[55] F. A. Yates, *The art of memory*. Chicago: University of Chicago Press, 1966.

[56] J. A. Yesavage, "Imagery pretraining and memory training in the elderly," *Gerontology*, vol. 29, pp. 271–275, 1983.

[57] Y. Zhang, F. Monrose, and M. K. Reiter, "The security of modern password expiration: An algorithmic framework and empirical analysis," in *CCS*, 2010.

[58] M. Zviran and W. J. Haga, "A comparison of password techniques for multilevel authentication mechanisms," *The Computer Journal*, vol. 36, no. 3, pp. 227–237, 1993.