IMPROVING MEMORIZATION AND LONG TERM RECALL OF SYSTEM ASSIGNED PASSWORDS

By

JAYESH DOOLANI

Presented to the Faculty of the Graduate School of

The University of Texas at Arlington in Partial Fulfillment

of the Requirements

for the Degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

THE UNIVERSITY OF TEXAS AT ARLINGTON

DECEMBER 2016

To my family, friends and to my advisor, Dr. Matthew Wright, who guided me to where I am today.

ACKNOWLEDGEMENTS

I would like to thank my supervising professor Dr. Matthew Wright for his guidance, motivation and invaluable support throughout my graduate studies. He always guided me and gave constructive feedback about my work. It was a great learning experience for me under his guidance.

I am grateful to Dr. Filia Makedon and to Dr. John Robb for taking time to serve on my thesis committee. I would specially like to mention the key role Dr. Fillia Makedon's course on Human Computer Interaction played and was extremely beneficial for me in completing this thesis. I also want to thank Dr. Taiabul Haque for his key inputs and for providing great insights in this research area.

I am also grateful to Dr. Feraydune Kashefi of Computer Science department who helped us recruit his class students for our user study.

Last but not the least, I would like to express my deepest gratitude to my parents who encouraged and motivated me to pursue my MS. This research would not have been possible without their emotional support.

November 11, 2016

ABSTRACT

IMPROVING MEMORIZATION AND LONG TERM RECALL OF SYSTEM ASSIGNED PASSWORDS

Jayesh Doolani, M.S.

The University of Texas at Arlington, 2016

Supervising Professor: Matthew Wright

Systems assigned passwords have guaranteed robustness against guessing attacks, but they are hard to memorize. To make system assigned passwords more usable, it is of prime importance that systems that assign random passwords also assist users with memorization and recall. In this work, we have designed a novel technique that employs rote memorization in form of an engaging game, which is played during the account registration process. Based on prior work on chunking, we break a password into 3 equal chunks, and then the game helps plant those chunks in memory. We present the findings of 17-participant user study, where we explored the usability of 9 characters long pronounceable system assigned passwords. Results of the study indicate that our system was effective in training users to memorize the random password at an average registration time of 6 minutes, but the long-term recall rate of 71.4% did not match our expectation. On thorough evaluation of the system and the results, we identified potential areas of improvement and present a modified system design to improve the long-term recall rate.

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

CHAPTER 1

INTRODUCTION

Passwords are the most dominant form of authentication that exists in the wild. In spite of the hue and cry, by advocates of alternatives to passwords, that "passwords are dead", they still appear to be widely used in most systems and are here to stay for the foreseeable future [3]. The main factor for the popularity of passwords lies in its usability and ease of implementation by service providers. Users only need to recall a secret (password) or a particular sequence (gesture) from memory and do not require carrying anything physically with them. Passwords can be broadly classified into two categories: User-chosen (one where the password is constructed by the user) and System-assigned (one where the system assigns a password to the user). When given a choice between choosing your own password and choosing a system assigned one, users tend to choose the former as they can create passwords that have some meaning to her [1]. It is easier for the user to develop mental connections to the password she constructs, which helps her memorize it [2].

Despite their widespread use, the rampant use of insecure passwords still remains a major concern for system administrators, which is attributed to the irrational human behavior when it comes to constructing a secure password. Prior studies [15, 16, 17] have shown that traditional user-chosen passwords are inherently insecure since most users choose weak and easily guessed passwords and have been observed to construct passwords with predictable patterns [6, 14].

To overcome these shortcomings of user's mentality when constructing passwords, system administrators have adopted various password-composition policies, which prevent the user from constructing passwords that are too easy to crack [18]. A typical password-composition policy includes constructing a password that contains at least one uppercase letter, one digit and one special character. Unfortunately, these strict password-composition policies have sometimes lead to frustration and burden for the user [5], and users often follow predictable patterns to get around these policies and subvert the system. Previous research [4, 19] has also reported that such policies do not improve the security of passwords, rather they negatively affect their memorability.

One of the arguments put forward to make passwords more secure is to avoid giving users the choice to construct their own passwords and instead have the system assign them a randomly generated password (e.g. "lxcprjoj"). Such system-assigned passwords have guaranteed security and are extremely difficult to crack because of the random selection of characters. They have an innate defense against an *offline attack* (e.g. brute force attack), where an attacker tries all possible combinations with the hope of eventually guessing the correct password. In spite of these strengths of system-assigned passwords, they are considered less usable because of a major memorability issue, as memorizing a string of random characters is a challenging task that users are generally not trained for. Given the appropriate training to memorize random strings, system-assigned passwords can be made more usable.

To make system-assigned passwords more usable, we argue that systems that assign random passwords should also assist users in memorizing the password for long-term recall. Training users to memorize passwords during the registration process isn't a novel idea, previous research works [24] have adopted this approach to ease the memorability of passwords assigned by the system, but they either generate passwords of lower entropy or do not provide sufficient memorability.

This thesis addresses the memorability issue associated with system-assigned passwords. We propose novel techniques that leverage human's cognitive abilities to assist users in memorizing system-assigned passwords and be able to recall quickly in the future. We reviewed the literature of human memory and various memorization techniques and picked two effective techniques which have been proven to enhance memorability. One such technique is *rote memorization,* which involves repetitive rehearsal of information, so that it is retained in the short-term memory long enough. We then harness the effectiveness of the *chunking* technique to further help in encoding of the information which eventually helps in retaining the information in long-term memory. Since rote memorization is a boring task, we incorporated both these techniques in a simple ball and cup game, which is played during the registration process, which helps in making the learning process more pleasant.

To test the effectiveness of this system on pronounceable system-assigned passwords, we conducted a two phase in-lab user study with 17 participants. Our results showed that with recall rate of 71.4%, this technique was effective in

increasing the memorability of system-assigned password to a certain extent, it was not sufficient enough to guarantee better memorability than other schemes. With a mean registration time of 6 minutes and mean login time of 4.2 seconds, it shows that even with a long registration time, which is a onetime activity for each account, it is possible to achieve similar short login time as other text-based password schemes.

To further improve the memorability, we analyzed the results of our user study and found key areas for improvement in the proposed technique. We decided to provide more intense training to the user in order to improve the memorability. We propose a modified version of our technique, which uses the *method of loci* (also known as memory palace method) before the rote memorization and chunking technique. *Method of loci* uses the spatial and visual memory to assist in memorization. We expect our modified technique will have a higher registration time, but since this is a onetime activity, we believe users can leverage this technique to memorize cryptographically stronger passwords (56 bit or 12 character).

CHAPTER 2

RELATED WORK

Many researchers have identified the problems associated with choosing strong passwords. Despite the constant efforts to replace traditional text-based passwords, no other scheme has proven to be superior to text-based passwords [6, 7]. Text-based user-chosen passwords continue to dominate in the wild; however, they continue to cause agonizing pain to system administrators because of the fact that users tend to construct predictable passwords [6, 14] and most of them continue to use the same password across multiple accounts [20]. This bad practice often leads to user's accounts being compromised and on various occasions have caused huge losses [21].

System-assigned passwords provide much stronger security but they suffer from a major usability issue, as they may be difficult to remember and may lead to user's writing them down. Many proposals have been put forward to use some variant of system-assigned passwords, which can be easier to remember and recall.

In this chapter, we start with the techniques recommended by previous research studies to make user-chosen passwords much stronger and then discuss the related-work around system-assigned passwords. We also present their limitations to understand the motivation of our work.

2.1 User-chosen Passwords

Various techniques have been suggested by organizations to assist users in constructing stronger passwords. One technique is to have password-composition policies in place, so as to force the user to construct passwords based on strict rules, which would make the password stronger. However, Bander AlFayyadh [8] et all studied the password composition policies of different institutions, companies and websites and found several inconsistencies in policy requirements. Moreover, such strict policies have often lead to user frustration [5,31] and since registration and password creation is not the main motive of many users, they have been found to subvert the system, ultimately leading to construction of passwords with predictable patterns [32].

Another approach is to proactively check the strength of password at the time of creation by user and the display the strength of password to the user. Prior studies suggested adopting strategies such as rejecting passwords that are from a pre-defined list containing popular/common passwords [33] and one's that are deemed weak [34]. However, such password meters have been found to be annoying to users [19]. Additionally, a comprehensive study on password meters demonstrated the weakness and inconsistencies in deployment of these meters on real-world websites [35]. It clearly suggests there is a need to reach a consensus on strengths of user-chosen passwords.

2.2 System-assigned Passwords

Some security experts suggest system-assigned passwords are the best alternative to tradition text-based user chosen passwords. In a setting where system-assigned passwords are used, users are assigned a randomly generated password by the system and it's the user's responsibility to memorize the password and recall it for future logins. Several studies have revealed that although system-assigned passwords offer a higher degree of security, they often fail to offer sufficient memorability [2, 28, 29].

To solve the problem of weak memorability, researchers have come up with unique design schemes for systems assigning random passwords. Some of these schemes are discussed below.

2.2.1 Pronounceable Passwords

M Gasser in 1975 [25] made an attempt to make system-assigned passwords more memorable by creating a pronounceable but random password generator. He suggested that the more "English" a word appears to look like, the easier it is to remember it. He stressed that the generator should only focus on generating a word that can be pronounced rather than focusing on how it is to be pronounced and this can be achieved by use of phonemes. With appropriate rules, random phonemes can be arranged together to form a pronounceable phoneme-word. This work by Gasser has been adopted with a little modification by NIST [26]. However, Ganessan et all [27] studied that the Gasser system produces passwords which can be guessed

more easily as the system relies on frequencies of syllables as they appear in English language.

The Pronounce3 scheme generates such pronounceable random passwords. The flaw highlighted by Ganesan et all [27] for pronounceable passwords is avoided in Pronounce3 scheme, by adopting a simple approach in password construction which results in uniform entropy for all passwords generated in the password space.

2.2.2 Passphrases

Passphrase is a password that is composed of a sequence of full or partial words. They are typically longer than ordinary passwords, and hence many argue that they are more secure and easier to remember. The advantage of passphrases is that for each word in the passphrase, the user has a mental connection associated with each word, using which the user can form passwords by concatenating several such words. However, there exists little empirical evidence that supports the claim of superiority of passphrases over ordinary passwords.

Richard Shay et all [28] explored the usability of 3 and 4 word system-assigned passphrases against 8 character system-assigned pronounceable passwords and found no substantial improvement in performance of system-assigned passphrases compared to system-assigned passwords of similar entropy. In their study, they compared the usability of 8 different variants of passphrases and three variants of system-assigned passwords. They found that the users disliked

system-assigned passphrases and many of them opted to writing it down. Another major issue with passphrases was selecting the dictionary. A major takeaway from their study is the performance of pronounceable passwords. Users who were assigned eight character long pronounceable passwords performed extremely well both in terms of accuracy and login time.

2.2.3 Mnemonic Passwords

Mnemonic is a learning technique that helps in information retention in the memory by using elaborative encoding or imagery to encode information to be retained in the human memory. Carrier et all [23] suggested that mnemonic has been recognized as an effective way to encode and retrieve information. A study by Yan et all [24] demonstrated that mnemonic strategies can be exploited by users to memorize tough passwords. For example, the sentence “The rainbow has 7 colors” could be used as a mnemonic to remember the password “Trh7c”.

However, the effectiveness of this technique depends solely on user’s ability to form mnemonics that are memorable. Sundararaman [22] developed a technique to generate memorable mnemonics for a given password, thereby releasing the user of its responsibility to form mnemonics. Their system generated mnemonics for 80.5% of six-character passwords and 62.7% for seven-character passwords. Because of lack of sophisticated systems to generate plot lines for mnemonic stories from scratch, the mnemonics formed are often repetitive, semantically unrelated

and mechanical in nature, which affects the memorability of the password as well as limits the number of unique mnemonic stories that can be generated.

CHAPTER 3

SYSTEM MODEL

In this chapter, we propose a novel technique based on the concept of rote-memorization and chunking, to improve the memorability and long-term recall of system assigned passwords. In Section 3.1, we describe the design of our system and then explain our reasoning for choosing this design based on cognitive psychology (refer Section 3.2).

3.1 System Design

There are two major parts of our system: account registration and login. During the account registration process, one randomly generated pronounceable password, of length 9 characters, is assigned to the user. To assist the user in memorizing the random password, a part of the registration process is to play a simple ball and cup game which is based on combination of rote memorization and chunking technique, which makes memorization easy and fun. The motive of the game is to help plant the random password in user's memory with rigorous training, so that it can be easily recalled in the future. On completion of the game, the user is asked to type in the entire password to complete the registration process.

During subsequent logins, users only need to recall the randomly assigned password from memory and type it to complete the authentication process, similar to any recall-based textual password schemes. The main advantage of such technique is a very short login time, which is a major usability issue for any

recognition-based password schemes [36]. More detailed description of the password generator and game is presented below.

3.1.1 Random Password Generator

While purely random strings of characters can be learned in our game, we discovered in prototyping that typing and memorizing such strings could be difficult in some cases (e.g. "wza"). To avoid this, we propose the use of pronounceable random passwords, such that users can associate the string with a short sound. While prior work (see Section 2.2.1) shows that pronounceable passwords offer no substantial benefit in memorization in the general case, our initial tests found them more usable in the context of our game.

We have used a tweaked version of the pronounce3 password scheme for generation of pronounceable random passwords. The pronounce3 scheme produces pronounceable passwords for English speakers. For our study, we used the tweaked version of pronounce3 to generate three different strings of three characters each and then concatenated these strings to form a nine-character password. For generation of each three-character password set, we defined rules as follows:

i. The string must begin and end with a consonant.

ii. Every consonant must be followed by a vowel.

Based on these rules, a template ***T*** for a nine-character password can be defined as:

$$T = \beta\alpha\beta\beta\alpha\beta\beta\alpha\beta$$

Where β represents a consonant and α represents a vowel. Let P_T denote the set of passwords generated by our scheme. For a template consisting of V vowels and C consonants, P_T can be defined as:

$$| P_T | = 5^V \text{ x } 22^C$$

Hence, using the tweaked scheme of our nine-character password generator, the generator chooses a password from the set P_9 defined as:

$$| P_T | = 5^3 \text{ x } 22^6 = 2^{33.72}$$

The generator thus provides 33.72 bits of entropy. For comparison, six random lowercase letters would offer 28.2 bits of entropy. Fig. 3-1 shows the sample output of our passport generator.

```
vujwibcox
fudyuxzim
zudyipvez
munnewxom
loswilver
zokkehdiy
daymiqkat
vijheqdon
```

Figure 3-1 Sample output of tweaked version of pronounce3 password scheme

3.1.2 Game Design

The game consists of a falling ball and a cup, as represented by Fig. 3-2. The game has 7 levels and the aim of the game is to catch the falling ball in the cup and clear all the levels. The randomly assigned password of length nine is broken down into three chunks of three letters each, to take advantage of chunking (see Section

3.2.2). You can see in Figure 3-2, that the screen is divided into three separate columns and each column is associated with one chunk. So for a password "higcokbuc", the first column contains the chunk "hig", second contains "cok" and the last column contains "buc". At a time, only 1 ball falls and only 1 column is active.

Figure 3-2 A screenshot of our game containing a falling ball and a cup

When the ball falls in a particular column, the user has to correctly type the chunk associated with that column to move the cup under the ball to catch it. For example, in Figure 3-2, to catch the ball in the cup, the user has to type "hig" to move the cup under the ball. If the user types the chunk incorrectly, the cup stays in its position and the ball falls quickly to the ground. This process is repeated five times per chunk per level and during the first two levels, the chunk is shown in center of that column as a hint in order to plant the chunk in user's short-term memory. In later levels (level 3 and 5), to test the user's short-term memory, the hint is shown only when the ball falls below half the screen size. After completion of each level, a

diamond is added above the progress bar, to help users keep track of their progress. In the 7th level, no hints are shown at all and users are forced to use their long-term memory to type the chunk to catch the ball. Any mistake made while typing the chunk for first time in 7th level takes the user back to level 5 to allow for more training.

3.1.2.1 The distractor Task

Our intention to have a distractor task was to distract participants from the subject of our investigation and to require them to spend a small non-trivial effort. We wanted this distractor task to be meaningfully relevant to the ongoing task but also wanted this to be quick and fast, so as to avoid a long registration time.

In the distractor levels (level 4 and 6), the password chunks were replaced by random 3-digit numbers for each column and were shown as hints on the center of the column (Figure 3-3). Every time a ball was falling in a column, a new random number chunk was generated. The users still had to type the random number chunk to catch the ball in the cup but were not asked to memorize the numbers. To help differentiate between the distractor levels and normal levels, the color of the ball was also changed.

3.1.3 Development Platform and Tools

Phaser.js, a HTML5 based game framework, was used to develop the game. The pronounceable password generator was implemented in JavaScript and the

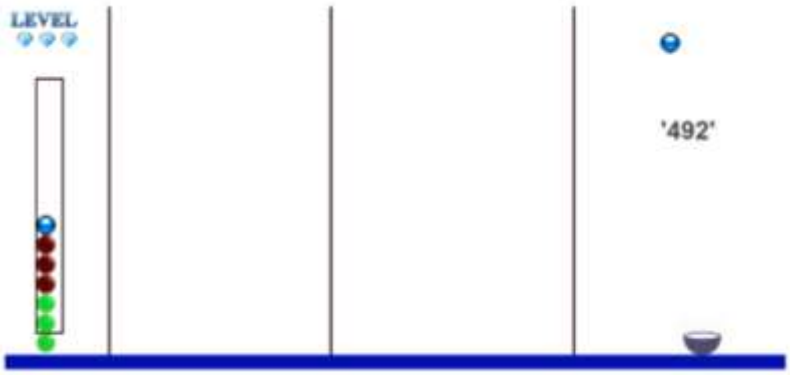

Figure 3-3 Screenshot of the game with a distractor task

sample website was developed using HTML5, CSS, JavaScript and PHP. The game assets were developed in Adobe Photoshop CS5.

3.2 Science behind Proposed Technique

In 1968, Atkinson and Shiffrin proposed a theoretical framework of the human memory [9], in which they suggested that human memory is composed of a series of stores, namely: Sensory Memory, Short-term Memory and Long-term Memory (Illustrated by Figure 3-4). According to their theory, any new information not immediately attended to, enters the sensory memory, where it remains for a very brief amount of time before getting decayed and erased. However, information that is attended to, arrives in another store called short-term or working memory. The information in this store is maintained for roughly 30 seconds, before eventually getting decayed. However, if the information is been actively rehearsed, it can be retained in the short-term store longer. Finally, the long-term memory store

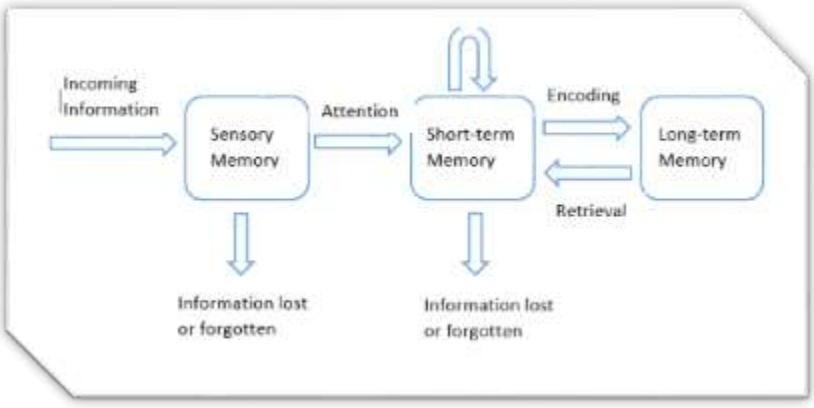

Figure 3-4 Atkinson-Shiffrin Memory Model

acts as a permanent storage of information for humans. The transfer of information (copying) from short-term store to long-term store depends on further processing and encoding. Memorization techniques can assist in encoding of information and thereby eventually assist in transfer of information from short-term store to long-term store, aiding in long-term recall.

3.2.1 Rote Memorization

Rote memorization is a form of a learning technique, which is based on repetition. The fundamental idea behind rote memorization is that the more one performs the same task repeatedly to memorize a material, the easier it will be to quickly recall it. This form of learning is routinely used in scenarios where fast memorization is required, such as learning a dialogue from a script or memorizing a phone number. The science behind rote memorization is based on the working of

human memory, described in section 3.1, where repetition and rehearsal of information helps to maintain the information in the short-term store, and eventually supplements the process of transferring the information to long-term store. Atkinson and Shiffrin cite evidence for this transfer of information in studies by Hebb [11] and Melton [10], where subjects had to repeat sequences of digits, which were then gradually learned by the subjects. Similar basic repetition tasks have also been used before to train users to learn stronger (56-bit) passwords [12, 13].

Rote memorization is a boring task, and effective if used properly. We propose to harness the power of rote memorization by making it pleasant and effective with use of games played at time of registration. This game based learning approach has been used before [37] and has proven to be an effective technique, since playing the game increases the user's engagement level. Given the appropriate training at time of registration, general users can avail power of rote memorization to memorize system assigned passwords in a fun way.

3.2.2 Chunking

Traditional concept of *chunking* refers to the practice of breaking down an element into multiple smaller elements that are semantically meaningful. A good example of chunking is representation of a phone number in the United States, where a ten-digit phone number is broken down into smaller chunks of 3-3-4 (e.g. 123-456-7890) where each chunk represents area code, exchange code and

subscriber number respectively. Since the chunking concept already exists and is working well in the real world, we hypothesized that breaking down a long system-assigned password into smaller chunks of equal lengths, even if they have no semantic meaning, would improve the password's long-term memorability. Jun Ho Huh et all [38] studied the effect of chunking on system-generated PIN's memorability and found that, overall, there was an improvement in memorability of system-generated PIN's.

Chunking is a psychological process where individual pieces of information are pieced together to form a meaningful whole. Previous literature work, such as Miller's [30], has shown that probability of recall increases when chunking strategy is used. He suggested that short-term memory has a capacity of "seven plus or minus two" chunks. Hence remembering 10 separate digits of a phone number can be difficult, as it's beyond the 'seven plus-or-minus two' memory span. Chunking on the other hand proves beneficial as with 3 chunks of 3-3-4 (which is well under the seven plus-or-minus two limit of short-term memory), it become easier to remember a phone number.

We evaluated various chunking policies [39], and found breaking a 9-character password into chunks of 3-3-3 to be an optimum technique to aid in memorization.

CHAPTER 4

USER STUDY

This chapter focuses on the design of our user study to evaluate our proposed technique of assisting users to memorize system-assigned passwords. The study was conducted on-campus at University of Texas – Arlington, in a controlled lab environment, and was approved by the Institutional Review Board (IRB) of UTA.

4.1 Participants

4.1.1 Recruitment

For our in-lab user study, we recruited participants by collaborating with students of CSE 1301 class in the Department of Computer Science and Engineering at University of Texas at Arlington. These participants were compensated one lab credit for completing the entire study. We also recruited participants through distribution of flyers and word of mouth and such participants were compensated with one $10 Amazon gift card.

4.1.2 Demographics

We had 17 participants in total, where 7 were male and 10 were females. The youngest participant was 19 years old whereas the oldest one was 32 years old and the mean age of our participants was 22.06. All the participants were students of UT-Arlington and came from diverse background including Psychology,

Chemistry, Public Relations, Mechanical Engineering, and Healthcare Administration etc.

Of the 17 participants who reported their current Degree level, 13 reported as currently pursuing Bachelor's degree whereas 4 reported pursuing Master's degree. All 17 participants completed the Phase 1 of our study and only 14 participants returned one week later to complete the Phase 2 of the study.

4.2 Apparatus

To test the effectiveness of our technique for a general web application, we created a sample website which we outfitted with our study condition. The sample website records user's behavior such as time taken to complete the registration process, number of attempts made to login, time taken for each login attempt and keystroke.

4.3 Procedure

Our user study was divided into two phases, both separated one week apart where each study was roughly 20 minutes long. The gap between both phases was one week because it was larger than the average interval for a user between subsequent logins for her crucial user accounts (like Bank accounts) [40]. Several other studies on authentication systems [41, 29] also followed a gap of 1 week between sessions.

4.3.1 Phase 1

Participants had to be physically present in the lab and were asked to report at a specific time previously agreed upon. They were then presented with the consent form to read and sign after which they were given an overview of our study. They were given sufficient time to ask questions before starting the user study. The participants were then asked to perform registration on the sample website. On entering the required details on our sample website, the system generated a 9 character long random password, following which they were asked to play a game, as part of the registration process, to memorize the password. On completion of the game, the website prompted the user to enter their entire password for verification and the account registration process came to an end. The participants were then asked to complete a paper-based survey (see Appendix A) about their experience for this phase of the study. Before leaving, the participants were reminded to show up for the second phase of the study after one week.

4.3.2 Phase 2

After a week of completing the Phase 1, when participants returned for the Phase 2 of the study, they were asked to log in to the sample website using the password that was assigned to them in Phase 1. They were allowed to make a maximum of five attempts for a successful login. After finishing, they were asked to complete a paper-based survey (see Appendix B) about their overall experience. Participants were then compensated and thanked for their time and participation.

4.4 Ecological Validity

Our participants came from diverse majors, were young, educated and hence they represent a large number of real world Internet users, but do not necessarily generalize to an entire population of Internet users. The choice of conducting a lab-based user study was made based on the fact that a lab setting has been preferred studies to test brain-powered memorability of passwords [42]. A lab setting also allows us to restrict influence of unwanted variables on our study and helps us establish performance criteria to determine if field study would be beneficial to conduct in the future.

CHAPTER 5

RESULTS AND DISCUSSION

In this section, we present the results of our user study described in Chapter 4 followed by a discussion. The metrics we used to evaluate the usability of our proposed technique were: memorability, registration time, number of login attempts, login time and user feedback. Since 3 out of 17 participants did not return to complete the Phase 2 of our user study, their data has been excluded, so we present the findings of 14 participants.

5.1 Results

5.1.1 Memorability

Our results show that out of 14 participants in the user study, 10 participants (71.43%) were able to recall their system-assigned password after 1 week and were successful in logging into our sample website. Of the 10 participants who were able to login successfully, 9 participants (90%) were able to login in their first attempt whereas 1 participant succeeded in the fifth attempt.

5.1.2 Registration Time

We define registration time as the time taken by participants to finish playing the game to memorize the system-assigned password.

The mean registration time using our technique was 362.4 seconds (6.04 minutes) and the median and standard deviation was 357 seconds and 30.59

seconds respectively. At the end of Phase 1, we asked for the perception of participants on the registration time (time for learning the password) of our proposed technique through a five-point Likert scale (Strongly Disagree: 1 to Strongly Agree: 5) question "Learning my password was Time consuming". The feedback we received for this question had a Median: 3 and Mode: 3 (See Figure XX). At the end of Phase 2, we asked the participants, through a five-point Likert scale question, if the time spent for learning the password was worth it. The feedback we received was Median: 4 and Mode: 4 (See Figure YY).

5.1.3 Login Time

In our study, we have only considered the login time of participants who were able to login successfully. Additionally, we have defined login time as the summation of time of all the unsuccessful and successful attempts made to log in. For example, if a user required three attempts to login successfully, then the login time is defined as the sum of time taken for the two unsuccessful attempts and time taken for the third attempt, which was successful. We have excluded the data of all participants from result analysis who made more than five unsuccessful attempts to login.

Our results show that the mean login time was 4.2 seconds and the median and standard deviation was 3.29 seconds and 3.25 seconds respectively. Compared to login times of other password schemes [12,13,22,28,29], this login time is considered ideal for recalling and typing a 9-character password.

5.1.4 Number of attempts

In our study, we take into account the number of attempts made by users who were able to login successfully. The mean number of attempts for successful login was 2.4, median being 1 and standard deviation of 2.02.

5.1.5 User Feedback

To understand user's sentiments while using our system, we asked the participants to answer a paper-based survey (see Appendix A & B) at the end of each phase of our user study. Most of the questions were on a 5-point Likert scale and participants were asked to indicate their agreement from "Strongly Agree" (5 points) to "Strongly Disagree" (1 point). The feedback received for each phase is described below.

Phase 1

At the end of Phase 1, we asked for the feedback from participants about their learning experience and whether learning through rote memorization by playing a game was annoying or time consuming. Figure 5-1 shows some of the user's responses after completing Phase 1. We received positive responses from participants regarding the fun they had and about the easy learning process. We received mixed responses regarding the process being time consuming, whereas most participants disagreed that the process was annoying.

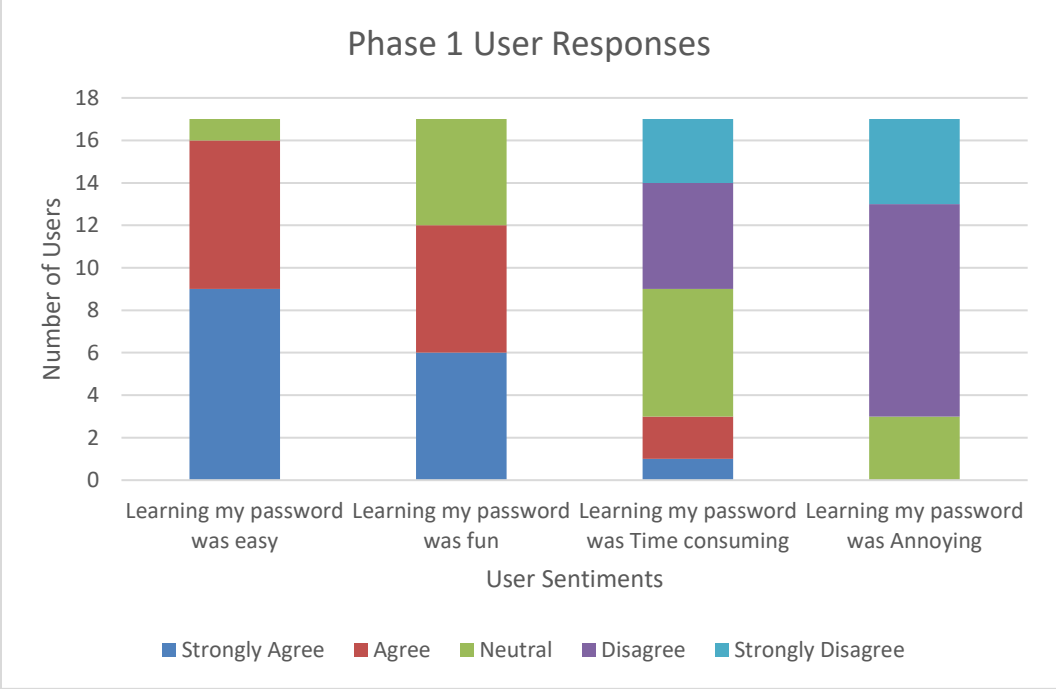

Figure 5-1 User responses to survey questions after Phase 1

Phase 2

At the end of Phase 2, we asked the participants about their feedback regarding our password system and whether they found it easy to recall their password after playing the game. Figure 5-2 shows users responses to some of the survey questions asked at the end of Phase 2. Most participants reported that recalling the password was easy and majority of them felt the password system was secure.

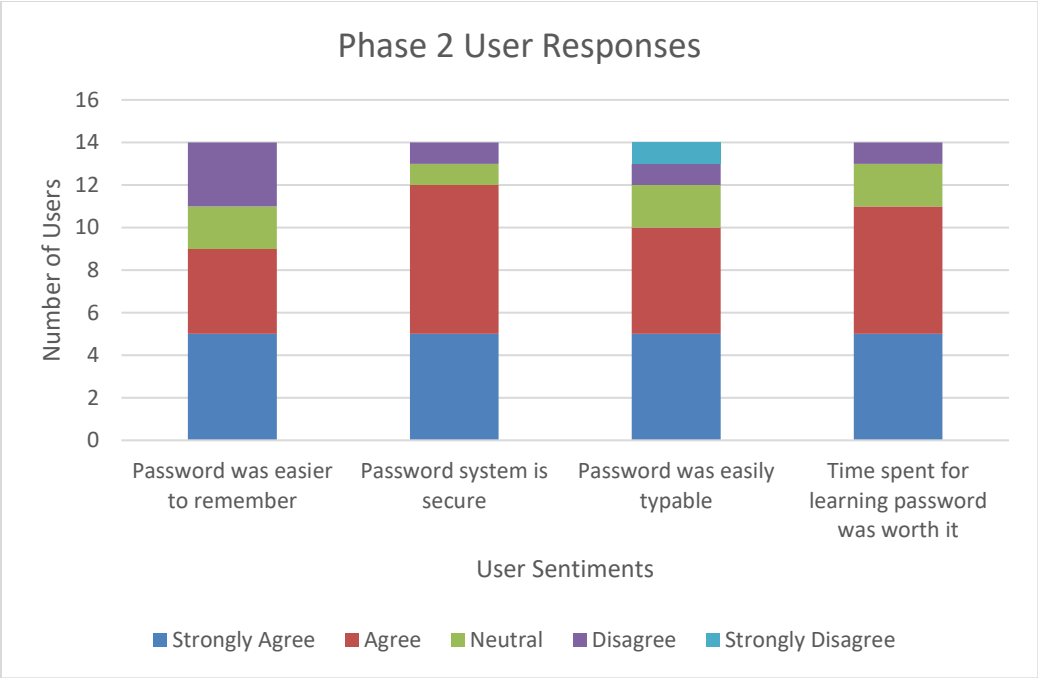

Figure 5-2 User responses to survey questions after Phase 2

5.2 Discussion

System-assigned passwords offer high level of security against brute force attacks, however, they fail at providing satisfactory memorability, as general users are not trained to memorize random passwords. We studied the human memory model by Atkinson and Shiffrin [9], where they stated that the transfer of information from short-term memory to long-term memory requires further encoding. Based on that, we designed a technique, using rote memorization and chunking which have been proven to effective learning techniques, in form of a game to engage the user in actively learning the password. Our technique explores a

new area to improve memorability of system-assigned passwords by leveraging power of human memory.

To understand the efficacy of our technique, we developed a system that employs the above technique using games, played during the account registration process, to assist users in memorizing their password. To further assist the user in learning, we used a tweaked version of pronounce3, a pronounceable password scheme, to generate random passwords. To investigate the impact of this system on improving memorability of system-assigned passwords, we conducted a user study with 17 participants.

We agree with the fact that the sample size of our experiment was not very large. Hence, generalizing our findings to a broader community should be made with great care.

5.2.1 Memorability

After a gap of seven days between learning the password and recalling it to login, we found the successful recall rate of 71.43%. This is not a significant improvement in memorability. The repetitive rehearsal of typing chunks of password should have been sufficient enough to help in the encoding of information, the recall rate suggests otherwise. The pronounceable password made a security-tradeoff to offer better memorability, but the recall rate suggest that with our technique, this tradeoff is not valuable. We conclude that our technique alone cannot offer significant improvement in memorability.

5.2.2 Registration Time

In our study, we found registration time (time to finish the game) of 6 minutes to be reasonable, as the game has 7 levels and the rote memorization technique requires lots of repetitive typing of password chunks. The game is the most crucial part of the system as the ability to easily recall the password in the future depends on the encoding of the password through rote memorization. Hence, even a longer registration time can be beneficial with more intense training, provided it offers a higher memorability.

5.2.3 Login Time

We found that the login time of 4.2 seconds to type a 9-charater password to be ideal. Since our training technique helps in encoding the information to be saved in long-term memory, at the time of login, users only need to recall the password from memory. Compared to other recognition-based password schemes, the performance of our recall-based scheme performs significantly better.

5.2.4 User Feedback

A crucial part of our user study was the feedback we asked from participants for our system after each phase of our study. The survey questions (Appendix A & B) focused on learning the user's sentiment for our proposed system and the effectiveness of the technique. Based on the survey responses we received, majority of participants found that using our technique, learning their password was fun and

easy. This is very crucial as users are spending extra effort during registration to memorize a password and the training experience plays a major factor in the usability of the system. Participants found it easier to remember their password and reported that the time spent to learn the password was worth it. This indicates that our system has potential to be used in a general setting if the memorability provided is exceptionally better.

5.3 Key Takeaways

The overall positive feedback received from participants regarding the ease of use of our system and its effectiveness suggests that the system design has the potential to improve the memorability of system-assigned passwords. With the current recall rate of our technique, the key takeaway is that rote memorization and chunking alone do not provide sufficient encoding of password in long-term memory and perhaps a more intense training could prove to be beneficial. The rote memorization and chunking technique does help in retaining the password longer in short-term memory but more work is required to transfer the password stored from short-term to long term memory.

CHAPTER 6

MODIFIED SYSTEM MODEL

In previous chapter, we discussed the results of the rote memorization and chunking technique and found that the technique was not quite as helpful as we had expected it to be. In this chapter, we propose an improved design of our previous technique, were we add the method of loci applied using a video clip before starting the game. In Section 6.1, we describe the design of our system.

6.1 System Design

There is no change in the number of components in the system compared to one described in section 3.1. At the time of registration, the system assigns a randomly generated 12-character password composed of lowercase letters from the English alphabet. In the next step, the system generates a video clip dynamically, based on the letters in the assigned password. The video clip is based on the concept of *method of loci*. As soon as the video clip ends, the user is asked to type the password after which she is tasked with playing the game, based on rote memorization and chunking. The functionality of the game is same as one described previously, but instead of using three chunks and dividing the screen into three columns, we use 4 chunks, each of 3 characters, and divide the screen into 4 columns, one for each chunk. Once the game is completed, the user is again asked to type in the password to complete the registration process.

The login process is the same, as before, the user only needs to recall the password from memory and type it in to complete the authentication process. We expect the average login time to be slightly longer as before, since the user has to type twelve characters instead of nine.

A detailed description of the password generator and video clip for *method of loci* is given below for a better understanding of our system.

6.1.1 Password Generator

Our previous stint with pronounceable passwords didn't reveal any significant results, as even with rote memorization, pronounceable passwords didn't offer any substantial gain in memorability of system-assigned password, and hence we decided to use traditional system-assigned password generators to generate random passwords.

6.1.2 Method of Loci

Although method of loci seems to be more effective if the user is extremely familiar to the environment, one research study demonstrated that virtual environments could be as effective as familiar environments. Hence, we implemented the method of loci in a virtual environment.

The virtual environment we designed was modeled after a regular real world apartment that consists of a study area, staircase to upper floors, dining room, kitchen, living room and a fireplace. Figure 6-1 shows 4 different scenes in our

virtual apartment. The 12 *loci* points we picked were study table, drawer, staircase, dining table, kitchen sink, microwave, coffee table, book shelf, sofa, fireplace, flower vase and a chair near the window. The camera visited these 12 points in the same order as above and the layout of the apartment was fixed. We also had a predefined list of 26 objects to pictorially represent the 26 alphabets of English language (for example, an apple for letter 'a', a party popper for letter 'p'). Depending on the random password assigned, 12 objects were selected, and each object would appear in order, at the 12 loci points in our virtual apartment.

Let's say the system generated a password "gupatsiekcbr", then the video clip would first show Grapes on top of study table, then an umbrella over the drawer, a party popper on the staircase, an apple on the dining table, a torch in kitchen sink, a saw near the microwave, an ice cream on top of coffee table, an egg in the book shelf, a kite on the sofa, a coin near the fireplace, a basketball on top of flower vase and lastly, a rabbit on the chair near the window.

The video clip shows the tour of the apartment, starting from first loci and ending with last, three times. In the first tour of the apartment, objects are not placed near the loci, in order familiarize the user with the apartment and its layout. The video clip visits each loci in order and every loci is spotlighted, so the user knows that it is one of the loci in the apartment. Once this is done, the camera returns to the starting position and the apartment navigation re-starts. This time, the objects are placed near the loci. This tour will be repeated again for one more time.

Figure 6-1 Screenshot of 4 different scenes in video clip

To assist the user in recognizing each object and to plant each object's visual aid in user's memory, the camera stops at the loci and the navigation is paused briefly. The object is then highlighted, flown to the center of screen with magnification, and the name of the object appears below the object with the first letter highlighted (Figure 6-2). The duration of the entire clip, including all 3 tours, is roughly 7 minutes.

Figure 6-2 Magnified object near a loci with object name

6.1.3 Development Platform and Tools

The virtual environment was developed using Unity3D and the apartment assets were developed in Autodesk Maya. The 3D objects starting with the 26 alphabets were first modeled in Autodesk Maya and were then imported in Unity3D game engine. Unity3D was used to add the camera navigation, object animation, adding light sources in apartment and adding wall textures. The placing of objects near *loci* and other functionality was implemented using C# scripting.

CHAPTER 7

CONCLUSION AND FUTUREWORK

User-chosen passwords are easily susceptible to brute force attacks, which stems from the poor decisions made by many users while constructing a password. System-assigned passwords, on the other hand, have a higher security measure but often suffer from memorability, which directly affects its usability. Hence, making system-assigned passwords more usable is the need of the hour and this can be achieved by solving their memorability issue. In this thesis, we attempted to solve this problem by exploring various memory techniques and developed a system that assists users memorize system-assigned passwords and be easy to recall it in the future. To achieve this, we harnessed human's cognitive ability and chose rote memorization and chunking technique in form of a fun game, to plant pronounceable password's in user's memory. To our knowledge, this is a novel technique to improve memorization of system-assigned passwords.

Our lab study showed that the proposed technique had a recall rate of 71.4% and mean registration time of 362.4 seconds. From our analysis, we infer that rote memorization and chunking alone do not provide good memorability, even after using pronounceable random passwords. The mean login time of 4.2 seconds in our user study indicated that a good training technique could provide the same amount of lower login time as user-chosen passwords.

Based on our findings in the user study and after analyzing the deficiencies of the technique, we modified our training technique and incorporated the *method*

of loci in our previous design technique. This new technique shows potential to improve the memorability of system-assigned passwords, as *method of loci* has been proven to be effective in increasing memorability, and once effective, it can be used in a general setting in place of user-chosen passwords.

In future, we plan to conduct a user study to test the effectiveness of the improved design. It would also be interesting to observe the performance of our technique on mobile handsets. Prior works have demonstrated the inconvenience of using uppercase letters, digits and special characters when constructing a password on a mobile device. Thus, we would like to test the technique using lowercase password on mobile devices in the future.

Appendix A

PHASE 1 PAPER-BASED SURVEY

This appendix contains the paper-based survey questions presented to participants in the end of Phase 1 of our user study.

Learning my password was easy.

() Strongly Agree

() Agree

() Neutral

() Disagree

() Strongly Disagree

Learning my password was fun.

() Strongly Agree

() Agree

() Neutral

() Disagree

() Strongly Disagree

Learning my password was time consuming.

() Strongly Agree

() Agree

() Neutral

() Disagree

() Strongly Disagree

Learning my password was annoying

() Strongly Agree

() Agree

() Neutral

() Disagree

() Strongly Disagree

I prefer memorizing the password in my own way rather than using the training method.

() Strongly Agree

() Agree

() Neutral

() Disagree

() Strongly Disagree

I will need to write down my password for remembering them even after playing the game.

() Strongly Agree

() Agree

() Neutral

() Disagree

() Strongly Disagree

Do you have a password or set of passwords you reuse in different places?

() Yes

() No

() I prefer not to answer

If my bank's online banking system assigned me a password like the one I used in this study, it would make my online bank account more secure.

() Strongly Agree

() Agree

() Neutral

() Disagree

() Strongly Disagree

Are you willing to return and try to recall your password again in a few days?

() Yes

() No

() I prefer not to answer

If you have any additional feedback about passwords or this survey, please enter your comments here.

What is your gender?

() Male

() Female

() I prefer not to answer

How old are you?

What is your major?

Appendix B

PHASE 2 PAPER-BASED SURVEY

This appendix contains the paper-based survey questions presented to participants in the end of Phase 2 of our user study.

The password was easier to remember because I played the game.

() Strongly Agree

() Agree

() Neutral

() Disagree

() Strongly Disagree

I needed to write down my password.

() Strongly Agree

() Agree

() Neutral

() Disagree

() Strongly Disagree

I feel this password system is secure.

() Strongly Agree

() Agree

() Neutral

() Disagree

() Strongly Disagree

I could easily type the passwords.

() Strongly Agree

() Agree

() Neutral

() Disagree

() Strongly Disagree

The time spent for learning the password was worth it.

() Strongly Agree

() Agree

() Neutral

() Disagree

() Strongly Disagree

I prefer this system to using a typical user-selected password system for my banking accounts.

() Strongly Agree

() Agree

() Neutral

() Disagree

() Strongly Disagree

I prefer this system to using a typical user-selected password system for my webmail accounts.

() Strongly Agree

() Agree

() Neutral

() Disagree

() Strongly Disagree

I prefer this system to using a typical user-selected password system for my social networking accounts.

() Strongly Agree

() Agree

() Neutral

() Disagree

() Strongly Disagree

I prefer this system to using a typical user-selected password system for my university portal.

() Strongly Agree

() Agree

() Neutral

() Disagree

() Strongly Disagree

I prefer this system to using a typical user-selected password system for my e-commerce accounts.

() Strongly Agree

() Agree

() Neutral

() Disagree

() Strongly Disagree

REFERENCES

[1] Gaw, Shirley and Edward W. Felten. "Password management strategies for online accounts", in Proceedings of the second symposium on Usable privacy and security, pp. 44-55. ACM, 2006.

[2] Leonhard, Michael D., and V. N. Venkatakrishnan. "A comparative study of three random password generators." Pp. 227-232. IEEE EIT (2007)

[3] Bonneau, Joseph, Cormac Herley, Paul C. Van Oorschot, and Frank Stajano. "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes." In 2012 IEEE Symposium on Security and Privacy, pp. 553-567. IEEE, 2012.

[4] 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.

[5] Inglesant, Philip G., and M. Angela Sasse. "The true cost of unusable password policies: password use in the wild." In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 383-392. ACM, 2010.

[6] Bonneau, Joseph. "The science of guessing: analyzing an anonymized corpus of 70 million passwords." In 2012 IEEE Symposium on Security and Privacy, pp. 538-552. IEEE, 2012.

[7] C. Herley and P. Van Oorschot. A research agenda acknowledging the persistence of passwords. IEEE Security and Privacy, 10(1): pp. 28–36, 2012.

[8] AlFayyadh, Bander, Per Thorsheim, Audun Jøsang, and Henning Klevjer. "Improving usability of password management with standardized password policies." In 7eme Conférence sur la Sécurité des Architectures Réseaux et Systemes d'Information (7th Conference on Network and Information Systems Security)(SAR-SSI 2012). 2012.

[9] Atkinson, Richard C., and Richard M. Shiffrin. "Human memory: A proposed system and its control processes." Psychology of learning and motivation 2 (1968): 89-195.

[10] Melton, Arthur W. "Implications of short-term memory for a general theory of memory." Journal of Memory and Language 2, no. 1 (1963): 1.

[11] Hebb, Donald Olding. "Distinctive features of learning in the higher animal." Brain mechanisms and learning (1961): 37-46.

[12] Blocki, Jeremiah, Saranga Komanduri, Lorrie Cranor, and Anupam Datta. "Spaced repetition and mnemonics enable recall of multiple strong passwords." arXiv preprint arXiv:1410.1490 (2014).

[13] Bonneau, Joseph, and Stuart Schechter. "Towards reliable storage of 56-bit secrets in human memory." In 23rd USENIX Security Symposium (USENIX Security 14), pp. 607-623. 2014.

[14] Dell'Amico, Matteo, Pietro Michiardi, and Yves Roudier. "Password Strength: An Empirical Analysis." In INFOCOM, vol. 10, pp. 983-991. 2010.

[15] Brodkin, Jon. "10 (or so) of the worst passwords exposed by the LinkedIn hack." Ars Technica (2012).

[16] Goodin, Dan. "Why passwords have never been weaker-and crackers have never been stronger." Ars Technica (2012).

[17] L. Kornblatt. When “most popular” isn’t a good thing: Worst passwords of the year – and how to fix them. http://www.splashdata.com/press/PR111121.htm, November 2011.

[18] Burr, William E., Donna F. Dodson, and William T. Polk. Electronic authentication guideline. US Department of Commerce, Technology Administration, National Institute of Standards and Technology, 2004.

[19] Proctor, Robert W., Mei-Ching Lien, Kim-Phuong L. Vu, E. Eugene Schultz, and Gavriel Salvendy. "Improving computer security for authentication of users: Influence of proactive password restrictions." Behavior Research Methods, Instruments, & Computers 34, no. 2 (2002): 163-169.

[20] Florencio, Dinei, and Cormac Herley. "A large-scale study of web password habits." In Proceedings of the 16th international conference on World Wide Web, pp. 657-666. ACM, 2007.

[21] Baker, W. H., A. Hylender, C. David Pamula, J. Porter, and C. Spitler. "M," 2011 data breach investigations report,"." Verizon RISK Team, Available: www. verizonbusiness. com/resources/reports/rp_databreach-investigationsreport-2011_en_xg. pdf (2011): 1-72.

[22] Jeyaraman, Sundararaman, and Umut Topkara. "Have the cake and eat it too-Infusing usability into text-password based authentication systems." In 21st Annual Computer Security Applications Conference (ACSAC'05), pp. 10-pp. IEEE, 2005.

[23] Carrier, Carol, Karen Karbo, Heather Kindem, Gertrude Legisa, and Laurie Newstrom. "Use of self-generated and supplied visuals as mnemonics in gifted children's learning." Perceptual and motor skills 57, no. 1 (1983): 235-240.

[24] Yan, Jeff Jianxin, Alan F. Blackwell, Ross J. Anderson, and Alasdair Grant. "Password Memorability and Security: Empirical Results." IEEE Security & privacy 2, no. 5 (2004): 25-31.

[25] Gasser, Morrie. A random word generator for pronounceable passwords. No. MTR-3006. MITRE CORP BEDFORD MA, 1975.

[26] NIST. Federal information processing standards publication 181: Automated password generator (APG). Technical report, 1993.

[27] Ganesan, Ravi, Chris Davies, and Bell Atlantic. "A new attack on random pronounceable password generators." In 17th NIST-NCSC National Computer Security Conference, pp. 184-197. 1994.

[28] Shay, Richard, Patrick Gage Kelley, Saranga Komanduri, Michelle L. Mazurek, Blase Ur, Timothy Vidas, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. "Correct horse battery staple: Exploring the usability of system-assigned passphrases." In Proceedings of the eighth symposium on usable privacy and security, p. 7. ACM, 2012.

[29] Wright, Nicholas, Andrew S. Patrick, and Robert Biddle. "Do you see your password?: applying recognition to textual passwords." In Proceedings of the Eighth Symposium on Usable Privacy and Security, p. 8. ACM, 2012.

[30] Miller, George A. "The magical number seven, plus or minus two: Some limits on our capacity for processing information." Psychological review 63, no. 2 (1956): 81.

[31] Adams, Anne, Martina Angela Sasse, and Peter Lunt. "Making passwords secure and usable." In People and Computers XII, pp. 1-19. Springer London, 1997.

[32] Stanton, Jeffrey M., Kathryn R. Stam, Paul Mastrangelo, and Jeffrey Jolton. "Analysis of end user security behaviors." Computers & Security 24, no. 2 (2005): 124-133.

[33] Schechter, Stuart, Cormac Herley, and Michael Mitzenmacher. "Popularity is everything: A new approach to protecting passwords from statistical-guessing attacks." In Proceedings of the 5th USENIX conference on Hot topics in security, pp. 1-8. USENIX Association, 2010.

[34] M. Bishop and D. V. Klein. Improving system security via proactive password checking. Computers & Security, 14(3):233–249, 1995.

[35] Ur, Blase, Patrick Gage Kelley, Saranga Komanduri, Joel Lee, Michael Maass, Michelle L. Mazurek, Timothy Passaro et al. "How does your password measure up? the effect of strength meters on password creation." In Presented as part of the 21st USENIX Security Symposium (USENIX Security 12), pp. 65-80. 2012.

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

[37] Prensky, Marc. "Digital game-based learning." (2001).

[38] Huh, Jun Ho, Hyoungshick Kim, Rakesh B. Bobba, Masooda N. Bashir, and Konstantin Beznosov. "On the Memorability of System-generated PINs: Can Chunking Help?." In Eleventh Symposium On Usable Privacy and Security (SOUPS 2015), pp. 197-209. 2015.

[39] F. Gobet, P. C. R. Lane, S. Croker, P. C. H. Cheng, G. Jones, I. Oliver, and J. M. Pine. Chunking mechanisms in human learning. Trends in Cognitive Sciences, 5(6), June 2001.

[40] 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, pages 2627–2630, May 2011.

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

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

BIOGRAPHICAL INFORMATION

Jayesh Doolani was born in Mumbai, India in 1992. He received his Bachelor of Engineering (B.E) degree in Computer Engineering from University of Mumbai, India in June 2014 and Master of Science (M.S) in Computer Science from University of Texas at Arlington, USA in December 2016. His research interests cover a range of topics including but not limited to distributed systems, human computer interaction (HCI), and security and privacy. Since joining University of Texas at Arlington, he was an active member of Software Engineering Research Group and iSec, the Information Security Lab.