LEARNING A STRONG AUTHENTICATION SECRET

BY LEVERAGING THE METHOD OF LOCI AND A COMPUTER GAME

By

Rajesh Setty

An Abstract
of a thesis submitted in partial fulfillment
of the requirements for the degree of
Master of Science
In the School of Computer Science and Mathematics
University of Central Missouri
April, 2017

ABSTRACT

By

Rajesh Setty

System-assigned random passwords offer a lot of security benefits over traditional user-chosen passwords but suffer from memorability issues. In this work, we focus on resolving this memorability issue by designing two training methods that would help users in memorizing a system-assigned random password of twelve lowercase letters. We first leverage the method of loci to dynamically generate a training video clip, which leverages the spatial and visual memory of a user. We also design a computer game to consolidate the learning process. We conducted a user study to test the effectiveness of our training methods. Our study results show that compared to previous studies, participants in our study were able to better recall the long random password and login more quickly. The participants also expressed a high level of satisfaction with our training interface. This suggests that our training interface could be leveraged to help users memorize a strong random authentication secret in just one training session.

LEARNING A STRONG AUTHENTICATION SECRET

BY LEVERAGING THE METHOD OF LOCI AND A COMPUTER GAME

By

Rajesh Setty

A Thesis
presented in partial fulfillment
of the requirements for the degree of
Master of Science
In the School of Computer Science and Mathematics
University of Central Missouri
April, 2017

LEARNING A STRONG AUTHENTICATION SECRET

BY LEVERAGING THE METHOD OF LOCI AND A COMPUTER GAME

By

Rajesh Setty

April, 2017

APPROVED:

Thesis Chair: Taiabul Haque

Thesis Committee Member: Anshuman Singh

Thesis Committee Member: Hyungbae Park

ACCEPTED:

Chair, School of Computer Science and Mathematics: Xiaodong Yue

UNIVERSITY OF CENTRAL MISSOURI

WARRENSBURG, MISSOURI

ACKNOWLEDGEMENTS

I would like to thank my supervising professor Dr. Taiabul Haque for his guidance, insights, compassion, and limitless patience and faith in me. 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. Anshuman Singh and to Dr. Hyungbae Park for taking their time to serve on my thesis committee. I would especially like to thank Dr. Mahmoud Yousef, who has been supporting me from the beginning of my graduate studies. I am also thankful to all the participants who attended my user study sessions.

Last but not the least, I would like to express my deepest gratitude to my parents who encouraged and motivated me to pursue my Masters in the United States. This research would not have been possible without their emotional support. I also thank my friends and fellow members of UCM for their helpful comments and suggestions.

TABLE OF CONTENTS

List of Figures

Figure **Page**

List of Tables

Table **Page**

CHAPTER 1 – INTRODUCTION

A good authentication secret needs to satisfy two conflicting requirements at the same time: being easy to remember and hard to guess. System-assigned random passwords are almost impossible to guess, but they are also very hard to memorize. A randomly assigned system-assigned secret of twelve lowercase letters offers a lot of entropy and if users could be trained to memorize such a secret in just one training session, it would provide a new direction towards solving the usability-security tradeoff in user authentication.

The primary goal of this work is to design and test the effectiveness of a training session that would help users in learning such a strong secret. To this end, we used the methods of cognitive psychology to leverage the spatial, visual, and muscle memory of a user in a reasonably short period of time. Unlike previous studies, the current study does not involve multiple training sessions or any kind of hint for recalling the password. We first tested and extended a previously developed interface which would assist users with memorization. We then conducted a two-part user study to test its effectiveness.

Our study results demonstrated that our system offers both a higher recall success rate and a lower login time. We also collected the responses from our users regarding their satisfaction with the system. They expressed a high level of satisfaction and stated that they would use this system for their important accounts. All of these results highlight the potential of the human brain and suggest that if users could be provided with a good training interface, they are certainly capable

of memorizing a strong random authentication secret with a single training session of around 20 minutes.

This thesis is organized into several chapters. In Chapter 2, we discuss the background of password-based authentication and highlight the usability and security issues that are associated with it. We describe the motivation of our work in Chapter 3 and explain the memorization techniques in Chapter 4. We outline our system design in Chapter 5 and describe our user study in Chapter 6. In Chapter 7, we highlight our results and discuss their implications.

CHAPTER 2: BACKGROUND

2.1 Knowledge Based Authentication

Knowledge-based authentication (KBA) is the most popular form of user authentication. This KBA method requires the users to memorize something as their authentication secret and excludes schemes like biometric or token based authentication. Biometric schemes are developed based on the biometric properties of a user such as a fingerprint or a retina, while token based authentication requires a user to carry a physical token.

KBA is the most popular kind of authentication scheme in a real-world environment, since it does not require any special hardware requirements, and is theoretically very secure. However, in regard to practical implementation, user-chosen passwords are prone to several usability and security weaknesses.

In this chapter, we predominantly focus on KBA schemes such as textual and graphical passwords, discuss their strengths and weaknesses, and outline the key concepts of entropy which are direct measurements of the strength of a KBA secret.

2.1.1 Text Passwords

UNIX operating systems were the origin for these password-based authentication systems [1], where a password was saved into a file. However, a knowledgeable attacker could get access to this file and steal the information. Wilks popped up with the new idea of encrypting a passkey

before storing it in a file [2]. Although this idea adds an extra layer of security, once an attacker guesses the encryption key, the whole system would crumble. The concept of hash function, which was proposed by Evans and Kantrowitz, acted as the panacea for these attacks [3].

2.1.2 System-assigned vs user-chosen

Typical user chosen passwords are less secure because users always prefer passwords that are easy to memorize [4]. System assigned passwords are harder to memorize [5], as they are not associated with something meaningful and they are also almost impossible to guess [6, 7].

2.1.3 PINs

Personal Identification Numbers (PINs) are passwords that contain only numbers. PINs were originally designed for those systems with only numeric entry like telephone, ATMs, and two-factor authentication. Problems with PINs are well known such as memorability and small password space [8]. Generally, PINs are used for some internet services and for unlocking mobile phones. According to the survey conducted by Clarke & Furnell with 296 cell phone users [9], about 30% of users felt that PINs are an inconvenient way of authentication and 38% contacted technical teams for unlocking their mobile after three unsuccessful attempts. Moncur and Leplatre revealed that users are more comfortable in recalling four graphical images rather than remembering four-digit PIN numbers [10].

2.1.4 Graphical Passwords

Graphical passwords are a different kind of password that uses the visual format. Usable authentication researchers have been proposing a lot of graphical password schemes since human memory recalls visual things faster than textual objects [11, 12].

Biddle et al. [13] recently reported his analysis on graphical password systems. They confirm the tradeoff of usability and security for graphical passwords too and recommends developing systems that would find a reasonable compromise between the two. They categorize graphical systems into three major categories:

1. Recall-based system

   For recall-based system, users are prompted to draw a password on a grid. Draw a Secret [14] is the best example for recall-based systems, where a user draws on the top of the grid and the password is created based on a user's hand movement from one grid square to another. Users generally choose predictable patterns that are easy to guess.

2. Recognition-based system

   For recognition-based system, users need to recognize a set of pictures which had been previously selected during the time of registration. Passface [15] is a recognition based technique and it holds panels of different human faces. The login time is longer for Passfaces and it has issues such as race and beauty bias because users tend to choose pretty faces and faces from their own race.

3. Cued-based system

   For cued-based system, one or more images are displayed as a cue memory and a user needs to select appropriate spots on the picture to login successfully. Passport is an example for cued based systems, where a user can select the sequence of click points on the same image as a password. The security of this type of system is diminished by the fact that users tend to select predictable click points. Cued Click-points (CCP) has also been proposed where a user is prompted to choose one click point in five distinct images

and the next image is displayed based on previous click point location. CCP attack needs more effort since it uses a larger number of images.

Stobert and Biddle compared all these schemes and according to their analysis, cued-based systems are highly secure and memorable [16]. However, Chiasson et al. found that there are some common spots on images considered as predictable [17, 18].

2.2 Entropy

Entropy can be interpreted as the randomness of a system or a structure. Password entropy is a measurement of how resistant a password is against the brute force attack. Basically, password entropy is calculated in bits. The formula for measuring the entropy of a password is,

$$\text{Entropy, } H = L*\log_2 N,$$

Where L is the length of a password, and N is the total number of characters allowed for that password. For example, if a password policy enforces the use of the lowercase letter, uppercase letter, and digit, the value of N would be 62 (26+26+10).

From the above equation, it can be seen that there are two different ways to increase the entropy of a password: increasing the length and adding multiple character types such as an uppercase letter, lowercase letter, digit, and special character. Although the entropy is increased by adding multiple character types, it also makes the password more difficult to recall and harder to type on mobile devices.

2.2.1 Theoretical entropy and effective entropy space

As we discussed, entropy is the probability of randomly guessing a password. For password-based authentication system, the entropy in a practical scenario is not similar as the theoretical entropy. In theory, the probability of using the letter ‘a' for the password is same as the probability of using the letter ‘x'. However, in the practical case, some alphabets appear with more frequency than the others. The effective entropy space is thus a more important consideration for a real-world setting.

2.2.2 Entropy of system-assigned passwords vs. user-chosen password

In case of a system-assigned password, a user is randomly assigned a password by the system. As a result, users have no choice over the selection of the password and the theoretical password space is the same as the effective password space. This offers a huge benefit for system-assigned passwords compared to user-chosen passwords. Moreover, the desired level of entropy can be achieved easily by the system by adjusting the length or character types.

2.3 Memorability

Memorability is a very important usability issue for password-based authentication. This issue is aggravated by the fact that in modern days, a user needs to memorize multiple passwords. According to Florˆencio and Herley [19], an average user has 25 different password-protected accounts. It is very hard for a user to memorize so many passwords and as a result, users reuse the same password for multiple accounts. In fact, the major bottleneck for the system-assigned password is this poor issue of memorability. Although graphical passwords offer better memorability [20], they have deployment issues which make them a less popular option than the textual password.

2.4 Password Restriction policies

Restriction policies are an established set of rules that characterize the content and format of a password. These policies are usually set by system administrators to enforce users to choose a secure password.

To the best of our knowledge, Morris and Thompson proposed the first restricted password system [1]. According to their policy, a password is required to be more than a length of five characters with uppercase and lowercase letters, or a length of more than six.

The Federal Information Processing Standards (FIPS) proposed a standard for password usage in 1985 [21]. Sasse et al. recommended that since system configurations are getting updated every year, such standard needs to be updated too [22]. Several survey results showed that sometimes passwords created using a particular policy are less secure than proposed standard models [23, 24, 25, 26].

Klein introduced a new kind of password restriction policy known as proactive password checking [27, 28], where a system imitates an attacker during password creation and reset phases, and restricts some of the commonly used passwords like "QWERTY" "AAAAAA" etc. This kind of restriction makes dictionary attacks more challenging.

Some researchers claim that password restriction policies degrade the level of security [6] [29]. Florencio and Herley examined 75 educational, government and commercial websites [30], and concluded that password restriction policy would offer a bit more security with a slight compromise of usability.

2.5 Password Creation Advice

Furnell reviewed more than ten popular websites and revealed that password creation advice is incomplete in helping users to create a secure password [31]. Users are generally more focused on creating a memorable password rather than a secure one.

Barton and Barton proposed the concept of mnemonic phrase-based passwords [32], and Yan et al. [5] conducted an experiment with 288 students to assess the security of this type of password. They confirmed that mnemonic phrase-based passwords are as memorable as user-defined passwords and as secure as the system-assigned ones.

Kuo et al. conducted a detailed study on mnemonic-based passwords [33], and confirmed that mnemonic based passwords are prone to security issues. They used John the Ripper password cracker to crack almost 4% of passwords by using a customized dictionary of 400,000 words [34]. In a subsequent attempt, they cracked 11% of passwords constructed by the participants.

Vu et al. [6] proposed a new system of mnemonic-based passwords. He instructed his first group to choose a sentence by their own, and copy the first letter of every word to create a password. Another group was instructed to transform a sentence into the mnemonic set of characters like "I had four snakes" as “EyeH@4$nake$". Although they found little difference in creation time, login time and recall rate, mnemonic-based passwords produced more secure passwords. Other studies found that longer passwords are more resistant to attacks [35].

A chunking is the process of breaking up long strings of information into smaller units or chunks. Carstens et al. conducted a considerable amount of research on chunking to identify its role in helping users creating a memorable password [36] [37] [38]. They examined different

chunking methods and reported that four-chunk passwords are less secure than two-chunk or three-chunk passwords.

Password meters have gained more popularity in recent years and most of the popular websites like Gmail [40], PayPal [41], eBay [39], and Facebook have been using meter-based password advice mechanisms. Ur et al. analyzed 14 different password meter variants by recruiting 2000 users [59]. They found that passwords created using meters provided a higher level of security. Castelluccia et al. proposed a Markov-model based adaptive password meter [23], while Kelley et al. implemented a novel password checking method based on guessability [44], [45].

2.6 Password verification questions

Password verification questions are generally used for fallback authentication. If users forget their passwords and need to retrieve their account, they are required to provide correct answers to challenging questions such as mother's maiden name, high school mascot name etc. to reset their passwords. This has become an important research topic because such challenge questions are at times easily guessable by close friends or family members.

2.7 Social Knowledge-Based Authentication

Popular social networking sites like Facebook, LinkedIn, and Google+ implemented social authentication (somebody you trust), where a user can access his/her account with the help of people they know from the same group. Schechter et al. conducted a study [46], where a user selects a person from the same group as a trustee. The trustee can verify the user's identity by phone or in person. During the study, they noticed that a few users failed to access their account since they forgot who their trustee was. Yardi et al. implemented a lineup widget in Facebook

[47], where a user would be prompted to identify some pictures belonging to a group for the purpose of authentication.

CHAPTER 3: MOTIVATION

3.1 Passwords

Traditional user-chosen passwords are fraught with security problems, whereas system-assigned passwords have the issue of poor memorability. A random sequence of letters or characters cannot be memorized easily because it is not associated with anything particularly meaningful for the user.

3.1.1 User-chosen Passwords

According to study results, if users are given the freedom to choose passwords by their own, they create passwords that are easy to memorize, which contains predictable patterns [1, 49, 45]. These passwords are susceptible to guessing or dictionary attacks. In this regard, strict password policies might help but research results have demonstrated that strict password policies might lead to user frustration without providing a considerable benefit [1, 49, 45].

The issue of password reuse is also a major problem for user-chosen passwords. Several studies have demonstrated that users reuse the same password for multiple accounts, with little or no modification [50], [60], [61].

3.1.2 System-assigned passwords

System-assigned passwords overcome a lot of security issues such as dictionary attack, guessing attack, password reuse etc. If the desired entropy level is ensured by the system, it also guards

against the brute-force attack. The major problem, on the other hand, is the memorability issue. Several studies have reported even when natural language words are used, the memorability results are not satisfactory [51, 52].

3.1.3 Strong Authentication Secret

Based on the theoretical password space, Biddle et al. categorized passwords into three types: 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 [13]. A password offering crypto-level security is considered as a strong authentication secret. Although it is impractical to use them for regular daily authentication, they are extremely important for systems with high security requirements, including enterprise account login, master password for password managers, and password for protecting private keys in cryptography.

The main motivation of this work is to assist users in memorizing a strong authentication secret in just one training session. Based on the formula of entropy, as discussed in the previous chapter, a system-assigned random password of twelve lowercase letters offers an entropy of 56 bits. We consider lowercase letters only because previous research results have demonstrated the inconvenience of using uppercase letters, digits, or special characters when using a mobile device [62], [63].

Our work is a major extension of two previous works, which have been conducted to achieve the same goal. We now discuss these works and relate them to our current study.

3.2 Spaced Repetition Technique

According to conventional wisdom, the human brain is not capable of storing a strong authentication secret such as a 56-bit password. Bonneau and Schechter challenged this notion

and successfully used the spaced repetition technique to help users memorize such a secret [56]. Spaced repetition leverages the psychological spacing effect and incorporates increasing intervals of time between subsequent review of previously learned material for consolidating the learning process. Although they achieved a recall success rate of 82%, their scheme required the participants to log into a website 90 times over a period of up to 15 days, which does not reflect the real constraint for learning an important authentication secret. For example, in some cases, a system administrator needs to memorize a strong authentication secret today to be able to start using it for tomorrow. The spaced repetition technique does not provide a solution to such real-world requirements.

3.3 Leveraging the spatial memory

Haque et al. leveraged the spatial memory to achieve a similar recall success rate as Bonneau and Schechter in just one training session [64]. They used the method of loci to help users memorize a strong authentication in just one training session. Their study results demonstrated that out of 26 lab participants, 21 could successfully recall the secret after a week (81% recall success rate). However, their work has two limitations:

1. They incorporated a password hint during the login phase to assist users who forgot their password. Without the hint, their recall success rate was moderate (58%). This password hint was a video clip which needs to be embedded with the login interface.
2. More importantly, the login time was high for their scheme. The median login time for the participants who succeeded was 2 minutes and 51 seconds, including the duration of the password hint clip (1 minute and 30 seconds).

3.4 Motivation of current work

The motivation of our current work is to extend the training interface of Haque et al. to achieve two major goals:

1. Achieving a similar recall success rate without the password hint clip
2. Reducing the login time

We note that since registration is a one-time activity and a user is motivated enough to spend a good amount of time in memorizing a strong authentication secret in just one session, we relax the time constraint during the registration period.

One observation of the study of Haque et al. was some users were not comfortable with the visual and spatial learning style. We therefore decided to introduce a second learning style to consolidate the learning experience. To this end, we decided to leverage the muscle memory in addition to spatial and visual memory. We therefore decided to test and extend a previously designed password memorization game [65], and add it with the training interface of the method of loci to provide users a more useful training interface to learn a strong authentication secret. Moreover, we believe that by playing the game and repeatedly typing the password, the typing speed would increase, which might contribute to a shorter login time.

We further observe that chunking is a useful method for memorizing passwords or PINs. We therefore decided to incorporate chunking too, for both the video clip and the game. In this way, we plan to extend and test these previously designed training interfaces to achieve a better result in terms of memorability and login time. In our next chapter, we discuss these memorization techniques.

CHAPTER 4: MEMORY TECHNIQUES

4.1 Method of Loci

Method of loci is an ancient memory technique which is also used by many modern memory contestants [66]. This technique involves imagining a familiar route such as the route from home to work or from home to school. A few landmarks are selected across the route. For example, for commuting from home to work, a person might pass by a gas station, then a Walmart, then a hospital, and so on. When required to memorize a list of sequenced items, the person could imagine putting the first item at the gas station, second item at Walmart, and so on. During recall, the person reimagines passing through the same route and recalling the items for each landmark.

4.2 Learning password by playing a game

In the context of password memorization, implicit learning refers to planting a password in a user's brain without conscious knowledge of the user. This learning process is similar to the way people learn how to ride a bicycle or how to swim. In their work, Bojinov et al. leveraged this concept of implicit learning by designing a computer game [67]. They used the game to plant a secret in a user's brain so that the user had no conscious knowledge of the trained password, and thus, not susceptible to rubber hose cryptanalysis, where a cryptographic secret is extracted from

a person by coercion. We decided to use a game to leverage the muscle memory and implement a rote learning technique with more fun to avoid the boredom associated with repetition.

4.3. Chunking

Basically, chunking can be defined as breaking down a component into smaller sub-components. In the United States, a 10-digit phone number is divided into three chunks of a 3-3-4 pattern, where each chunk is associated with a particular context (for example, the first chunk represents the area code). The Social Security Number is another example of chunking. According to Miller, the probability of a successful recall increases when something is learned by chunking [38].

By reviewing the literature of cognitive psychology and computer game, we decided to leverage all three techniques to design and test an extended training interface for the users which would assist them to learn a strong authentication secret in just one training session. As mentioned earlier, rather than building a system from scratch, we extended the training interfaces designed and tested by Doolani and Haque et al [64], [65]. We describe our system model in the next chapter.

CHAPTER 5: SYSTEM MODEL

In our system, we randomly generate a password with twelve lowercase letters and dynamically create a video clip and a computer game to help users learn that password. We implement chunking by dividing the twelve letters into four chunks.

Our system has two parts: registration (training) phase and login phase. The login phase is exactly the same as the traditional textual password, so we describe the registration phase here.

5.1 The Video Clip

The video clip shows a model of a virtual apartment with twelve different locations highlighted as twelve different loci. To implement chunking, we divide the apartment into four segments:

1. The lawn segment
2. The bedroom segment
3. The dining/kitchen segment
4. The patio segment

Each segment has 3 loci (for example, trash can is a location for the lawn segment; similarly bed for the bedroom segment, stove for the kitchen segment, and garage for the patio segment).

The video first navigates through the apartment without showing the objects, by highlighting the twelve loci. This is done to make the user familiar with the virtual apartment and the loci. Next it re-navigates by showing the twelve objects on these twelve loci. The objects are generated from

a pool of 26 objects, depending on the letter of the randomly assigned password. Figure 1 shows the screenshot of four different loci and Figure 2 shows the placement of an object on a specific location. Each object is magnified and the name of the object appears on the screen so that the participants can see it clearly.

After each chunk is displayed, the video pauses and asks the users to type the three letters corresponding to the chunk. This helps the participants to clearly distinguish between subsequent chunks. The video re-navigates for a second time so that the user can see the objects for the second time.

For example, if the randomly generated password is ‘gupatsigxbcr’, the video clip will show a guitar (‘guitar’ for ‘g’) above the trash can, an umbrella (‘umbrella’ for ‘u’) over the lawn garden, and a pencil (‘pencil’ for ‘p’) above the doormat at the entrance. The video would then ask the users to type the first three letters. After that the video enters the apartment and displays an apple (‘apple’ for ‘a’) above the bed in bedroom, a television above the shoe rack (‘television’ for ‘t’), and so on.

Figure 1. Screenshot of 4 different scenes in the video clip

Figure 2. Magnified object near a loci with object name

Once the video clip ends, the user is redirected to the game. Now that the user have already seen the video clip and learned the password, the game acts as a second method which consolidates the learning process. Moreover, it might help the users who are not good with visual learning only.

5.2 The Game interface

The main concept of the game is to bring a cup under a falling ball to catch it so that the ball does not fall outside the cup when it reaches the ground. As can be seen in Figure 3, the screen is divided into four columns, corresponding to the four chunks. In order to bring the cup at the correct position just under the ball, a user needs to correctly type the three letters corresponding to that chunk. For example, if “gdxtiuchoywy" is the assigned password, the first column is associated with "gdx" (the first chunk), the second column with "tiu", the third column with "cho", and the last column with "ywy". When the game is running in the first column, all the other columns will be inactive.

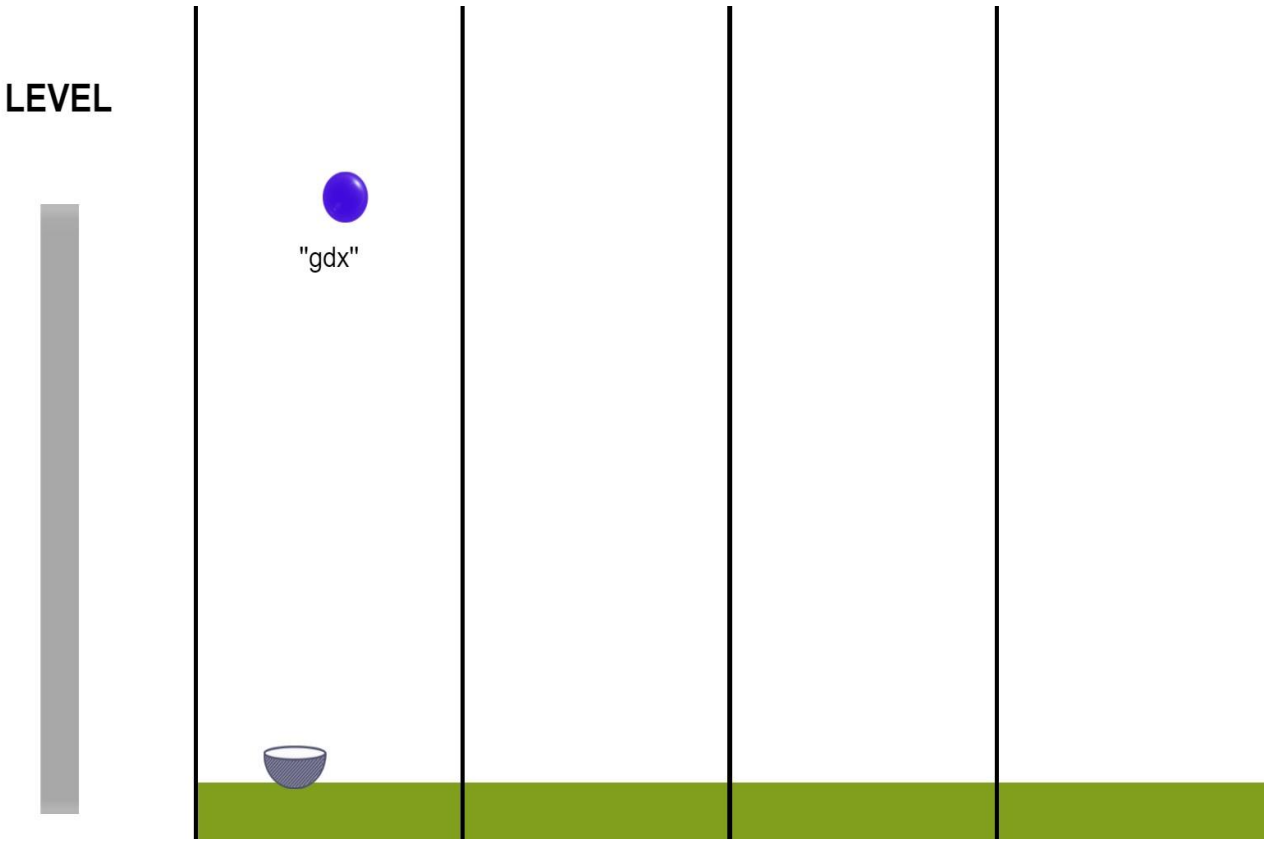

Figure 3. A screenshot of our game containing a falling ball and a cup

The game operates in multiple levels. During the first and second levels, the process will be repeated for five times for each chunk. The letters of the chunk are displayed in these two levels. During Level 3 and Level 4, the letters of the chunk are displayed when the ball crosses the half of the screen. For every successful entry of chunk one diamond is added to the scoreboard, and the user needs to achieve 15 diamonds to complete one level. Finally, in Level 5, no letter is displayed so that the user types them entirely from the memory. A failure in Level 5 makes the user restart the level.

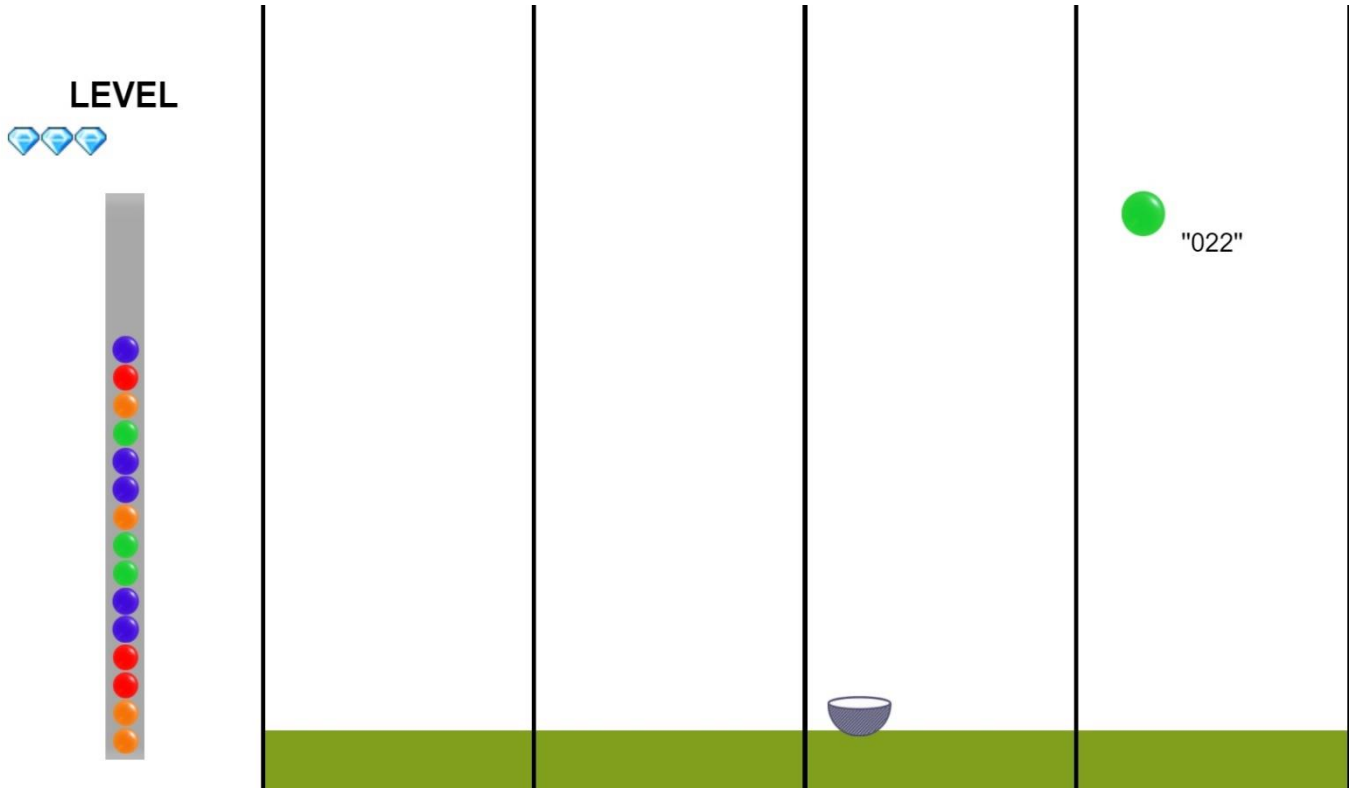

Figure 4. The distractor task

We also add a distractor task to flush the memory between the levels. The distractor task involves typing three random digits displayed on the screen, as can be seen from Figure 4.

5.3 Development Platform and Tools

We used the Unity engine for the apartment, while HTML5 framework and Phraser.js played an important role in designing the game. JavaScript and CSS were used to design the website. Game assets were designed by Adobe Photoshop CS5.

CHAPTER 6: USER STUDY

6.1 USER STUDY

We conducted a user study with University of Central Missouri (UCM) students to test the effectiveness of our system. The entire study was approved by the UCM Research Review Board.

6.1.1 Recruitment process

We recruited UCM undergrad majors from three different courses. In exchange for their time, they were compensated with extra course credits.

6.1.2 User Statistics

A total of 17 students (14 male and 3 female) participated in our study.

6.2 Apparatus

To make things realistic, we designed a website by following the layouts of a real-world website which was equipped with our password scheme. The website had two parts: registration and login. Figure 5 and Figure 6 show the screenshots of these two parts.

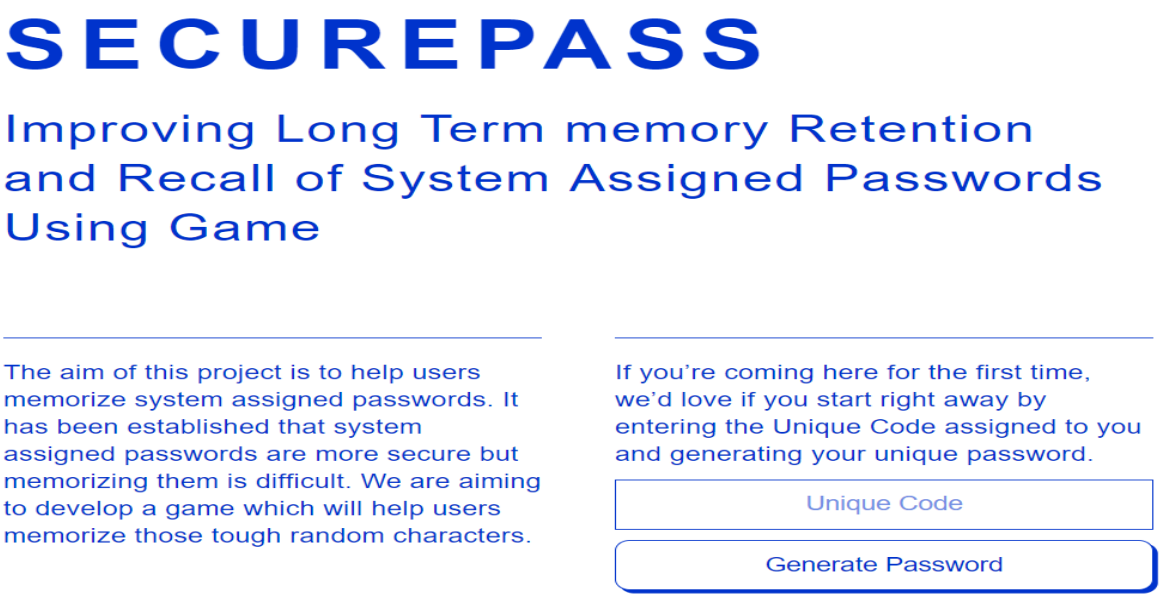

Figure 5. Registration screen

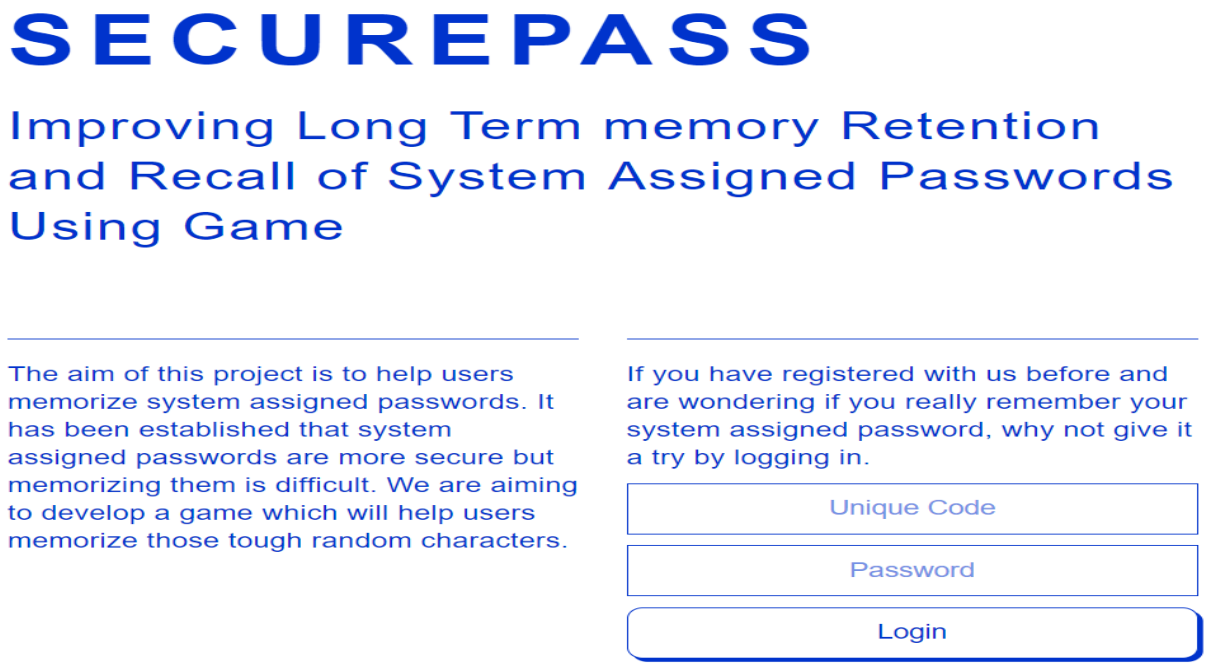

Figure 6. Login Screen

6.3 Procedure

To test the memorability, we divided the user study into two sessions, where the first session lasted around 20 minutes and the second session lasted less than 5 minutes. There was a delay of one week between the phases, and this duration is consistent with the related works [53, 54].

6.3.1 Session 1

The study was advertised as a password memory study in different sections of the three courses. The participation was completely voluntary and the participants who were unwilling to participate in our study had the opportunity to earn equal amount of extra credits by completing an alternative assignment.

The participants appeared in their scheduled timeslot and signed the consent form before beginning the study. After that they were presented with our system, as described in the previous chapter. Once they finished their training, we gave them a brief survey to express their opinion. Before leaving, we explicitly asked them to not write down their passwords.

6.3.2 Session 2

Exactly a week after the first session, participants returned for the second session. They were asked to login into the same system with the password which had been assigned in the first session. A user could only make five attempts to login into the system.

After completion of the second phase, they were asked to complete another survey. Finally, they were thanked for their time and awarded with the extra credits.

6.4 Ecological Validity

All the participants involved in our study are young and educated, and they represent a large segment of the Internet users. However, any attempt to generalize our results should be done with caution as all of our participants are undergraduate majors from Computer Science or a closely related discipline.

CHAPTER: 7 RESULTS AND DISCUSSION

Since one participant did not return for the second session, we exclude her data and present our results for 16 participants.

7.1 Memorability and Registration/Login Time

Out of 16 participants, 13 could successfully recall their password after a week, and none of them required more than three attempts. This yields a recall success rate of 81%.

7.1.1 Registration Time

The registration time is the total time required to watch the video clip and successfully complete all the rounds of the game. The mean registration time was 20 minutes and 4 seconds and the median was 18 minutes and 11 seconds.

7.1.2 Login Time

We report login time only for the participants who succeeded. The mean login time was 31 seconds and the median was 17 seconds.

7.1.3 Number of attempts

We report the number of attempts only for the participants who succeeded. The mean number of attempts was 1.44 and the median was 1.

7.2 User Feedback

As mentioned earlier, we conducted a survey in both sessions asking the participants about their opinion of our system. Their responses are summarized in Table 1, Table 2, Figure 7, Figure 8, Figure 9, and Figure 10. Some of the questions were reverse coded (for example, “Learning my password was annoying”), so a lower value means a higher level of satisfaction for these questions.

As can be seen from the tables and the figures, the participants expressed a high level of satisfaction with our system. In general, they said that learning the password was easy and fun, and they would not require writing down the password. They also said that they could easily type their password during the login session and the time spent for learning the password was worth it. Some of them even expressed their interest to use this password for their important accounts in daily life.

Seq	Questions	Mean	Median
1	Learning my password was easy	4.43	4.5
2	Learning my password was fun	4.18	4
3	Learning my password was time consuming	3.18	3
4	Learning my password was annoying	2.38	2.5
5	I prefer to remember the password in my own way rather than	2.38	2

	using the training method		
6	I will need to write down my passwords for remembering them even after playing the game	1.94	2
7	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	4.18	4

Table 1. Summary of Responses in Session 1

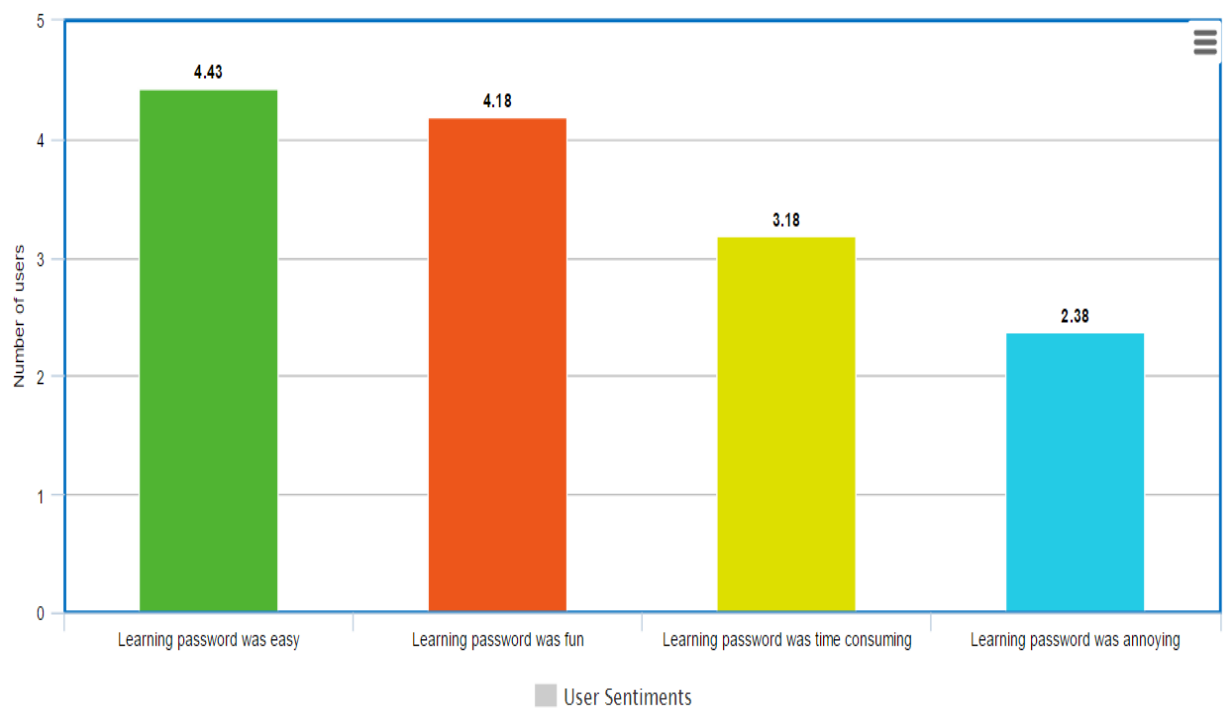

Figure 7. Responses for Session 1

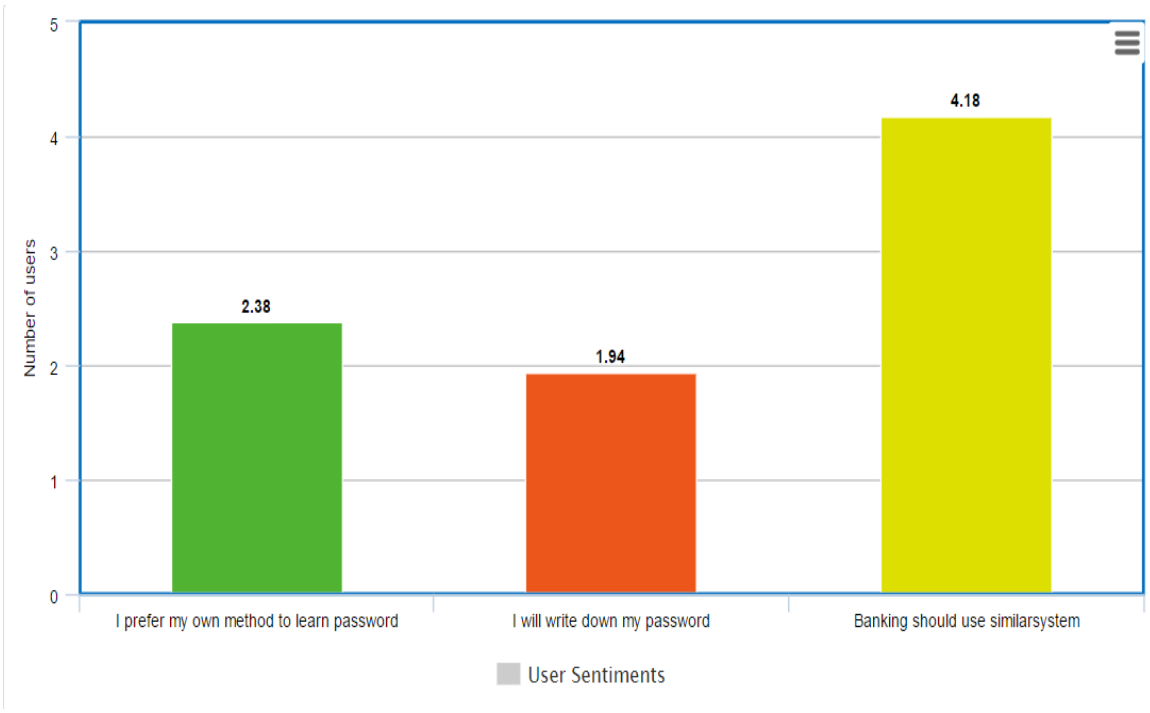

Figure 8. Responses for Session 1

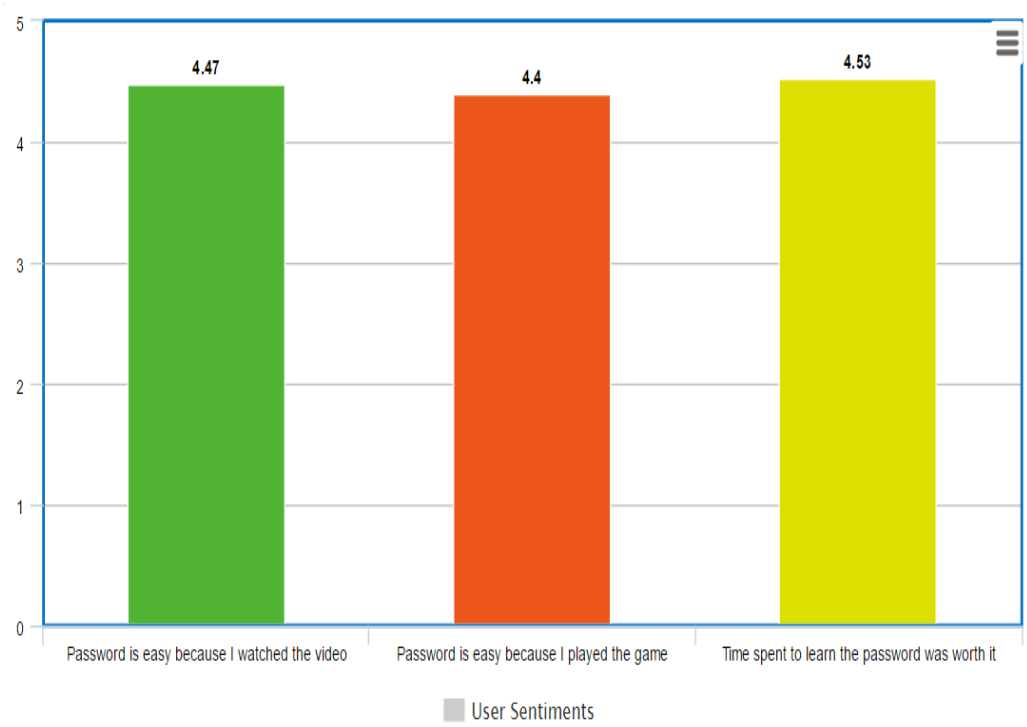

Figure 9. Responses for Session 2

Seq	Questions	Mean	Median
1	The password was easier to remember because I watched the video	4.5	4.4
2	The password easier to remember because I played the game	4.4	5
3	I feel the password system is secure	4.7	5
4	I could easily type the passwords	4.7	5
5	The time spent for learning the password was worth it	4.5	5
6	I prefer this system to using a typical user-selected password system for my banking accounts	4.1	4
7	I prefer this system to use typical user-selected password system for my webmail accounts	3.8	4
8	I prefer this system to using a typical user-selected password system for my social networking accounts	3.7	4
9	I prefer this system to using a typical user-selected password system for my university portal	4.2	4
10	I prefer this system to using a typical user-selected password system for my e-commerce accounts	4	4

Table 2. Summary of Responses in Session 2

As can be seen from Table 2, the participants expressed a favorable opinion regarding using this password for their important accounts such as bank, webmail, social network, e-commerce, university portal etc. Although we designed our system mainly for use cases like master password for a password manager and enterprise account login, we believe that it could also be used as a password for an important daily life account of a user. Our median registration time is less than 20 minutes and median login time is less than 20 seconds. We believe that these results are consistent with the time constraints of a user for one of their more important accounts. Furthermore, the participants were happy about the time spent learning the password.

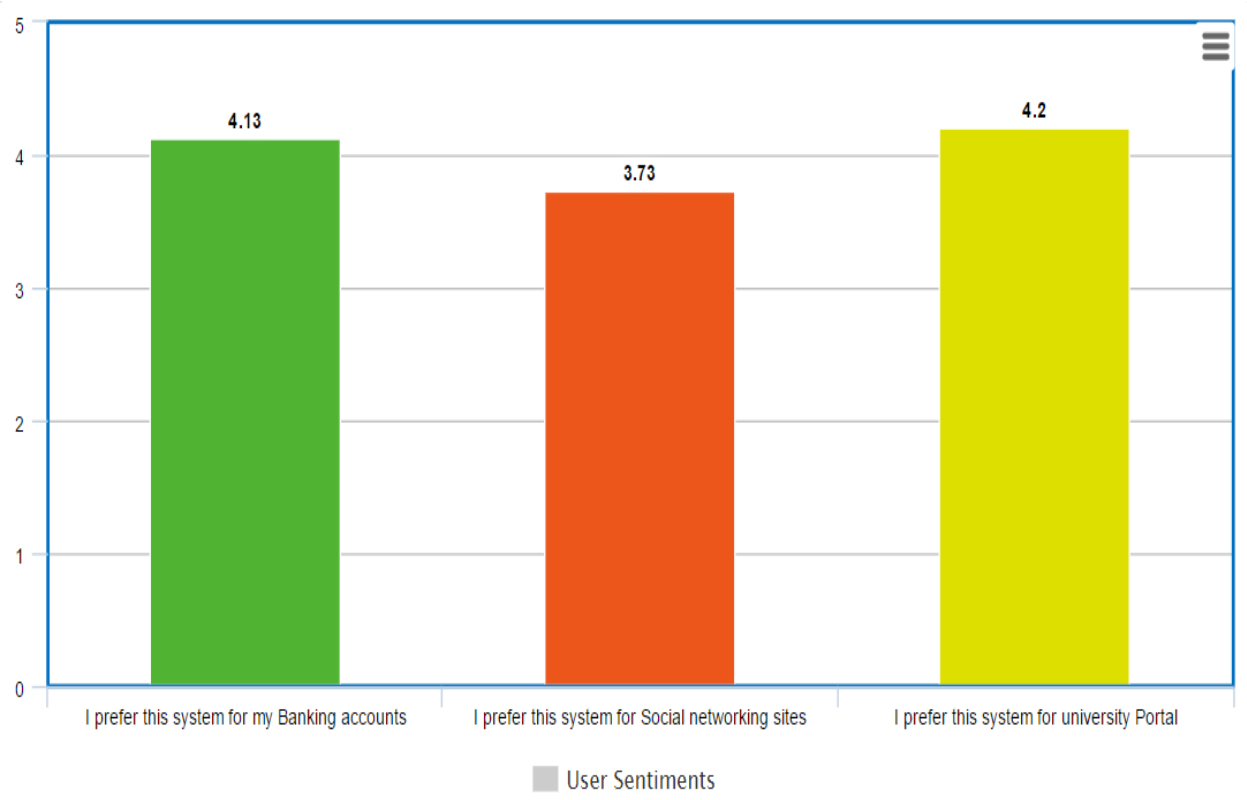

Figure 10. Responses for Session 2

Writing down a password is another bad security practice which is discouraged by security experts. We therefore explicitly asked them to not write down their password after Session 1. Our participants reported that they would not require writing down their password after completing the training session.

The participants also favored both the video and the game almost equally. Their feedback regarding the game and the video were very positive (mean was around 4.5 out of 5). We believe that both interfaces complemented each other in assisting the users to memorize their password.

We carefully analyzed the mistakes made by the three participants who failed to recall their password. One of them reported that he is not efficient with remembering things and believed that it would not be possible for him to recall the password even after multiple attempts. The other two participants were close, one of them failed to recall the middle chunk and the other missed a few objects.

7.3 Discussion

As mentioned earlier, security experts are generally not optimistic about the ability of users to remember a strong authentication secret. Bonneau and Schechter first challenged this notion and used the spaced repetition technique to help users memorizing such secret after dozens of training sessions [56].

Haque et al. further advanced this important work and achieved a similar result in one long training session [64]. However, their recall success rate was poor (58%) without a password hint which they used for the participants who failed to login successfully after three attempts. The hint clip showed the twelve loci without displaying any objects, just like the first round of

navigation during the training session. The duration of this hint clip was 90 seconds and it helped in increasing the recall success rate from 58% to 81%.

We decided to not use any hint clip as it adds a delay of 90 seconds. Our main objective was to improve both the recall success rate and the login time. In regard to recall success rate, we achieved a similar result as Haque et al. even without using the hint clip (81% in both studies), and achieved a better result if we consider their recall success rate without the hint clip (58% in their study, 81% in our study). We note that the password complexity is equal for both studies and our sample size is 18, which is smaller than their experimental sample size of 26.

Our median login time for successful attempts was 17 seconds which is another very important improvement. The median login time for the study of Haque et al. was 28 seconds for the participants who succeeded without the hint clip and 171 seconds for the participants who required to see the hint clip to authenticate successfully.

We therefore believe that the two new techniques which we added here (the chunking and the game) effectively helped the participants to increase the recall success rate and improve the login time. Although our training duration was longer, we believe that users are motivated enough to spend a longer time in a single registration session to learn an important authentication secret. Our work thus offers a fine balance between registration duration, recall success rate, and login time. The survey responses from the participants also suggested that they are satisfied with the system.

We note that our sample size is not very large and all our participants are undergraduate college majors from Computer Science or a closely related discipline. They are certainly motivated enough to learn a strong authentication secret, which might not be equally true for a larger

population base. A field study with Mechanical Turk might provide better insights about our system and help us to decide whether the system could be deployed in the real world. So far, our lab study results have demonstrated a promising initial efficacy of our system.

If we obtain good results from the field study, we believe that our system could eventually be adopted by different organizations, mainly for the purpose of internal authentication. The strength of the assigned password, the time constraint for memorizing it, and the recall success rate certainly provide a good compromise between security and usability.

7.4 Future Work

The feedback from the participants provided important insights about our system. We would like to incorporate these suggestions and make minor design changes to our system to deploy it for a Mechanical Turk field study. We would like to conduct a field study with delays of 3 days, 7 days, and 30 days (40 days from the initial registration session) to observe the long-term memorability and better understand the efficacy of our system in a more real-world setting.

REFERENCES

1. R. Morris and K. Thompson. (1979) Password security: A case history. Communications of the ACM, (22).
2. M. Wilkes. (1968) Time-Sharing Computer Systems. American Elseviser.
3. A. Evans, W. Kantrowitz, and E. Weiss. (August 1974) A user authentication scheme not requiring secrecy in the computer. Communications of the ACM 17(8).
4. 4. A. Adams and M. Sasse. (1999) User's are not the enemy. Communications of the ACM, 42(12).
5. J. Yan, A. Blackwell, R. Anderson, and A. Grant. (2004) Password memorability and security: Empirical results. Security & Privacy, 2(5).
6. K.-P. Vu, R. Proctor, A. Bhargav-Spantzel, B.-L. Tai, J. Cook, and E. Schultz. (2007) Improving password security and memorability to protect personal and organizational information. International Journal of Human-Computer Studies, 65(8).
7. M. Zviran and W. Haga. (1993) A comparison of password techniques for multilevel authentication mechanisms. The Computer Journal, 36(3).
8. R. Anderson. (December 1993) Why cryptosystems fail. In 1 st Conference on Computer and Communications Security. ACM.
9. N. Clarke and S. Furnell. (2005) Authentication of user's on mobile telephones a survey of attitudes and practices. Computers & Security, 24(7).
10. W. Moncur and G. Leplˆatre. (, April 2007) Pictures at the ATM: Exploring the usability of multiple graphical passwords. In Conference on Human Factors in Computing Systems (CHI). ACM.
11. A. Paivio, T. Rogers, and P. Smythe. (1968) Why are pictures easier to recall than words? Psychonomic Science, 11(4).
12. L. Standing, J. Conezio, and R. Haber. (1970) Perception and memory for pictures: Single-trial learning of 2500 visual stimuli. Psychonomic Science, 19(2).
13. R. Biddle, S. Chiasson, and P.C. van Oorschot. (2012) Graphical passwords: Learning from the first twelve years. ACM Computing Surveys, 44(4), in press.
14. I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin. (1999) The design and analysis of graphical passwords. In USENIX Security Symposium.
15. Passfaces Corporation. The science behind Passfaces. White paper, http: //www.passfaces.com/enterprise/resources/white_papers.htm.
16. E. Stobert and R. Biddle. (2012) Memorability and usability of graphical password forms: A graphical password bake-off. In Annual Computer Security Applications Conference (ACSAC). IEEE, in submission.
17. S. Chiasson, A. Forget, R. Biddle, and P.C. van Oorschot. (2009) User interface design affects security: Patterns in click-based graphical passwords. International Journal of Information Security, 8(6).

18. S. Chiasson, E. Stobert, A. Forget, R. Biddle, and P.C. van Oorschot. (March/April 2012) persuasive Cued Click-Points: design, implementation, and evaluation of a knowledgebased authentication mechanism. IEEE Transactions on Dependable and Secure Computing (TDSC).
19. D. Florˆencio and C. Herley. (May 2007) A large-scale study of WWW password habits. In International World Wide Web Conference (WWW). ACM.
20. S. Chiasson, A. Forget, E. Stobert, R. Biddle, and P.C. van Oorschot. (November 2009) Multiple password interference in text and click-based graphical passwords. In 16th Conference on Computer and Communications Security (CCS). ACM.
21. Federal Information Processing Standards (FIPS). (May 1985) Password usage. Publication 112, http://www.itl.nist.gov/fipspubs/fip112.htm.
22. M. Sasse, S. Brostoff, and D. Weirich. (July 2001) Transforming the 'weakest link' - a human/computer interaction approach to usable and effective security. BT Technology, 19(3).
23. C. Castelluccia, M. Duermuth, and D. Perito. (February 2012) Adaptive password strength meters from Markov models. In Network and Distributed System Security Symposium (NDSS). ISOC.
24. Komanduri, R. Shay, P. Kelley, M. Mazurek, L. Bauer, N. Christin, L. Cranor, and S. Egelman. (2011) passwords and people: Measuring the effect of password composition policies. In Conference on Human Factors in Computing Systems (CHI). ACM.
25. L. St. Clair, L. Johansen, W. Enck, M. Pirretti, P. Traynor, P. McDaniel, and T. Jaeger. (December 2006) Password exhaustion: Predicting the end of password usefulness. In 2 nd International Conference on Information Systems Security. Springer.
26. M. Weir, S. Aggarwal, M. Collins, and H. Stern. (2010) Testing metrics for password creation policies by attacking large sets of revealed passwords. In 17th Conference on Computer and Communications Security (CCS). ACM.
27. D. Klein. (1990) Foiling the cracker: A survey of, and improvements to, password security. In USENIX Security Workshop.
28. J. Brustoloni and R. Villamarin-Salom´on. (2007) Improving security decisions with polymorphic and audited dialogs. In Symposium on Usable Privacy and Security (SOUPS). ACM.
29. M. Keith, B. Shao, and P. Steinbart. (2007) The usability of passphrases for authentication: An empirical field study. International Journal of Human-Computer Studies, 65(1).
30. D. Florˆencio and C. Herley. (July 2010) Where do security policies come from? In Symposium on Usable Privacy and Security (SOUPS). ACM.
31. S. Furnell. An assessment of website password practices. Computers & Security, 26(7-8), 2007.
32. B. Barton and M. Barton. (1984) User-friendly password methods for computer mediated information systems. Computers & Security, 3(3).

33. C. Kuo, S. Romanosky, and L. Cranor. (2006) Human selection of mnemonic phrasebased passwords. In Symposium on Usable Privacy and Security (SOUPS). ACM.
34. S. Designer. John. (December 2008) the Ripper password cracker, accessed http: //www.openwall.com/john/.
35. R. Proctor, M.-C. Lien, and K.-P. Vu. (2002) Improving computer security for authentication of user's: Influence of proactive password restrictions. Behavior Research Methods, Instruments, & Computers, 32(2).
36. D. Carstens, L. Malone, and P. McCauley-Bell. (2006) Applying chunking theory in organizational password guidelines. Journal of Information, Infortmation Technology, and Organizations, 1.
37. N. Cowan. (2001) The magical number 4 in short-term memory: A reconsideration of mental storage ca-pacity. Behavioral and Brain Sciences, 24(1).
38. G. Miller. (1956) The magical number seven, plus or minus two: some limits on our capacity for processing information. Psychological Review, 63(2).
39. eBay Inc. (June 2012) eBay home page, accessed. http://www.ebay.com/.
40. Google Inc. (June 2012) Gmail: Email from google, accessed. http://www. Gmail.com.
41. PayPal. (July 2012) PayPal home page, accessed. http://www.paypal.com.
42. A. Rabkin. (July 2008) Personal knowledge questions for fallback authentication: Security questions in the era of facebook. In Symposium on Usable Privacy and Security (SOUPS). ACM.
43. C. Manning and H. Sch¨utze. (1999) Foundations of Statistical Natural Language Processing. MIT Press.
44. P. Kelley, S. Komanduri, R. Shay, M. Mazurek, T. Vidas, L. Bauer, N. Christin, L. Cranor, and J. Lopez. Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms. In Symposium on Security and Privacy.
45. M. Bishop and D. Klein. (1995) Improving system security via proactive password checking. Computers & Security, 14(3).
46. S. Schechter, S. Egelman, and R. Reeder. (April 2009) It's not what you know, but who you know: A social approach to last-resort authentication. In Conference on Human Factors in Computing Systems (CHI). ACM.
47. S. Yardi, N. Feamster, and A. Bruckman. (2008) Photo-based authentication using social networks. In Proceedings of the 1st Workshop on Online Social Networks. ACM.
48. A. De Angeli, L. Coventry, G. Johnson, and K. Renaud. (2005) Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems. International Journal of Human-Computer Studies, 63(1-2).
49. Y. Zhang, F. Monrose, and M. K. Reiter, (2010) "The security of modern password expiration: An algorithmic framework and empirical analysis," in CCS.
50. B. Ives, K. R. Walsh, and H. Schneider, (2004) "The domino effect of password reuse," Commun. ACM, vol. 47, no. 4, pp. 75–78.

51. R. Shay, P. G. Kelley, S. Komanduri, M. L. Mazurek, B. Ur, T. Vidas, L. Bauer, N. Christin, and L. F. Cranor, (2012) “Correct horse battery staple: Exploring the usability of system-assigned passphrases,” in SOUPS.
52. N. Wright, A. S. Patrick, and R. Biddle, (2012) “Do you see your password?: Applying recognition to textual passwords,” in SOUPS.
53. Wright, Nicholas, Andrew S. Patrick, and Robert Biddle. (2012) "Do you see your password?: applying recognition to textual passwords." In Proceedings of the Eighth Symposium on Usable Privacy and Security, p. 8. ACM.
54. J. Nicholson, L. Coventry, and P. Briggs. (2013) Age-related performance issues for PIN and face-based authentication systems. In CHI.
55. Blocki, Jeremiah, Saranga Komanduri, Lorrie Cranor, and Anupam Datta. (2014) "Spaced repetition and mnemonics enablerecall of multiple strong passwords." arXiv preprint arXiv:1410.1490.
56. Bonneau, Joseph, and Stuart Schechter. (2014) "Towards reliable storage of 56-bit secrets in human memory." In 23rd USENIX Security Symposium (USENIX Security 14), pp. 607-62.
57. Jeyaraman, Sundararaman, and Umut Topkara. (2005) "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.
58. Shay, Richard, Patrick Gage Kelley, Saranga Komanduri, Michelle L. Mazurek, Blase Ur, Timothy Vidas, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. (2012) "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.
59. B. Ur, P. Kelley, S. Komanduri, J. Lee, M. Maass, M. Mazurek, T. Passaro, R. Shay, T. Vidas, L. Bauer, N. Christin, and L. Cranor. (2012) “How does your password measure up? the effect of strength meters on password creation”. In USENIX Security Symposium.
60. S. M. T. Haque, M. Wright, and S. Scielzo. (2013) “A study of user password strategy for multiple accounts”. In CODASPY 2013.
61. S. M. T. Haque, M. Wright, and S. Scielzo. (2014) “Hierarchy of users’ web passwords: Perceptions, practices and susceptibilities”. International Journal of Human-Computer Studies. vol. 72, no. 12, pp 860-874.
62. S. M. T. Haque, M. Wright, and S. Scielzo. (2013) “Passwords and interfaces: towards creating stronger passwords by using mobile phone handsets”. In SPSM 2013.
63. S. M. T. Haque, S. Scielzo, and M. Wright (2014) “Applying psychometrics to measure user comfort when constructing a strong password”. In SOUPS 2014
64. S. M. T. Haque, M. N. Al-Ameen, S. Scielzo, and M. Wright. (2017) “Learning system-assigned passwords (up to 56 bits) in a single registration session with the methods of cognitive psychology”. In USEC 2017

65. J. Doolani. (2016) “Improving memorization and long-term recall of system-assigned passwords”. MS Thesis, UT Arlington
66. F.A. Yates. (1966) The art of memory. Chicago: University of Chicago Press
67. H. Bojinov, D. Sanchez, P. Reber, D.Boneh, and P. Lincoln. (2012) “Neuroscience meets cryptography: Designing crypto primitives secure against rubber hose attacks”. In USENIX 2012