ICONIC AUTHENTICATION METHODS

by

Arnaud Ajdler

Burgerlijk Werktuigkundig Elektrotechnisch Ingenieur
Afgestudeerd van de Vrije Universiteit Brussel, 1998

Submitted to the Department of Aeronautics and Astronautics
in partial fulfillment of the requirements for the degree of

Master of Science in Aeronautics and Astronautics

at the

Massachusetts Institute of Technology

February 2000

Author_____
Department of Aeronautics and Astronautics
January 14, 2000

Certified by_____
John-Paul Clarke
C.S. Draper Assistant Professor of Aeronautics and Astronautics
Thesis Supervisor

Accepted by_____
Nesbitt W. Hagood IV
Associate Professor and Chair, Aeronautics and Astronautics Graduate Committee

Iconic Authentication Methods

by

Arnaud Ajdler

Submitted to the Department of Aeronautics and Astronautics
on January 14, 2000, in partial fulfillment of the
requirements for the degree of
Master of Science in Aeronautics and Astronautics

Abstract

Iconic passwords were compared to traditional passwords. The comparison was realized in two cases, the case where the user could choose his password and the case where the user was assigned a password. Results indicate that iconic passwords are better when the user is assigned the password but traditional passwords are better when the user chooses the password. Results also indicate that allowing users to choose their passwords (instead of assigning them their passwords) increase significantly the performance of traditional passwords but not the performance of iconic passwords.

The impact of spatial memory was also studied. Results indicate that spatial memory has a significant impact on the increase of memorization performance of passwords.

Thesis Supervisor: Professor John-Paul Clarke
Title: C.S. Draper Assistant Professor of Aeronautics and Astronautics

Acknowledgments

My experience at the Massachusetts Institute of technology has been wonderful and would not have been such without the encouragement, help, friendship, and support of the people whom I want to thank now.

First, I wish to thank my family for their constant encouragements and support throughout my studies and in particular during my stay in the United States.

I would like to thank my advisor, Professor Clarke, for agreeing to supervise my research. His advice and encouragement was invaluable during this work. I also want to thank Professor McCauley-Bell from the University of Florida with whom I started this research. Her enthusiasm and her help were extremely useful for the completion of this thesis.

I want to thank Professor Markey and Professor Deyst for providing me the great experience of being the teaching assistant for the class 'Principle of Automatic Control' (or 16.060 for the insiders). This has been one of the most enriching and fun experiences I have ever known.

I want to thank all my friends for making my MIT experience much more than academic. I want to thank in particular Yoav, Alex, Patrick, Amalia, Joe, Omar, Aristide, Soulaymane and Frederic.

Last but not least, I want to thank Jeannie for always being here to support and motivate me. This work wouldn't be the same without her help.

This project was supported by a Fellowship of the Belgian American Educational Foundation (B.A.E.F.). I particularly thank the president of the foundation, Professor Boulpaep.

Contents

List of Tables

List of Figures

CHAPTER 1

1 Introduction

Authentication is the process of reliably verifying someone's identity. There are many examples of authentication in human interaction. People who know each other can recognize each other based on appearance or voice. A guard who does not know someone however might authenticate others by comparing them with the picture on their badge.

This thesis addresses the issue of user authentication by computers, and in particular password-based authentication. Although the use of passwords is so prevalent that users no longer think about it, there are many problems associated with passwords for authentication. Among them are:

- The password may be easy to guess for someone making direct login attempts to the computer.

- In attempting to force users to choose passwords that are difficult to guess, logging into the system might become so inconvenient that it becomes unusable, or users might resort to writing passwords down

These two problems summarize the trade-off that network administrators face. On one hand, they want to minimize the load of the users by allowing them to choose passwords that are easy to remember. On the other hand however they also want to maximize the security of the system. To minimize the load of the users, it is possible to imagine assigning users very easy passwords like their middle names or other personal information. The danger is that these passwords can be easily guessed. It is also possible to imagine assigning complex passwords to users but the chance they would forget the password is high. Even worse, they could write down the password to avoid having to remember it. This can also have dramatic consequences if a stranger finds the password.

The Massachusetts Institute of Technology gives the following password selection guidelines to help students understand the importance of password security. The guidelines first recommend the type of passwords a user should choose:

- Something easy for the user to remember with at least six characters and no more than 16 characters.

- Something obscure. For instance, the user might deliberately misspell a term or use an odd character in an otherwise familiar term, such as "phnybon" instead of "funnybone". Or the user may use a combination of two unrelated words or a combination of letters and numbers.

- A combination of letters and numbers, or a phrase like "many colors" and then use only the consonants, "mnYc0l0rz".

- An acronym for the user's favorite saying, for example, L!isn!" (Live! It's Saturday Night!).

The guidelines then recommend the type of passwords the users shouldn't choose:

- The user's name in any form -- first, middle, last, maiden, spelled backwards, nickname or initials.

- One's user identification, or the user identification spelled backwards.

- Part of one's user identification or name.

- Any common name, such as Joe.

- The name of a close relative, friend, or pet.

- The user's phone or office number, address, birthday, or anniversary.
- The user's license-plate number, the user's social-security number, or any all numeral password.
- Names from popular culture, e.g., spock, sleepy.
- Any word in a dictionary.
- Passwords of fewer than four characters

MIT also recommends that users never tell their password to anyone (not even their system administrator or account manager), never writing their password down and change their password frequently.

If the administrator allows users to choose their own password, then they can use the guidelines to pick something easy for them to remember but difficult for others to guess. Nevertheless, since the users select their passwords, they might put the entire system in danger by not selecting a sufficiently obscure password. Thus, in some cases, the administrator might be required to assign passwords because they cannot tolerate the possibility that a user might select a password that is easily guessed or deciphered. If the administrator assigns the passwords, then, it probably will not be an easy password to remember for the user with the danger that the user will write the password down.

This thesis seeks to investigate the use of iconic passwords as a means of achieving a greater level of password obscurity while increasing or at least not reducing the memorization abilities of the user.

1.1 Motivation

Icons (and sequence of icons) have been used for centuries as a means of telling stories to the religious faithful. Thus, as a means of communication information that is easily remembered, they are effective. They have not however, been used widely in the form of passwords although they might have two advantages.

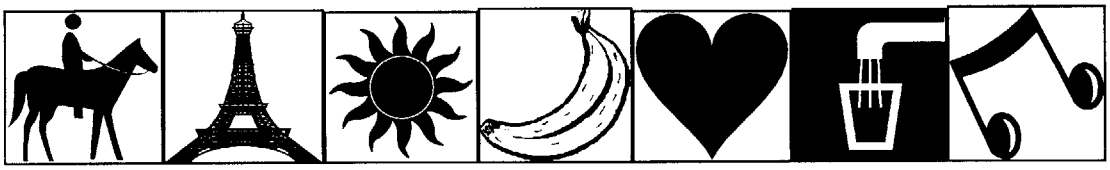


Figure 1.1: Iconic Password

The first advantage is the attribute that makes it so useful in the religious context: the ability to weave a sequence of icons into a story. Figure 1.1 shows an iconic password (constituted of seven icons) which might be used for authentication in the following manner. During login, a user would be presented with a screen filled with icons. The identification process would consist of clicking on the appropriate icons in the right order. In this case, the user would have to click on the icon with the horse, then on the icon with the Eiffel tower until the icon with the musical note to enter the system. The story corresponding to this sequence of icons might be "I was on a horse in Paris, it was sunny and I was eating a banana. Suddenly, I saw a gorgeous man/woman and I invited him/her for a drink and we listened to music."

The second advantage of iconic passwords is the obscurity of the stories that might be developed and the corresponding increase in security. Problems associated with traditional passwords might therefore be nullified as users could no longer choose passwords that could be easily guessed such as their names or dictionary words.

1.2 Objectives

The goal of this thesis was to determine the relative benefits of iconic passwords versus character passwords when passwords are assigned and selected, and the impact of spatial memory.

1.3 Approach

This goal was achieved through two experiments. The first investigated the relative benefits of iconic passwords and spatial ordering when passwords are assigned, while the second investigated the relative benefits of iconic passwords when users are allowed to select their own passwords. The details of these two experiments are described in Chapter 2 and the results are presented in Chapter 3. The results are framed within the context of the following questions:

- Do users remember iconic password or character passwords better when passwords are assigned?
- Do users remember iconic password or character passwords better when passwords are selected?

3. Is spatial memory is an important factor in memorization?

CHAPTER 2

2 Experimental Procedure

The first experiment investigated the relative benefits of iconic passwords and spatial ordering when passwords are assigned, while the second experiment investigated the relative benefits of iconic passwords when users are allowed to select their own passwords. The results of these experiments were used to determine (a) the relative benefit of icons versus characters when passwords are assigned, (b) the relative benefit of icons versus characters when passwords are selected, and (c) the impact of spatial ordering on the ability of users to remember passwords.

Evaluating the five test cases is equivalent to testing five different interfaces (see Appendix). The most inclusive experiment would therefore have a fully counterbalanced within-subject test matrix with 120 users. Because such an experiment was difficult to conduct, a combination of between and within-subjects experiments was developed to reduce the number of users to a low number (practically acceptable) and to make the user's workload acceptable (not more than three experiments per user).

The primary drawback was that comparisons between the performance of specific passwords when assigned versus when selected could not be measured directly but would have to be inferred.

2.1 Test Cases

Five test cases were developed and utilized in the experiments. The test cases are described below. Each test case represents two login sessions done on two successive days. On the first day, the user selects (or is assigned) a password. On the second day, the user is asked to recall that password.

- Test case A1 consisted of a randomly selected combination of characters with non-constant spatial ordering. Thus, the password was selected at random and given to the user at the initial login session and each character appeared at a different place on the screen at the subsequent login so that no spatial memory could be used to remember the password.

- Test case A2 consisted of a randomly selected combination of icons with non-constant spatial ordering. Thus, the password was selected at random and given to the user at the initial login session and each icon appeared at a different place on the screen at the subsequent login so that no spatial memory could be used to remember the password.

- Test case A3 consisted of a randomly selected combination of characters with constant spatial ordering. Thus, the password was selected at random and given to the user at the initial login session and each character appeared at the same place on the screen at the subsequent login so that spatial memory could be used to remember the password.

- Test case B1 consisted of a user selected combination of characters with non-constant spatial ordering. Thus, the user selected the password at the initial login session and each character appeared at a different place on the screen at

the subsequent login so that no spatial memory could be used to remember the password.

- Test case B2 consisted of a user selected combination of icons with non-constant spatial ordering. Thus, the user selected the password at the initial login session and each icon appeared at a different place on the screen at the subsequent login so that no spatial memory could be used to remember the password.

The different test cases are summarized in Table 2.1. As the table shows, test cases A1, A2 and A3 can be categorized as "test cases when passwords are assigned" while test cases B1 and B2 can be categorized as "test cases when passwords are selected."

Table 2.1: Password Categories

	Characters	Symbols	Choice of password	Space
A1	√			
A2		√		
A3	√			√
B1	√		√	
B2		√	√	

2.2 Experiment A: Relative benefits of icons and spatial order when passwords are assigned

The three test cases in Experiment A were studied using the fully counterbalanced text matrix shown in Table 2.2. This experiment had 18 subjects thus each test case was tested three times.

Table 2.2: Test Matrix for Experiment A

	First Test Case	Second Test Case	Third Test Case
User 1	A1	A2	A3
User 2	A1	A3	A2
User 3	A2	A1	A3
User 4	A2	A3	A1
User 5	A3	A1	A2
User 6	A3	A2	A1

In this experiment, two screen with characters (A1, A3) and a screen with icons (A2) were presented to the users and a specific combination of symbols was assigned to them. After 24 hours, the same symbols were again presented to the users. In test cases A1 and A2 the symbols were randomly placed at different locations on the screen so that spatial memory could not play any role. In test cases A3 the symbols were placed at the same locations as the previous time. In all three cases, the fact that passwords were assigned eliminated the effects of such factors as personal password selection strategies.

The set of characters that could be used in traditional passwords was used. The 26 letters of the alphabet, the 10 numbers, and a set of 4 non-traditional characters were presented to the users. For the screen of icons, 40 icons were presented.

2.3 Experiment B: Relative benefits of icons when passwords are selected

The two test cases in Experiment B were studied using the fully counterbalanced text matrix shown in Table 2.3. This experiment had 16 subjects thus each test case was tested eight times.

Table 2.3: Test Matrix for Experiment B

	First Test Case	Second Test Case
User 1	B1	B2
User 2	B2	B1

In this experiment, a screen filled with characters (B1) and a screen filled with icons (B2) were presented to the users and a specific combination of symbols was assigned to them. After 24 hours, the same symbols were again presented to the users. In both test cases the symbols were randomly placed at different locations on the screen so that spatial memory could not play any role.

The set of characters that could be used in traditional passwords was used. The 26 letters of the alphabet, the 10 numbers, and a set of 4 non-traditional characters were presented to the users. For the screen of icons, 40 icons were presented. The passwords were assigned because other effects (as the strategy of choosing a password) should not interfere in this experiment.

This experiment reproduced the A1-A2 sub-pairing of Experiment A with the password choice left up to the user instead of being assigned by the researcher.

2.4 Statistical Analysis

The data gathered during the experiments were analyzed using three different statistical tests: a normal analysis, a paired analysis and a binomial analysis.

2.4.1 Normal Analysis

In this approach, the results of the experiments are assumed to follow normal distributions. The results of the first test case are considered to follow the normal distribution $N_1(\mu_1,\sigma_1)$ and the results of the second test case are considered to follow a normal distribution $N_2(\mu_2,\sigma_2)$. A one sided t-test was then used to determine if one mean is bigger than the other mean.

Given that the goal of the test is to prove that $\mu_1 > \mu_2$, then the testable hypothesis is H_1: $\mu_1 > \mu_2$ while the null hypothesis is H_0: $\mu_1 = \mu_2$. The decision to accept H_1 or reject it in favor of the null hypothesis H_0 is made based on the location of the Z statistic relative to the critical region. If Z lies in this critical region, then the decision will be to reject H_1 and accept H_0. If Z lies outside this critical region, then the decision will be to reject H_1.

The Z statistic is given

$$Z = \frac{x_1 - x_2}{\sqrt{\frac{s_1^2}{m_1} + \frac{s_2^2}{m_2}}} \qquad (2.1)$$

where x_i and s_i represents the average and the standard deviation of the available data related to the normal distribution N_i and where m_i represents the number of available data.

The critical region will be defined by the following interval

$$(-\infty, \phi^{-1}[1-\alpha]) \qquad (2.2)$$

where α represents the significance level (usually 1 or 5 %) and where

$$\phi(x) = 0.5 + \frac{1}{\sqrt{2\pi}} \int_0^x e^{-0.5t^2} dt \qquad (2.3)$$

2.4.2 Paired Analysis

When paired observations are available, such as in table 2.4, a paired analysis may be performed.

Table 2.4: Table of Paired Observations

Performance	Experiment 1	Experiment 2	Difference
User 1	X_1	Y_1	$D_1 = X_1 - Y_1$
User 2	X_2	Y_2	$D_2 = X_2 - Y_2$
User 3	X_3	Y_3	$D_3 = X_3 - Y_3$
:	:	:	:
User n	X_n	Y_n	$D_n = X_n - Y_n$

The data consisted of n couples (X_i, Y_i) with X_i following the normal distribution $N_1(\mu_1, \sigma_1)$ and with Y_i following the normal distribution $N_2(\mu_2, \sigma_2)$. The null hypothesis is that the mean of both distributions are equal or in other words $\mu_1 = \mu_2$. The statistic $D_i = X_i - Y_i$ was then considered. D_i followed a normal distribution $N(\mu_1 - \mu_2, sqrt(\sigma_1^2 + \sigma_2^2))$. The idea here was to use the t-test on D_i and see if the mean of this distribution was zero. The t-test on D_i was used with the null hypothesis $\mu=0$.

The T statistic is defined by the following formula:

$$T = \frac{D_n \sqrt{n}}{S} \approx t_{n-1} \tag{2.4}$$

or, in other words, the stochastic T follows a t-distribution with parameter $n-1$.

In this formula

$$D = \frac{1}{n} \sum_{i=1}^{n} D_i \tag{2.5}$$

and

$$S^2 = \frac{1}{n-1} \sum_{i=1}^{n} (D_i - D_n)^2 \tag{2.6}$$

The hypotheses of the test are the following

$$H_0: \mu = 0$$

$$H_1: \mu > 0$$

If the null hypothesis can be rejected we could conclude that the mean of one of the distribution is bigger than the mean of the other distribution. At a 5% level, the critical region is $(-\infty, 1.753)$. If the statistic T is outside the critical region, then the null hypothesis can be rejected and the alternative hypothesis is accepted. At a 1% level, the critical region is $(-\infty, 2.602)$.

2.4.3 Binomial Analysis

In practice, a user can only enter a system if this user recalls the password perfectly. Therefore, a third way to evaluate the results is to consider the number of cases where the user could have entered the system versus the number of cases where he could not have entered the system. If the results are binomial, the statistical test is the following:

$$H_0: \pi_1 = \pi_2$$

$$H_1: \pi_1 > \pi_2$$

where π_1 represents the proportion of the binomial distribution associated with the one experiment and where π_2 represents the proportion of the binomial distribution associated with the second experiment. The test statistic can be calculated by the following formula:

$$Z = \frac{p_1 - p_2}{\sqrt{P(1-P)\left(\frac{1}{n_1} + \frac{1}{n_2}\right)}} \qquad (2.7)$$

with

$$P = \frac{p_1 n_1 + p_2 n_2}{n_1 + n_2} \qquad (2.8)$$

Under the null hypothesis that $\pi_1 = \pi_2$, Z is approximately distributed as a standard normal deviate, from there the possible test. The critical region is $(-\infty, 1.64)$ at a 5% significance level and $(-\infty, 2.33)$ at a 1% significance level. If the statistic is outside the critical region, then the null hypothesis can be rejected and the alternative hypothesis can be accepted.

2.5 Instructions to subjects

The following instructions were given to the participants of this experiment:

Purpose of this experiment:

The purpose of this experiment is to test 2 types of passwords, iconic passwords and character passwords in order to quantify their performance.

Procedure:

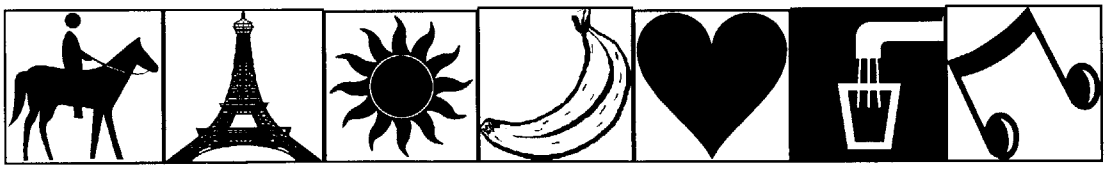
You will be asked to choose a password of 7 symbols (icons or characters depending on the experiment you are doing), write down this password, and give it to me (so that I can check if you remember your password!). Tomorrow, you will be asked to recall the password. Each participant will be asked to repeat the experiment once with a iconic password and once with a character password.

How should you choose an iconic password?

Look at the icons and try to create a story around them. For example, looking at the icons, you may start thinking about the following:

I was on a horse in Paris, it was sunny and I was eating a banana. Suddenly, I saw a gorgeous man/woman and I invited him/her for a drink and we listened to music.

That would lead to the following password:



How to choose a character password?

Do choose:

- *A combination of 7 characters, mixing alphabetical and numerical characters and punctuation.*
- *Try here to use acronym of a sentence that you think you will be able to remember. For example, if your sentence is: Yesterday, AT the Restaurant, I Met 3 Giants, then your password could be Y@RIM3G. That would be a great password.*

Don't choose:

- *A password similar to one that you already use, as that would totally falsify the experiments.*
- *Any dictionary word or your real name in any form.*

Please, in both case, iconic and character passwords, write down the password and your associated strategy to remember it (the story that you associate with the password or any other way that you use to remember it)

Thanks a lot for your help.

CHAPTER 3

3 Experimental Results and Analysis

The data gathered during the experiments were analyzed using the methods described in the previous chapter to assess the performance of iconic passwords and character passwords, and the impact of spatial memory.

3.1 User Selected Passwords

This experiment addressed the case where users selected the passwords. The counterbalanced test matrix is presented in Table 3.1. Each sequence was repeated 8 times, thus the total number of subjects was 16.

Table 3.1: User Selected Password Experiments Test Matrix

	Day 1	Day 2
User 1	Character password	Iconic password
User 2	Iconic password	Character password

The test group population consisted of the following:

- Juniors (46% of the population)
- Seniors (32% of the population)
- Graduate Students (22% of the population)

3.1.1 Results

3.1.1.1 Iconic passwords

The following results were obtained

- 9 users got the right passwords (7 icons in the right order)
- 6 users got 5 icons at the right place
- 1 user got 4 icons at the right place

The most common error that occurred (6 users) was the inversion of two icons. In other words, they remembered the right icons but inversed two of them.

3.1.1.2 Character passwords

The following results were obtained

- 13 users got the right passwords (7 characters in the right order)
- 3 users got 6 characters at the right place

The error that occurred for the three people who did not remember the right password was that they could not remember one of the characters.

3.1.2 Analysis

Initial cursory analysis indicated that user recall was better with character passwords than with iconic passwords. This hypothesis was investigated using the statistical analysis techniques described in the previous chapter. The results are presented below.

3.1.2.1 Normal Analysis

The following results were obtained from the data from the character password experiments.

- $x_1 = 6.8125$
- $s_1 = 0.4031$
- $m_1 = 16$

and from the data from the iconic password experiments, the following results were obtained:

- $x_2 = 6.0625$
- $s_2 = 1.1236$
- $m_2 = 16$

Based on these results, the Z statistic was determined to be 2.51. For a 5% significance level, the critical region is $(-\infty, 1.64)$. Since the statistic Z is outside this region, it can be concluded that character approach gives significantly better results than

the iconic approach. At a 1% significance level, the conclusion remains unchanged since the critical region becomes $(-\infty, 2.32)$ and the statistic Z is still outside the critical region.

3.1.2.2. Paired Analysis

Table 3.2 summarizes the results of the paired comparison between the iconic password method and the character password method.

Table 3.2: Results of the Paired Comparison between Iconic and Character Password

Performance	Character password	Iconic password	Difference
User 1	7	7	0
User 2	7	7	0
User 3	7	7	0
User 4	7	7	0
User 5	7	7	0
User 6	7	7	0
User 7	7	7	0
User 8	7	7	0
User 9	7	5	2
User 10	7	5	2
User 11	7	5	2
User 12	7	5	2
User 13	7	5	2
User 14	6	5	1
User 15	6	7	-1
User 16	6	4	2

For the given number of comparisons (n = 16) the values D = 0.75 and S = 1.0646. Thus the T statistic is equal to 2.83. At a 5% level, the critical region is (-∞, 1.753). Since the statistic T is outside the critical region, it may be concluded that character passwords are significantly better than the iconic passwords. This conclusion does not change at the 1% significance level as the critical region is (-∞, 2.602) and the statistic T is still outside the region.

3.1.2.3 Binomial Analysis

Table 3.3 summarizes the results.

Table 3.3: Results of the User Selected Password Experiment (Binomial Analysis)

Performance	Perfect recollection	Imperfect recollection
Character passwords	13	3
Iconic passwords	9	7

In this case, p_1=13/16 and p_2=9/16, and the Z statistic is 2.67. The critical region is (-∞, 1.64) at a 5% significance level and (-∞, 2.33) at a 1% significance level. In both cases, the statistic is outside the critical region and the null hypothesis can be rejected. Thus, it may be concluded that the binomial distribution associated with the character password method has a bigger proportion π_1 than the proportion π_2 of the binomial distribution associated with the iconic password method. In other words, the character approach gives better results than the iconic approach

3.1.3 Conclusion

These results show that when users can choose their passwords, character passwords are better than iconic passwords. It may be postulated that people use the following two elements to memorize their passwords

- The succession of characters or icons
- A personal strategy that was developed during the creation of the password

Although it is difficult to decide what the determinant element is, the conclusion is that the combination of these elements gives better results in the case of character passwords than in the case of iconic passwords.

3.2 Assigned Passwords

This analysis addresses the case where the user could not choose his password. For proper counterbalancing, 'triples' of six users were used to achieve for each triple, the following configuration:

Table 3.4: Assigned Password Experiment Test Matrix

	Day 1	Day 2	Day 3
User 1	Character password	Iconic password	Letter/spatial password
User 2	Character password	Char. /spatial password	Iconic password
User 3	Char. /spatial password	Character password	Iconic password
User 4	Char. /spatial password	Iconic password	Character password
User 5	Iconic password	Character password	Letter/spatial password
User 6	Iconic password	Char. /spatial password	Character password

The experiment had 18 subjects, thus each configuration was tested three times.

The test group population consisted of the following:

- Freshmen (6% of the population)

Sophomores (12% of the population)

- Juniors (36% of the population)
- Seniors (20% of the population)
- Graduate Students (26% of the population)

In the following analysis, the focus was put on the results related to the iconic password and the character password experiments and not on the experiments related to spatial memory (Char. /spatial password in table in Table 3.4).

3.2.1 Results

3.2.1.1 Iconic passwords

The following results were obtained:

- 8 users got the right passwords (7 icons in the right order)
- 4 users got 5 icons at the right place
- 4 users got 4 icons at the right place
- 2 users got 3 icons at the right place

The most common error that occurred to six users was the inversion of two icons.

3.2.1.2 Character passwords

The following results were obtained

- 5 users got the right passwords (7 characters in the right order)
- 4 users got 5 characters at the right place
- 1 user got 4 characters at the right place
- 3 users got 3 characters at the right place
- 2 users got 1 characters at the right place
- 3 users got 0 characters at the right place

Usually, errors occurred because users could not remember the right characters rather than because they inversed right characters.

3.2.2 Analysis

3.2.2.1 Normal Analysis

From the iconic password data, the following results were obtained:

- $x_I = 5.4444$
- $s_I = 1.5424$
- $m_I = 18$

and from the data from the character password experiments, the following results were obtained:

- $x_2 = 3.8889$
- $s_2 = 2.6321$
- $m_2 = 18$

Thus, the Z statistic is equal to 2.16. For a 5% significance level, the critical region is $(-\infty, 1.64)$. Since the Z statistic is outside this region, H_0 can be rejected and the alternative hypothesis can be accepted. The conclusion is that μ_1 is statistically significantly bigger than μ_2 or in other words, the iconic approach is better than the character approach. At a 1% significance level, the critical region is $(-\infty, 2.32)$. Since the statistic is inside the critical region, H_0 cannot be rejected. At a 1% significance level, the conclusion that the iconic password method is better than the character password method cannot be reached. Nevertheless since the Z statistic is very close to the border, the null hypothesis is close to being rejected.

3.2.2.2 Paired Analysis

Table 3.5 summarizes the results of the paired comparison between the iconic password method and the character password method.

Table 3.5: Results of the Paired Comparison between Iconic and Character Password

Performance	Iconic password	Character password	Difference D_i
User 1	7	7	0
User 2	7	7	0
User 3	7	7	0
User 4	7	7	0
User 5	7	5	2
User 6	7	5	2
User 7	7	5	2
User 8	7	4	3
User 9	5	7	-2
User 10	5	3	2
User 11	5	1	4
User 12	5	0	5
User 13	4	3	1
User 14	4	3	1
User 15	4	1	3
User 16	4	0	4
User 17	3	5	-2
User 18	3	0	3

For the given number of comparisons, $n = 18$, $D = 1.56$ and $S = 1.98$. Thus the T statistic = 3.34. At a 5% level, the critical region is $(-\infty, 1.74)$. Since the statistic T is outside the critical region, it may be concluded that iconic passwords are significantly better than character passwords. This conclusion doesn't change at the 1% significance level as the critical region is $(-\infty, 2.57)$ and the statistic T is still outside the region.

3.2.2.3 Binomial Analysis

Table 3.6 summarizes the results.

Table 3.6: Results of the Assigned Password Experiment (Binomial Analysis)

Performance	Perfect recollection	Imperfect recollection
Character passwords	5	13
Iconic passwords	8	10

In this case, p_1=8/18 and p_2=5/18, and the Z statistic is 1.04. The critical region is $(-\infty, 1.64)$ at a 5% significance level and $(-\infty, 2.33)$ at a 1% significance level. In both cases, the statistic is inside the critical region and the null hypothesis cannot be rejected. Thus it may not be concluded that that the binomial distribution associated with the iconic password method had a bigger proportion π_1 than the proportion π_2 of the binomial distribution associated with the character password method. In other words, it may not be concluded that iconic passwords are better than character passwords.

3.2.3 Conclusion

Although it is not possible to conclude that the iconic method gives better results than the character method because of the results obtained with the binomial analysis, the conclusion that when users are assigned a password, iconic passwords performs better than character passwords is still valid (from the normal and the paired analysis). When users are assigned their passwords, humans use two elements to memorize their passwords

- Just the succession of characters or icons
- A strategy that the user develops when he receives the assigned password

The goal was, based on the results of this experiment and based on the results of the previous experiment, to try to understand what are the determinant factors that play a role in the memorization of passwords. The assumption in building this model is that the first element, the simple memorization of the characters or icons plays a very small role in the memorization. This assumption is based on the observation of the way users remembered their passwords in this experiment (where they were assigned the password). Users were asked how they remembered their passwords and their answers in every case involved a strategy. No users tried to simply remember the succession of symbols. Therefore the results of this experiment can be explained by stating that iconic passwords enhance better strategies to remember passwords than character passwords do. This explanation makes sense. It seems indeed much easier to come up with an easy to remember story around icons than to come up with an easy sentence that matches the character password and that could be used to help the user to remember the password.

When users have the choice of the password, it is just the opposite. It is easier and more natural to come up with an easy to remember sentence and then from that sentence to build a password than thinking about a story and find matching icons. Therefore, according to the model, icons are not easier to remember than characters and the difference in performance should be related to the strategies these symbols enhance.

When users have their chosen password, characters enhance better strategies than icons would. When users are assigned a password, icons enhance better strategies than characters would.

These different elements are summarized in figure 3.1.

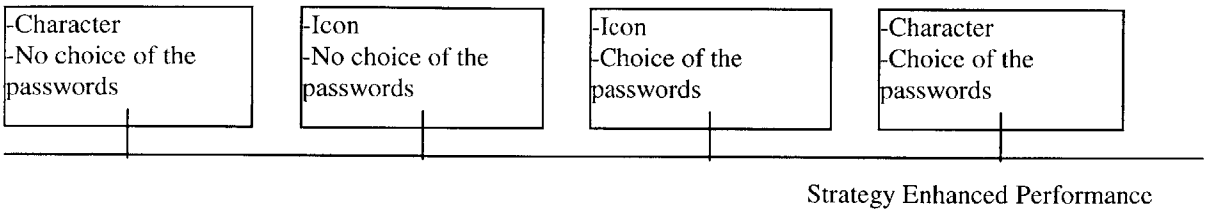


Figure 3.1: Strategy Enhanced Performance Representation

A way to check this model would be to look at the decrease of performance for one type of password when both the case when the user can choose his password and when the user cannot choose his password are considered. If this model is correct, an important decrease of performance for the character password method should be observed and a less important decrease of performance should be observed in the case of the iconic passwords.

3.3 Character Passwords

The goal of this analysis was to see if there is a significant decrease of performance of character passwords when we assign the user a password instead of letting him choose. This has some practical implications. Indeed, if there is no significant decrease of performance, then passwords could always be assigned because that would reduce security dangers and would not reduce the memory performance.

3.3.1 Normal Analysis

When users were allowed to choose their passwords, the following results were obtained:

$x_1 = 6.8125$ and $s_1 = 0.4031$ with $m_1 = 16$

When users were assigned their passwords, the following results were obtained:

$x_2 = 3.8889$ and $s_2 = 2.6321$ with $m_2 = 18$.

The Z statistic is 4.6515.

At a 5% significance level, the critical region is $(-\infty, 1.64)$ and at a 1% significance level, the critical region becomes $(-\infty, 2.32)$. The statistic is therefore outside the critical zone for both the 5% and the 1% level. The null hypothesis can therefore be rejected for both significance level and the conclusion is that the difference is statistically significant. In other words, the performance of character passwords decreases significantly when users are assigned their passwords rather than being able to choose them.

3.3.2 Binomial Analysis

Table 3.7 summarizes the results:

Table 3.7: Results of the Character Password experiment

Performance of character passwords	Perfect recollection	Imperfect recollection
User chooses it	13	3
User does not choose it	5	13

In this case, p_1=13/16 and p_2=5/18, and the *Z* statistic is 3.12. The critical region is (-∞, 1.64) at a 5% significance level and (-∞, 2.33) at a 1% significance level. In both cases, the statistic is outside the critical region and the null hypothesis can be rejected. Thus, it may be concluded that the performance of character passwords decreases significantly when users are assigned their passwords instead of being able to choose them.

3.3.3 Conclusion

In the case of character passwords, allowing users to choose their password improves performance. The difference in performance may be due to the fact that the strategy that users develop when they choose their password is much more powerful than the strategy they can develop when they cannot choose the password.

3.4 Iconic Passwords

The goal of this experiment was to see if there is a significant decrease of performance of the iconic password method when users are assigned a password instead of letting them choose it. According to the model, there should be a small decrease of performance but not too much because icons are well suited to enhance strategies even if the password is assigned.

3.4.1. Normal Analysis

When users were allowed to choose their iconic passwords, the following results were obtained:

$x_1 = 6.0625$ and $s_1 = 1.1236$ with $m_1 = 16$.

When users were assigned their iconic passwords, the following results were obtained:

$x_2 = 5.4444$ and $s_2 = 1.5424$ with $m_2 = 18$.

The Z statistic is 1.3454. At a 1% significance level, the critical region is $(-\infty, 2.32)$. Since the statistic Z is inside the critical region, the H_0 hypothesis cannot be rejected. At a 5% significance level, the critical region is $(-\infty, 1.64)$. The statistic Z is again inside the critical region and the H_0 hypothesis cannot be rejected. In other words, it may not be concluded that the performance of iconic passwords significantly decrease when users are assigned their passwords instead of choosing them.

3.4.2 Conclusion

It is therefore not possible to conclude that there is a significant difference between both distributions. This means that the two cases lead to passwords that enhance strategy of similar quality. This confirms the model. According to the model, there should not be a too much decrease in performance in the case where the user is assigned the password because it is not to hard to build a story around given icons. The only problem related to iconic passwords is that users tend to mix the icons and do not recall them in the right order. This does not happen with character passwords when users can choose their password because the strategy that that approach enhances is more robust. It is possible to mix two elements of a story but it is harder to mix two words of a sentence.

3.5 Spatial Memory

The goal of this experiment was to quantify the additional effect of spatial memory. In all the preceding experiments, users were shown a different screen when they were choosing their passwords and when they were restituting their password. The goal, here, was to eliminate the potential effect of spatial memory that would have disturbed the results. By showing users the same screen, a new parameter was added to improve memory performance: spatial memory. The experiment was incorporated in the following configuration:

Table 3.8: Spatial Memory Test Matrix

	Day 1	Day 2	Day 3
User 1	Character password	Iconic password	Char. /spatial password
User 2	Character password	Char. /spatial password	Iconic password
User 3	Char. /spatial password	Character password	Iconic password
User 4	Char. /spatial password	Iconic password	Character password
User 5	Iconic password	Character password	Char. /spatial password
User 6	Iconic password	Char. /spatial password	Character password

The experiment had 18 subjects, thus each configuration was tested three times.
The idea was to compare the results of the case when users were asked to remember a random password of characters with a different screen when they chose the password and when they recalled it and the similar case when users were shown the same screen.

3.5.1 Results

3.5.1.1 No Spatial Memory

The following results were obtained:

- 5 users got the right passwords (7 characters in the right order)
- 4 users got 5 characters at the right place
- 1 user got 4 characters at the right place
- 3 users got 3 characters at the right place
- 2 users got 1 characters at the right place
- 3 users got 0 characters at the right place

3.5.1.2 Spatial Memory

The following results were obtained:

- 7 users got the right passwords (7 characters in the right order)
- 5 users got 5 characters at the right place
- 3 user got 4 characters at the right place
- 3 users got 3 characters at the right place

3.5.2 Analysis

3.5.2.1 Normal Analysis

When the users were shown the same screen and could use their spatial memory, the following results were obtained:

$x_1 = 5.2778$ and $s_1 = 1.5645$ with $m_1 = 18$

When the users were shown different screens, the following results were obtained:

$x_2 = 3.8889$ and $s_2 = 2.6321$ with $m_2 = 18$

The Z statistics is 1.9245.

At a 1% significance level, the critical region is $(-\infty, 2.32)$. Since the statistic Z is inside the critical region, the H_0 hypothesis cannot be rejected. At a 5% significance level, the critical region is $(-\infty, 1.64)$. Since the statistic Z is outside the critical region, the null hypothesis can be rejected. It may therefore be concluded that there is a significant difference between both distributions at a 5% level. In other words, at a 5% level, spatial memory has a significant impact.

3.5.2.2 Paired Analysis

Table 3.9 summarizes the results of the paired comparison between the performance of the character passwords with and without spatial memory.

Table 3.9: Results of the Paired Comparison between Character Passwords with and without Spatial Memory

Performance	Character password (Spatial memory)	Character password	Difference D_i
User 1	7	7	0
User 2	7	7	0
User 3	7	7	0
User 4	7	5	2
User 5	7	5	2
User 6	7	5	2
User 7	7	4	3
User 8	5	7	-2
User 9	5	1	4
User 10	5	5	0
User 11	5	3	2
User 12	5	3	2
User 13	4	7	-3
User 14	4	3	1
User 15	4	0	4
User 16	3	0	3
User 17	3	0	3
User 18	3	1	2

For the given comparison, $n = 18$, $D = 1.39$ and $S = 1.91$. Thus the T statistic is 3.09. At a 5% level, the critical region is $(-\infty, 1.74)$. Since the statistic T is outside the critical region, it is possible to conclude that the space memory has a significant impact. This conclusion doesn't change at the 1% significance level is considered. The critical region is then $(-\infty, 2.567)$ and the statistic T is again outside the critical region. It may therefore be concluded that spatial memory has a significant impact.

3.5.3 Conclusion

The purpose of this experiment was to quantify the effect of spatial memory. It was pretty evident intuitively that spatial memory would increase the performance of a password method but it was interesting to see more formally what would happen and see if statistically significant results could be obtained. The experiments could be ameliorated by doing the following. In this experience, spatial memory was realized by using the same screen when users were asked to choose their passwords and when users were asked to restitute them. It would be interesting to see if the effect of spatial memory would increase when users actually type their password on a real keyboard a few times rather than just visualizing the different characters.

CHAPTER 4

4 SUMMARY AND CONCLUSIONS

This thesis addressed the issue of user authentication by computers, and in particular password-based authentication. If the administrator allows users to choose their own password, then they can use the guidelines to pick something easy for them to remember but difficult for others to guess. Nevertheless, since the users select their passwords, they might put the entire system in danger by not selecting a sufficiently obscure password. Thus, in some cases, the administrator might be required to assign passwords because they cannot tolerate the possibility that a user might select a password that is easily guessed or deciphered.

The goal of this thesis was to determine the relative benefits of iconic passwords versus character passwords when passwords are assigned and selected, and the impact of spatial memory. This goal was achieved through two experiments. The first experiment investigated the relative benefits of iconic passwords and spatial ordering when passwords are assigned, while the second experiment investigated the relative benefits of iconic passwords when users are allowed to select their own passwords. The results of these experiments were used to determine (a) the relative benefit of icons versus characters when passwords are assigned, (b) the relative benefit of icons versus characters when passwords are selected, and (c) the impact of spatial ordering on the ability of users to remember passwords.

Results indicate that

- Iconic passwords are better than character passwords when the user is assigned a password
- Character passwords are better than iconic passwords when the user selects a password
- Allowing users to choose their passwords (instead of assigning the password) has no significant impact on the memorization of iconic passwords
- Allowing users to choose their passwords (instead of assigning the password) has a significant impact on the memorization of character passwords
- Spatial memory has a significant impact on the memorization of passwords

These results have some practical implications for systems that require high security where administrators cannot tolerate the risk of a user selecting an easily decipherable password and are required to assign passwords. In most systems, i.e. systems where administrators allow users to select their password, character passwords appear to be better than iconic passwords.

One possible explanation for the better memorization of users in the case where users selected character passwords is their familiarity with characters. Possible future studies should therefore investigate the relative performance of users using icons and character passwords after extended familiarization and training with iconic passwords.

Bibliography

[1] Block Ned *Imagery* The MIT Press, 1981

[2] Caenepeel S. *Inleiding in de Waarschijnlijkheid en de Statistiek.* Vrije Universiteit Brussel, 1994

[3] Kanji, Gopal K. *100 Statistical Tests.* SAGE Publications, 1993

[4] Kaufman C., Perlman R., and Speciner M. *Network Security, Private communication is a public world.* Prentice Hall, 1995

[5] McCauley-Bell Pamela, Hansman John R., and Rodriguez Mario A. *An Exploratory Survey to Evaluate the Impact of Human Error in Information Security* MIT, 1999

[6] Norman D.A. *The Psychology of Everyday Things.* New York, 1990

[7] Norman D.A. *Things that make us smart.* Addison Wesley, 1993

[8] Parkin A.J. *Memory* Oxford, 1993

[9] Preece Jenny, Rogers Yvonne, Sharp Helen, Benyon David, Holland Simon, and Carey Tom *Human-Computer Interaction.* Addison-Wesley, 1994

[10] Waern Yvonne Cognitive *Aspects of Computer Supported Tasks* Chichester, 1989