Gkarafli, S. & Economides, A. A. (2010). **An experimental survey and comparison of proof by knowledge authentication techniques**. *International Journal of Applied Research on Information Technology and Computing*, Vol. 1, Issue: 3, pp. 240-271

An experimental survey and comparison of proof by knowledge authentication techniques

Stamati Gkarafli and Anastasios A. Economides

Information Systems Department, University of Macedonia,
Egnatia 156, Thessaloniki, 54006 Greece

Abstract. "Proof by knowledge authentication techniques" include traditional text passwords, visual passwords and graphical passwords. The paper compares these three techniques using an experiment. A total of 100 users participated in the experiment. After getting informed about the new authentication methods, users created their own text, visual and graphical passwords. Then they tried to confirm them correctly and finally they answered in a comprehensive questionnaire that we have created. Analysing those data, we concluded that the text passwords that were created are predictable and very vulnerable to attacks. Visual passwords attracted users very much, especially those that are over 45 years old, although the passwords that they made are really easy to be cracked. Graphical passwords did not impress very much many of the users and especially men, at the beginning of the process. However, at the end they were characterized as a very friendly method, mostly from women. Furthermore, the created graphical passwords were difficult, memorable and above all very safe.

Keywords: user authentication methods, text passwords, visual passwords, graphical passwords

1 Introduction

This paper focuses on the authentication problem, which is the process of confirming or not the user's identity. According to Jansen (2003) authentication techniques are separated into tree different categories:

- **Proof by knowledge** – techniques based on specific information that an individual has. If the user gives this information then he takes the right to enter the system (e.g. PIN, text-passwords).
- **Proof by property** – techniques based on a certain property that the user has and which can confirm his identity (e.g. fingerprint verification, voice verification, iris scanning).
- **Proof by possession** – techniques based on the possession of an object that an individual has. If the user gives the object, then he confirms his identity and enters the system (e.g. smart cards, digital certificates).

Nowadays, the most widespread authentication techniques are PIN and text-passwords, which are proof by knowledge techniques. Besnard et al (2004) presented passwords as the main threat in the security mechanism, as users cannot remember easily their passwords and need external memories. Moreover, users rarely choose passwords that are both hard to guess and easy to remember (Davies, 2005). As a result, passwords are often badly selected and therefore more easily guessed or cracked, forgotten, written down, shared with others, infrequently changed and kept the same for multiple systems. To show the severity of the problem, a security team in a large company cracked and identified about 80% of the passwords (Gilhooly, 2005). Also, Klein (1990) reported that 25% of 14000 passwords were cracked using a dictionary of only 3 million words. So, we can assume that these methods have become very unsafe. Despite their popularity, it is obvious that text passwords and PINs can cause serious problems to the users, which are summarized below:

- People choose passwords that are short in length, or easy to remember
- Many times, people write passwords down, or share them with others, in order not to forget them
- They use the same, or almost the same passwords for different applications
- Text passwords are very vulnerable to *"dictionary attacks"*. Because of the difficulty in remembering random characters in order to create a memorable and safe text passwords, many users tend to choose a common word, name, or date. Unfortunately, several tools have been

constructed that automatically crack those passwords, by checking all those words that are frequently used, and are in the dictionary.

2 Visual and Graphical Passwords

Considering the previously mentioned problems which make text passwords really unsafe and dangerous, researchers not only tried to find smart methods to create safe text passwords (Yan et al., 2004), but also invented visual and graphical passwords. Both have a lot of advantages that help users get over these problems (Angeli et al., 2005; Bolande, 2000; Suo et al., 2005):

- It is much easier for someone to remember pictures than a sequence of characters
- Pictures are independent from the language of each user
- Especially in graphical passwords, password space is very large
- Dictionary attacks are infeasible, as corresponding dictionaries do not exist yet, and it is very difficult to be constructed considering the large password space
- As a result automated attacks are very difficult to take place.

However, as Renaud and De Angeli (2004) refer, the main disadvantage that visual and graphical passwords have is the *shoulder surfing problem*. The shoulder surfing problem is when someone is watching over user's shoulders, during the login process (Sobrado and Birget, 2002; Tari et al., 2006). For example, this may happen when someone observes the keyboard in an ATM machine, when the user enters his PIN number. So, even if visual and graphical passwords are very hard to be guessed, a person who observes the login process may figure out the personal password. Next, let describe these new visual and graphical passwords.

2.1 Visual Passwords

Visual passwords refer to passwords that are created by selecting a sequence of pictures. Instead of remembering a sequence of numbers, characters or even symbols, users must remember a sequence of images (Jansen, 2003; Perrig and Song, 1999). Based on this idea, there was developed a number of commercial products that we will refer in the text below.

Real User Corporation developed a product named *"Passfaces"* (Real User Corporation, 2006; Renaud and De Angeli, 2004), where the user must select four images of human faces, in a specific order, from a database, as his secret password. Similar to this is *"Story Scheme"* (Davies at al., 2004). The only difference is that the images are not just human faces, but also everyday objects, animals, food, sports, cars. Dhamija and Perrig developed *"Déjà Vu" Scheme* (Dhamija and Perrig, 2000), where the user creates his *"image portfolio"*, by selecting a set of p images out of a larger set. During the login process, the user has to recognize the images that belong to his portfolio and click on them. The images here are based on Bauer's (1998) *Random Art* which can generate random abstract images, based on an initial seed. Jansen et al. (2003, 2006) developed *"Picture Password"* where images are grouped into different categories according to their theme and the user has to choose one of these themes and afterwards a sequence of images from this theme. "*Passlogix"* (Passlogix, 2006) is based on Blonder's (1995) idea who proposed that during authentication, the user must click on several locations in an image. Here, the user must click on a sequence of items in the image he sees on his screen in order to create his password. An extension of this idea is the *"Passpoint"* system developed by Wiedenbeck et al. (2005a, 2005b, 2005c). In this implementation, the user is able to make a click at any place on an image, and not only on a certain object, based on the invisible boundaries around each pixel.

2.2 Graphical Passwords

In this sub-section, we explore and analyze *graphical passwords*. Here, the user has to draw his personal design, which will be his secret password, to enter the particular system. More precisely, we examine the *DAS* (Draw-a-Secret) scheme and its extension which is *Multi-grid Passwords*.

DAS was proposed by Jermyn and allows the user to draw a simple design on a $G \times G$ grid (Jermyn et al., 1999), which will represent his password. Figure 1 depicts a 3×3 grid. The design that was drawn is mapped to a sequence of coordinate pairs, by making a list of the cells through which the

drawing passes in the correct order and separated by pen-up events, when the user raises his pen and continues from another point. The list is (1,2), (1,1), (2,1), (2,2), (3,2), pen-up, (2,3), (1,3).

Nali and Thorpe (2004) made their own survey and proved that users may draw passwords with predictable characteristics, which means centered or symmetric. These characteristics can reduce very much the password space and help attackers in creating dictionaries (Oorschot and Thorpe, 2005; Thorpe and Oorschot, 2004). Based on this remark, Birget et al. (2003) referred problems with the DAS scheme because of uncertainty in the clicking regions. Alexiadis et al. (2006) and Chalkias et al. (2006) made an extension to the DAS scheme and proposed *"multi-grid passwords"*, where nested grids are used in the initial one (Figure 2). With multi-grid passwords the users are able to create more complicated passwords and more memorable, while they have more points of focus to do their draw. So the user does not need to make his design in the center of the grid or symmetrically.

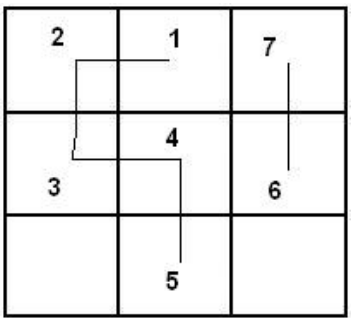

Figure 1: DAS Scheme.

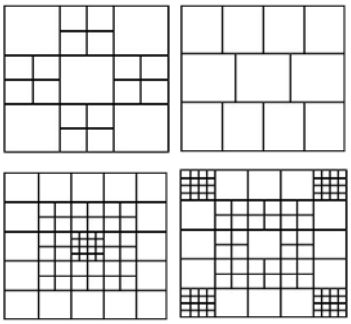

Figure 2: Multi-grid passwords (Alexiadis et al., 2006).

Weiss and Del Luca (2008) proposed PassShapes. In this system users authenticate themselves to a computing system by drawing simple geometric shapes constructed of an arbitrary combination of eight different strokes. Everitt et al. (2009) found that the frequency of access to a graphical password, interference resulting from interleaving access to multiple graphical passwords, and patterns of access while training multiple graphical passwords significantly impact the ease of authenticating using multiple facial graphical passwords. Chiasson et al. (2009) compared the recall of multiple text passwords with recall of multiple click-based graphical passwords. In a one-hour session (short-term), they found that participants in the graphical password condition coped significantly better than those in the text password condition. Similarly, Ozok and Holden (2008) compared alphanumeric and graphical passwords. Johnson and Werner (2008) found that passcodes are more memorable than alphanumeric passwords over extended retention intervals. Finally, various classification systems of graphical passwords were proposed (Hafiz et al., 2008; Por and Lin, 2008).

3 Related Work

Since security is a very important issue these days, several researchers have worked on the new authentication methods that we have described, with the aim to compare them with the widely known methods and to determine at what degree they can be accepted by users.

Irakleous et al. (2002) revealed that almost all people today use passwords for their every day needs. They found that 59% of the participants have 2 – 5 passwords, while about 15% have more that 10. Combining this, with the fact that 65% of them use at least one password daily, helps us understand the importance of password safety. Also, counting the number of successful authentications they found that 70% of the users confirmed successfully their passwords, something that makes more urgent the need for finding new authentication methods.

Tribelhorn (2006) showed that safety is a matter that puzzles many users. Examining the elements that the passwords are comprised of, they found that 58% of users use just numbers, 15% use also other symbols, while 27% have passwords of more than 8 characters, something that reveals that many people try to have at least one password safe, for their most important application. Nevertheless, even though they consider security as a major issue, 65% of them never change their passwords for security reasons.

Gaw et al. (2006) worked on security issues in online accounts. Their study indicated that most users have very few unique passwords and far more accounts that are multiplied every day. In order to

remember their passwords easily, they reuse their passwords without any transformation, making the whole process really vulnerable to attacks and not secure at all.

All these, lead to the fact that new authentication methods had to be invented, that is visual and graphical passwords. According to Jansen (2004), visual passwords are not really safe because users tend to select a small number of images. Comparing visual with text passwords, he found that people using 4-6 characters in their text password, select 4 images. Correspondingly, people that use 8-9 characters (a safe enough text password) select 6 images, creating this way a visual password easy to be cracked.

Many applications that are based on the image selection of visual passwords were created. At the same time, many researches were conducted, with the aim to reveal the advantages and drawbacks of each scheme:

- Kim and Kwon (2004) compared the "memorability" of visual passwords with respect to the different theme that the images have. They found that having images of known faces for each user, results to create much more memorable passwords than having images of random faces or landscapes. The amazing thing here is that even if the user selects 15 images with known faces, he is able to remember them in the correct order and login successfully, even after a week.
- Davis et al. (2004) compared the kind of images that men and women select in the Story Scheme. They found that females choose animals twice as often as men did, while males choose women twice as often as females did. Also the theme that females prefer more than others is food, in contrast with males who prefer nature and sports.
- Dhamija and Perrig (2000) worked on the Déjà vu scheme, and revealed that users spend much time to create their portfolio and make a login, especially if they use the random art technique. The positive result here is that after one week, that participants were tested again, users that use PINs and text passwords made more unsuccessful logins, than those that use visual passwords with the random art technique or simple photos.

Because visual passwords have drawbacks that make passwords really unsafe, graphical passwords were invented. Wiedenbeck et al. (2005) concluded that graphical passwords are much more time-consuming than alphanumeric and that until they get used with them, the percentage of unsuccessful logins is bigger. What confirms that graphical passwords is a very good method, is that after some practice, the percentages are reversed, as users create graphical passwords that are more difficult to be cracked than the text ones.

Goldberg et al. (2002) further examined graphical passwords. They concluded that many users make drawings that look identical to the original, but do not really match due to stroke order, stroke direction, or the number of strokes. The encouraging thing here is that users have the best results and many of them make successful logins, after some practice. This is confirmed also by the fact that almost 72% of them agreed that this method is easier to remember than the traditional PINs and text passwords.

Nali and Thrope (2004) conducted a survey which mainly examines the drawbacks of graphical passwords. The survey showed that 86% of participants drew a centered or approximately centered password, 45% of the passwords were totally symmetric and 29% were invalid.

Chalkias et al. (2006) proposed a multi-grid password scheme, comparing the results between non-technical inclined people with those that were well-informed. They found that 66% of non-technical users and 80% of technical users confirmed correctly their text passwords. In the DAS scheme the results were a bit lower, while the corresponding percentages were 47% and 60%. They also found that 80% of non-technical users and 67% of technical users drew centered drawings. In the multi-grid password scheme that was proposed, the situation is a bit different. The percentages of centered passwords are much lower (46% for non-technical users and 33% for technical users), something that testifies the fact that with the multi-grid scheme participants are able to create more difficult passwords and as a result less vulnerable to attacks.

All these surveys have two basic characteristics that must be referred in order to specify better the aim of our paper. Firstly, each survey is based on a new authentication method that is proposed. As a result, the authors made a comparison of the visual or graphical scheme that they propose, with the text passwords that exist today. Secondly, we have to point out that the number of users that participated in these surveys was very small (up to 40 users, while in most researches there were tested about 20 users), and that all users were up to 25 years old, as the surveys were conducted in schools, universities or colleges. The last two observations may be considered really serious drawbacks, as they may lead to insignificant results statistically.

Our experiment makes an extensive comparison among visual passwords, graphical passwords and the text passwords that are already in use. In our experiment, users created and confirmed their own passwords. Then, they answered to a comprehensive questionnaire. This way, we examined every basic

characteristic of all three methods, finding out what are the advantages that each one can offer. Moreover, in our survey, we tried to be more objective, with the aim to have better and more valid results. For this reason 100 users were participated from the age of 18 to 60 years old. Our basic purpose was to inform them about the new authentication methods (visual and graphical passwords), compare them with the text passwords, find the advantages that make them better and mostly determine at what degree our society will be able to change its habits and accept a new different idea.

4 Methodology

4.1 Questionnaire – Applications

In order to conduct our survey, we had to create a comprehensive questionnaire to obtain users' opinion and also make them create their personal passwords.

Our questionnaire is a completely new questionnaire which consists of 23 multiple choice questions and one last question where users can report their personal opinion or whatever they may notice during the whole process. More precisely, the key elements of the information that were collected with the questionnaire are summarized below and are the following:

- what do users plan to remember their passwords
- if they change passwords for security reasons, or they use the same password in many applications
- what kind of passwords they use (their characteristics)
- if they had ever heard about visual and graphical passwords or any other authentication method before
- if they are positive in using visual and graphical passwords
- what is their opinion about visual and graphical passwords in terms of security level, memorization, friendliness, time-consumption and overall liking.

From the other side, we also simulate on paper, the application where users would be able to create their own text, visual and graphical passwords and confirm them. We did the whole process on paper and not in a computer in order to control more easily the whole process and make it less time consuming, as the number of our participants is quite big and they were located in various places.

Combining the answers of the questionnaire with the personal passwords that users would create and their successful or unsuccessful confirmation, we would find out if users in our country are able to accept the new and safer authentication techniques and change their habits about using text passwords to login a system.

4.2 Participants

As we had already referred, 100 people were participated in the survey. Those people already knew the use of PINs and text passwords from their everyday experience. There were included males and females in the age of 18 to 60 years old.

More precisely, the sample included 49 men and 51 women that were divided into 3 categories according to their age: 59 users between 18 and 30 years old, 20 users up to 45 years old, and 21 users between 46 and 60 years old. Younger participants were students or post graduated students in the University of Macedonia (Thessaloniki), in the Aristotle University of Thessaloniki and in the TEI of Larissa. The elder ones were found in the places that they work. They were teachers in schools and Universities and people that work in public services, in the private sector, in manufactures and factories. All these participants were found in the cities of Thessaloniki and Larissa.

The most encouraging thing was that all persons were willing to participate in the study. This was evident, after introducing them the previous scientific results about the security of these authentication techniques.

What we have to mention here is that it was very hard and time-consuming to find all the users that participated in the survey and especially the elder ones that do not belong in a class. So, the whole process of collecting users' answers took almost three months, as we had to repeat it in schools, Universities and users' workplaces. Especially, in the users' workplaces, we repeated the whole process separately to 3 - 4 users, as it was not practical to find more people totally free at the same time.

4.3 Procedure

In order to accomplish our experiment and survey, we went through seven stages: 1) lecturing about passwords, 2) passwords' creation, 3) discussion, 4) passwords' confirmation, 5) answering the questionnaire, 6) analysis of passwords' creation and confirmation, and 7) analysis of users' answers.

At the first stage, we gave a short seminar (as many of them were at their work) to the participants about visual and graphical password explaining their main concept, the problems that they solve, what their advantages and disadvantages are, and how a user can create such passwords and login a system.

After understanding all these points, users had to create their own text, visual and graphical passwords. So, each one acquired a piece of paper, just like the one in Figure 3, where he had to create:

- a text password of more than 4 characters
- a visual password of more than 4 pictures in a particular order, by putting numbers in the corresponding picture, and
- a graphical password, by drawing a design in a 5 × 5 grid, going through more than 4 cells.

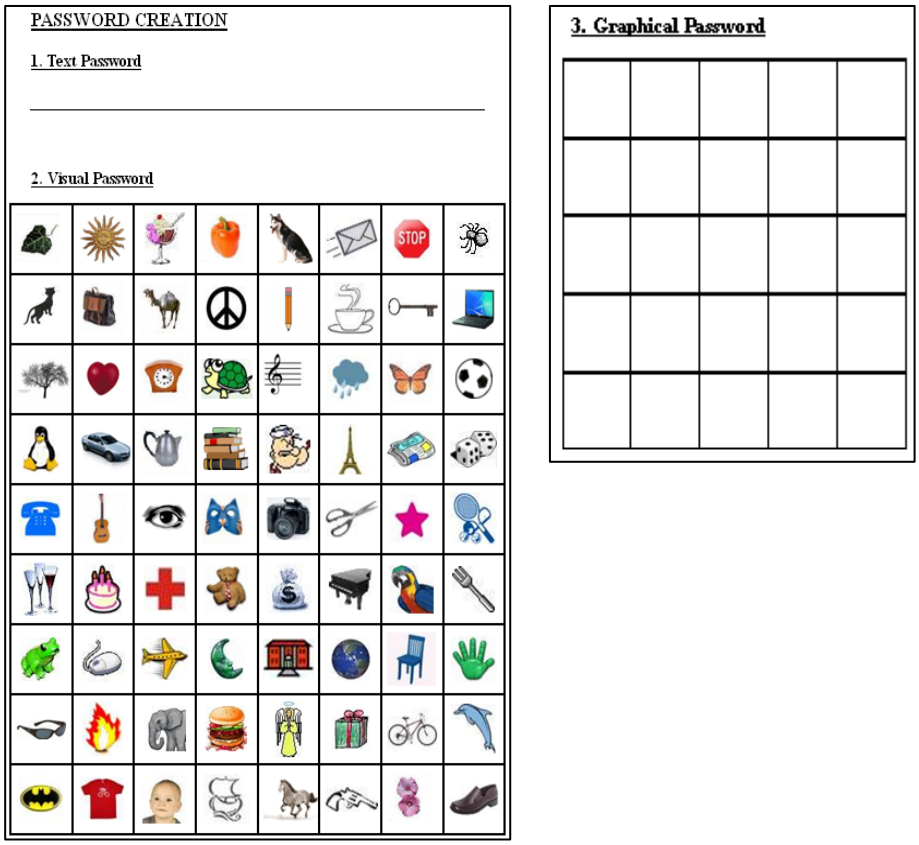

Figure 3: The form where users had to create the text, visual and graphical passwords.

After finishing this process, users spent about two hours before moving to the next stage. During these hours, participants were able to discuss anything they would like about passwords, security and the experiment itself, or get on with their work if they were in their workplace. We introduced this third stage for two reasons. The first reason was to help users place all the queries they had about visual and graphical password, and understand their use and their advantages in comparison to the traditional text passwords. The second reason was to spend some time before password confirmation. So, we engaged their mind with something else, before moving to the next stage.

At the forth stage, users had to confirm correctly the three passwords that they created. So, another piece of paper was given to them. This piece of paper was similar to the previous one but the pictures for the visual passwords were not at the same place as before (Figure 4).

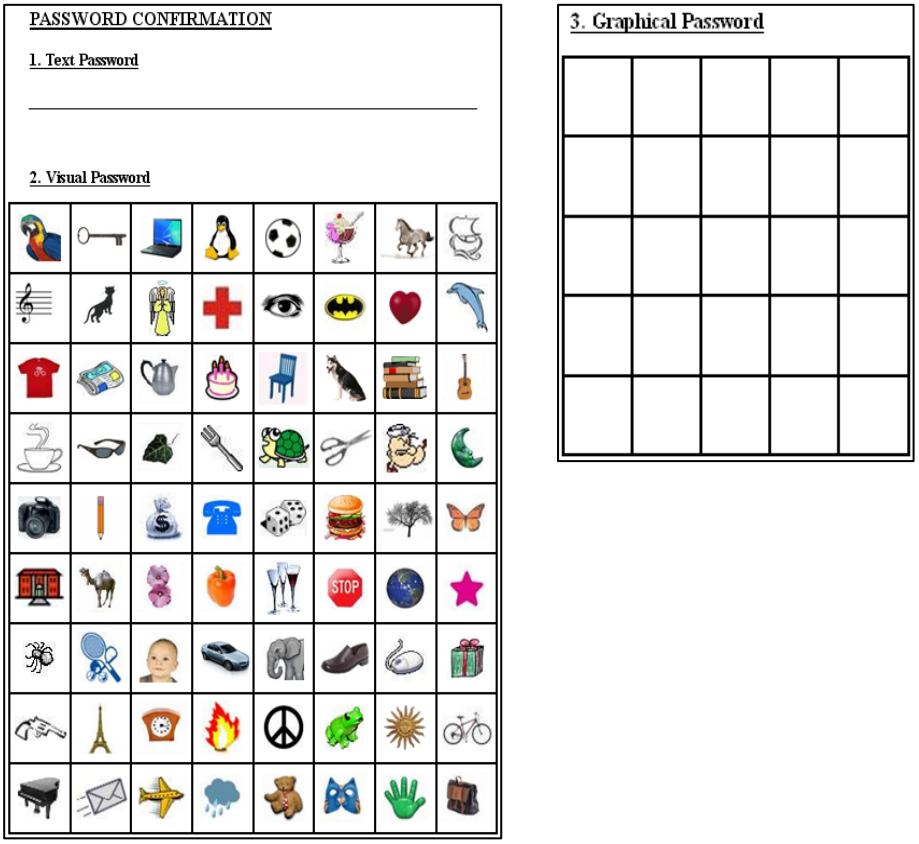

Figure 4: The form where users confirm their secret passwords.

After trying to confirm their passwords, users proceeded to the fifth stage of the process. At this point all the participants were asked to complete the questionnaire that was given to them in order to determine their personal opinion.

Finally, we analyzed the passwords that were created, their confirmation, and users' answers to the questionnaire. Next, we present the results.

5 Results

In this section, we present the results of the survey taking into consideration our observations during the experiment in creating, using and confirming text, visual and graphical passwords. We present the results in five categories: 1) problems with PINS and text passwords, 2) alternative authentication methods, 3) comparison among the three methods, 4) successful confirmation, and 5) difficulty of each method.

5.1 Problems with PINs and text passwords

In this section we investigate the problems associated with PINs and text passwords which are the authentication techniques that are used today. We begin by examining how many characters people use to create their passwords. 50% of participants indicated that their passwords are comprised of 5-8 characters, 41% of 4 characters, and only 9% of 8 or more characters, which can be considered as a difficult password, hard to be cracked (Figure 5). These results would be characterized satisfactory if the characters were not only numbers. Unfortunately, 49% of the created passwords consist of just numbers (Figure 6), something that makes them really vulnerable to an attacker.

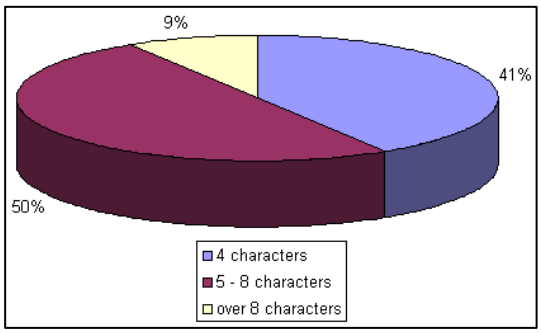

Figure 5: Number of characters in a text password.

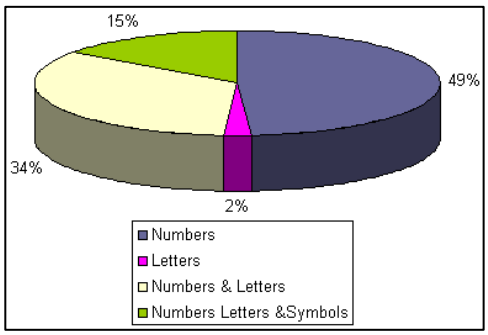

Figure 6: The kind of characters that text passwords are consisted of.

An encouraging result is that 15% of the participants do not use only numbers to their passwords but also letters and symbols. From those highly cautious users, 74% is under 30 years old, proving that more and more young people understand how important is to have a safe password that is not vulnerable to any attacker (Figure 7).

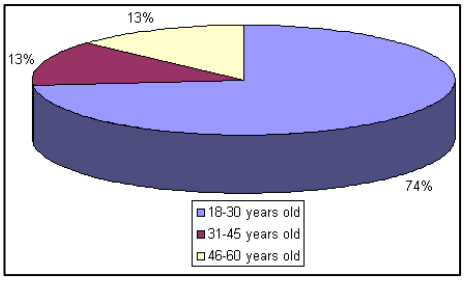

Figure 7: People that have passwords which are consisted of numbers, letters and symbols, according to their age.

Next, we found out that users are afraid of forgetting their passwords and not having any hope to find them again. So, they tried to find out methods that will help them if they face such a situation. Apart from trying to remember their passwords, they share them with other people (7%), write them down (34%), or use something very familiar to them (e.g. special dates, names) (33%) in order not to forget it (Figure 8). A respectable 78% of the participants tend to use the same or almost the same passwords to different applications (Figure 9). So, we can understand how hard is for someone to deal with all these passwords.

In order not to forget or mess up their passwords, users create one password for each application, and 81% of them never change it. However, an unchangeable password is a really vulnerable password to anyone who would try to make an attack. So, researchers tried to find out new easily memorable methods to authenticate a system. Next, we analyze these methods.

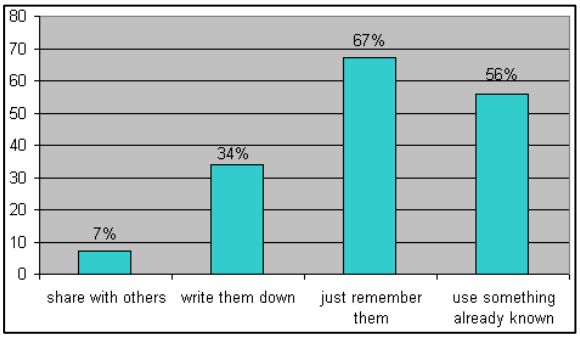

Figure 8: Methods (if any) to not forget passwords.

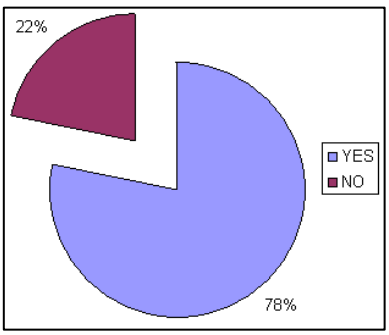

Figure 9: Users tend to use the same or almost the same passwords for different applications.

5.2 Alternative authentication techniques

Considering the problems presented above, it was inescapable that new alternative methods for authentication were needed. The following five main verification methods are not unknown to the participants (Figure 10):

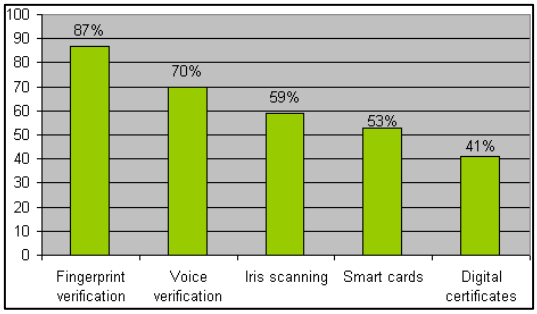

Figure 10: Knowledge of other authentication methods.

- **Fingerprint verification:** biometric identification by automatically scanning a person's fingerprints electronically
- **Voice verification:** biometric identification by automatically scanning a person's voice
- **Iris scanning:** biometric identification by scanning the iris of the eye, as the structure of the iris is very distinctive
- **Smart cards:** a card similar to a credit card, but with a small built-in microprocessor that holds information about the cardholder
- **Digital certificates:** an electronic "passport" which is issued by a certification authority, such as Entrust and Verisign. It contains, among others, the name, a serial number, expiration dates and the digital signature of the certification authority, so that the recipient can verify that the certificate is genuine.

These methods are known to the users mostly from movies, as they do not actually use them. Fingerprint verification is the most known method (87%), followed by voice verification (70%), and iris scanning (59%). It is strange that the other two methods, smart cards and digital certificates, are not so widely known despite the fact that they are already in use along with fingerprint verification.

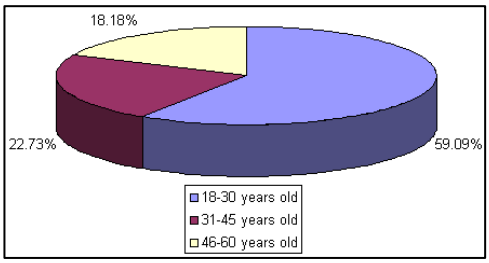

Figure 11: The age of users who had a previous knowledge about Visual and Graphical passwords.

Visual and Graphical Passwords were developed to create safer and more memorable passwords based on the fact that people are able to remember a sequence of images much easier than a sequence of characters. Since these methods were developed during the last years, only 22% of the participants knew visual and graphical passwords, while 78% of them had never heard anything about them.

It is also interesting that among the participants who already knew something about the new methods, nearly 60% are at the age of 18 to 30 years old, and just 18% between 46 and 60 years old (Figure 11).

Continuing our survey we present Figure 12 which examines whether users are positive in getting more informed about visual and graphical passwords and use them. It is encouraging that 83% of the participants are positive in using the new methods, and 17% of them are negative or really not very curious in identifying how useful these methods would be.

Finally, Figure 13 proves for one more time that there are no differences between men and women. More than 83% of both sexes are positive in knowing better the new methods.

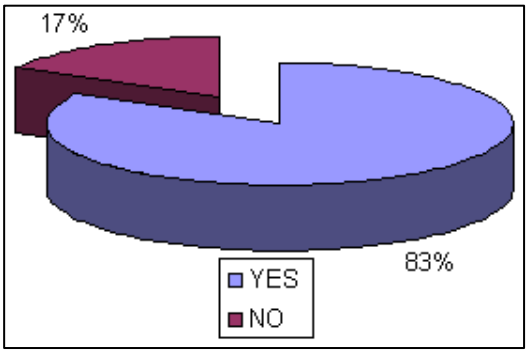

Figure 12: Users' acceptance about visual and graphical passwords.

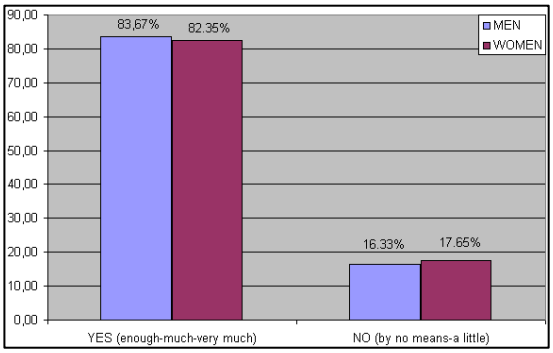

Figure 13: Users' acceptance about visual and graphical passwords based on their sex.

5.3 Analyzing text, visual and graphical passwords

In this section, we present the preferences of the participants regarding the various parameters of the three authentication methods (i.e. text, visual and graphical passwords). We asked the participants their opinion about the three methods with respect to the following six criteria: 1) easiness of remembering the passwords, 2) security, 3) easiness of understanding and learning how do they work, 4) user friendliness, 5) time consumption, and 6) aesthetics.

Let first examine which method is considered to be the most memorable. Since the users use PINs and text passwords every day, they are accustomed with them. So, they would consider text passwords as the most memorable one. Comparing the two new methods (visual passwords and graphical passwords) between themselves, 57% of the users considered visual passwords more memorable, while 43% considered that graphical passwords are more memorable (Figure 14). Discriminating between the two sexes (Figure 15), both men and women believe that visual passwords are more memorable. As for graphical passwords, more women (45.1%) than men (38.78%) believe that this is more memorable authentication method.

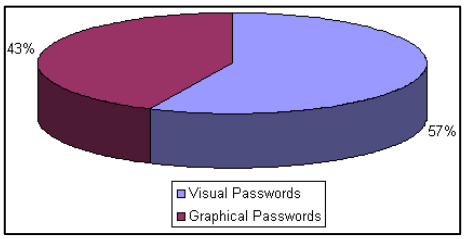

Figure 14: More memorable passwords.

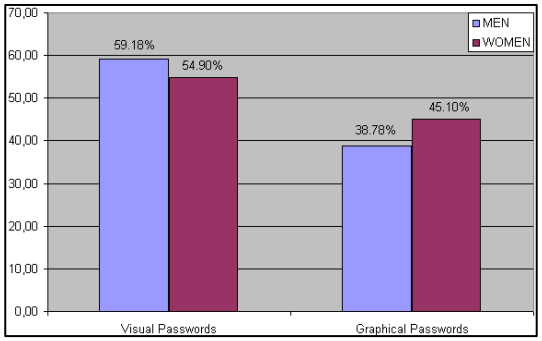

Figure 15: Men and women percentages of their belief about passwords are more memorable.

Let also examine which of the three authentication methods is considered to be the most secure. After explaining the new methods to the participants, 55% of them understand the advantages of graphical passwords and believed that this is the safest authentication method (Figure 16). However, a considerable percentage (28%) of the participants believe that the safest method is visual passwords, while 17% insists that text passwords do not have any problems and are very safe, ignoring everything that we had referred.

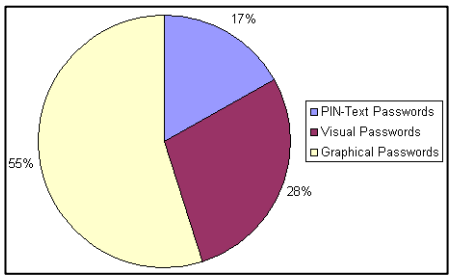

Figure 16: More secure authentication method.

It is worrying that 64.7% of the users who insist that the safest method is text passwords are young people under 30 years old. One reason that they may consider text passwords as the safest method is that when they refer to text passwords they have in their minds their own passwords of more that eight characters, that are comprised of numbers, letters and also symbols.

Next, we examine how easy is for someone to learn how the three authentication methods work (Figure 17). A large percentage of the participants considered really easy to understand and learn how to use the text (93%) and the visual passwords (91%). This percentage is smaller (75%) for the graphical passwords, since graphical passwords require more rules to be followed than the previous two methods.

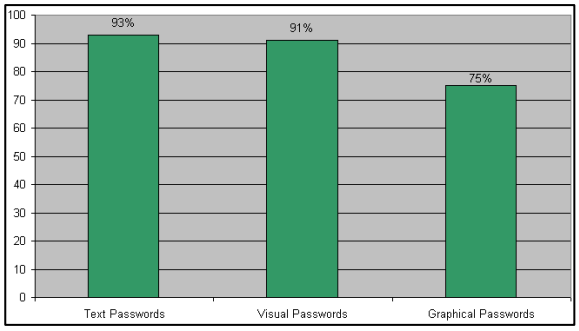

Figure 17: Convenience in learning how to use each method

Between the two genders, we can observe that the percentages of women who did not find any difficulties in learning how text and visual passwords are used, are bigger than those of men, while for graphical passwords we have an opposite situation (Figure 18). Also, based on Figure 19, we can refer that more difficulties are observed for users over 45 years old and only for the case of graphical passwords, while for the other two methods their percentages are really big.

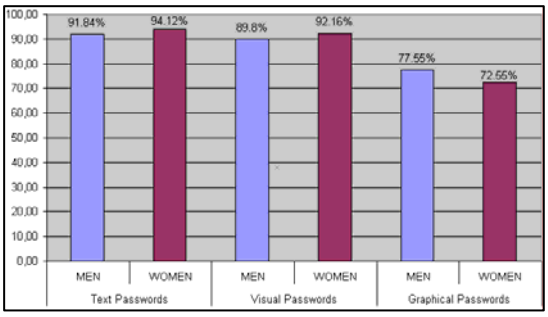

Figure 18: Convenience in learning how to use each method between the two genders.

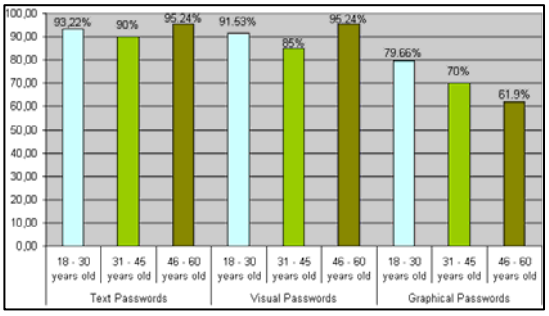

Figure 19: Convenience in learning how to use each method based on users' age

Let also examine how easy is for someone to use the three authentication methods. In Figure 20, we can see that text passwords are considered as the friendliest method (92%), followed by visual passwords (76%), and lastly by graphical passwords (71%). Thus, we remark that users accept more easily visual than graphical passwords, even though (as we will see later) they can create difficult and memorable graphical passwords, without any effort at all.

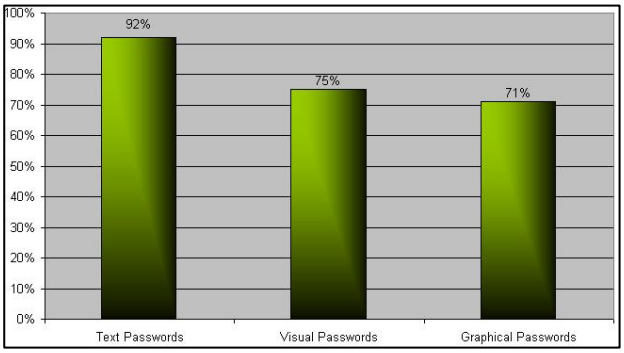

Figure 20: User friendliness of the three methods

Comparing men and women, we have to mention that more women than men find friendly the new authentication methods, while the percentages are opposite for text passwords (Figure 21). If we examine now the same situation based on users' age, we conclude in Figure 22. This Figure depicts that graphical passwords are considered as the most friendly method from users up to 30 years old (72.88%), while visual passwords are considered friendlier from the elder ones (46-60 years old).

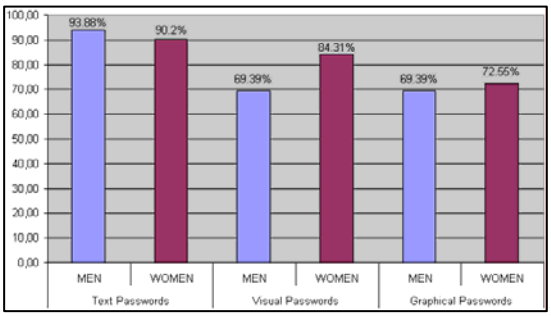

Figure 21: User friendliness of the three methods between the two genders.

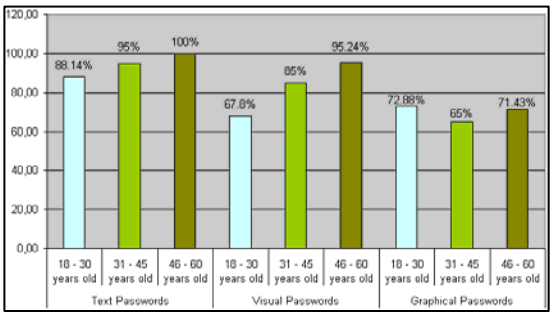

Figure 22: User friendliness of the three methods based on users' age.

Regarding the time that a user spends during login (Figure 23), most users believe that text passwords are not time-consuming at all (89%). As opposed to this, 46% of the participants believe that both visual and graphical passwords are rather time-consuming, for a different reason in each case. They believe that using visual passwords, a user may be lost in so many pictures and loose time trying to find his pictures even if he remembers his personal password. As for graphical passwords, their opinion does not change, because the user has to make up a personal draw and remember exactly the cells that he has passed through.

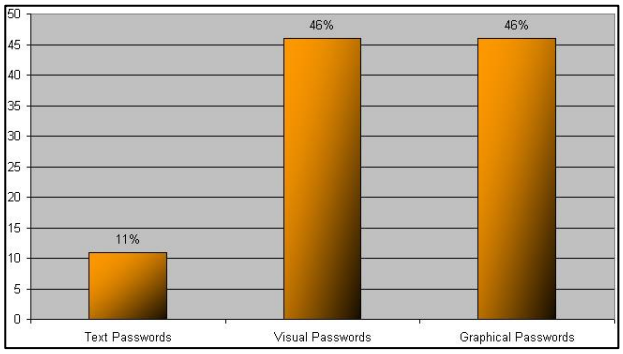

Figure 23: Are the three authentication methods time-consuming?

As far as for the two genders, more women (54.9%) than men (36.73%) believe that graphical passwords is a really time-consuming method (Figure 24). These percentages are reversed in visual passwords (37.25% for women and 55.1% for men), and men are now those who believe that visual passwords waste much of their time. Among the different ages (Figure 25), elder users are those who find more time-consuming all three methods. As a result, these percentages about visual and graphical passwords are a bit discouraging, even if users are really positive to change their habits and use them instead of text passwords that are unsafe.

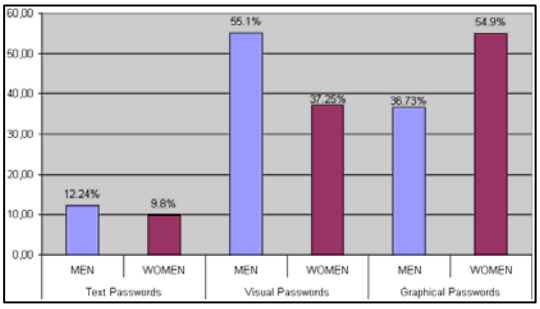

Figure 24: Waste of time for the three methods based on users' gender.

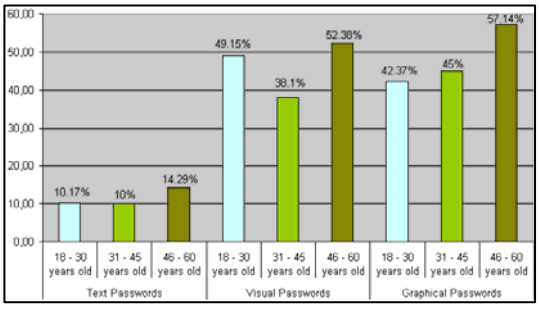

Figure 25: Waste of time for the three methods based on users' age

Finally, we examine what users think about the aesthetics of each method. According to Figure 26, most of them prefer aesthetically visual passwords (63%). Graphical passwords follow with a much

smaller percentage (25%). Obviously, most users consider that a sum of images, with different themes and colors, is much more impressive than a single draw, or even more than a sequence of characters.

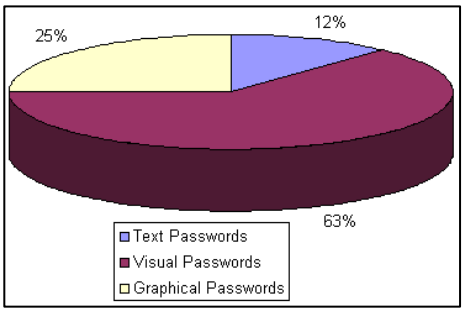

Figure 26: Better authentication method aesthetically.

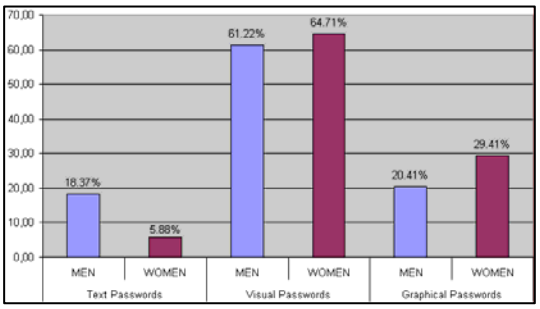

Figure 27: Better method aesthetically based on users' gender.

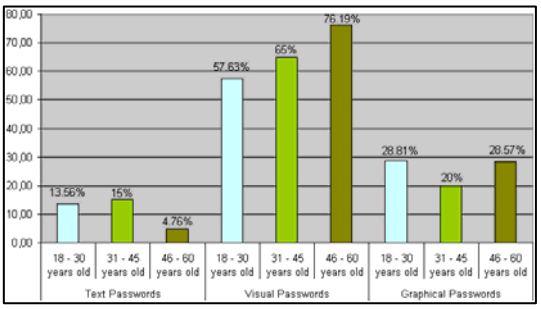

Figure 28: Better method aesthetically based on users' age.

If we have a look now on Figure 27 we can see that both visual and graphical passwords impressed more women than men, while the percentages for visual passwords are much bigger. This may be the explanation to the fact that women find the new methods friendlier than men. Examining Figure 28, we can observe that users from 46 to 60 years old were the ones that were impressed at most by visual passwords (76.19%), while the other percentages are smaller, but bigger than the corresponding percentages of the other two methods. Finally, we must point out that most of the users that prefer text passwords aesthetically (12%) are young people up to 30 years old (67%).

5.4 Confirming text, visual and graphical passwords

In this section, we present whether participants confirmed correctly the tree different personal passwords that they had created (Figure 29).

Almost all participants (97%) confirmed correctly their text passwords. This shows that people nowadays have become very familiar with PINs and text passwords.

A smaller percentage of the participants (86%) confirmed correctly their graphical passwords. We consider this as a good result since graphical passwords is a new method and a bit difficult to them according to their responses. Finally, fewer participants (82%) confirmed correctly their visual passwords. This situation seems to be a bit strange, especially if we consider that 57% of them believe that visual are more memorable than graphical passwords (Figure 14). From these users the 17.54% did not confirm correctly the visual password that they have made, even if they thought that this method was easier than the graphical. This percentage becomes even worse, if we take into account that most visual passwords consist of 4 or 5 images, a number that makes them really unsafe and vulnerable to attacks.

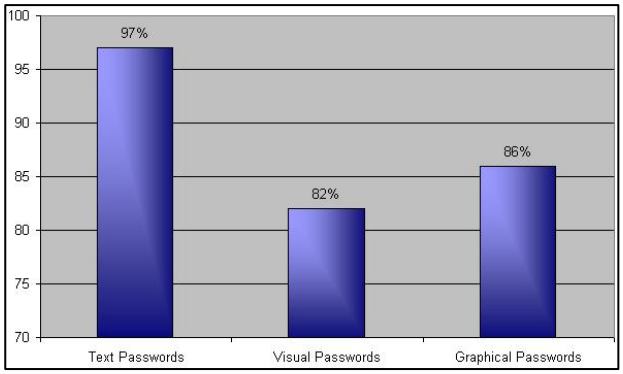

Figure 29: Successful confirmation of the passwords with the three authentication methods.

5.5 Grouping text, visual and graphical passwords based on their difficulty

In this section we classify each password type into three categories, in order to find out what kind of passwords do users chose in terms of the difficulty. So, the three categories are:

- Easy passwords
- Medium passwords
- Difficult passwords.

For this reason we will compute the ***"full password space"***, for each one of the three password types. The full password space includes all the combinations that can be performed, using the available elements, if the selection of each element is made randomly. In other words, the process we described is called *"brute force attack"*, as opposed to the *"dictionary attack"* where automated dictionaries are developed and used.

- **Text passwords**

In order to create a text password we have at our disposal 95 characters (52 letters uppercase and lowercase, 10 numbers and 33 symbols). So, the ***"full password space"*** for text passwords is 95^n, where $n \geq 4$ is the number of the characters in the password. Next, we compute the number of different combinations for various values of n.

$n=8 \rightarrow 95^8$ combinations $\rightarrow \approx \left(2^{6.57}\right)^8 \approx 2^{53}$
$n=7 \rightarrow 95^7$ combinations $\rightarrow \approx \left(2^{6.57}\right)^7 \approx 2^{46}$
$n=6 \rightarrow 95^6$ combinations $\rightarrow \approx \left(2^{6.57}\right)^6 \approx 2^{39}$
$n=5 \rightarrow 95^5$ combinations $\rightarrow \approx \left(2^{6.57}\right)^5 \approx 2^{33}$
$n=4 \rightarrow 95^4$ combinations $\rightarrow \approx \left(2^{6.57}\right)^4 \approx 2^{36}$

$\Rightarrow$

$n \geq 8$ Difficult password
n=7, n=6 Medium password
n=5, n=4 Easy password

We approximated the number of characters (95) as a power of 2, with the aim to make much easier the comparison with the other password types. Based on the number of different combinations, our personal knowledge about passwords, and the different opinions from other users and researchers, we classified text passwords into the three categories: i) difficult to be cracked for $n \geq 8$, ii) medium difficulty to be cracked for n=6 or 7, iii) easy to be cracked for $n \leq 5$.

- **Visual passwords**

In order to create a visual password in our experiment we can use $8 \times 9 = 72$ images. So the ***"full password space"*** here is 72^n, where $n \geq 4$ is the number of images selected in the password. As above we will compute the number of combinations for various values of n.

$n=9 \rightarrow 72^9$ combinations $\rightarrow \approx (2^{6.17})^9 \approx 2^{55}$

$n=8 \rightarrow 72^8$ combinations $\rightarrow \approx (2^{6.17})^8 \approx 2^{49}$

$n=7 \rightarrow 72^7$ combinations $\rightarrow \approx (2^{6.17})^7 \approx 2^{43}$

$n=6 \rightarrow 72^6$ combinations $\rightarrow \approx (2^{6.17})^6 \approx 2^{37}$

$n=5 \rightarrow 72^5$ combinations $\rightarrow \approx (2^{6.17})^5 \approx 2^{31}$

$\Rightarrow$

$n \geq 8$ Difficult password

$n=7, n=6$ Medium password

$n \leq 5$ Easy password

Based on the results about the text passwords, we classified visual passwords into the three categories: i) difficult to be cracked for $n \geq 8$, ii) medium difficulty to be cracked for n=6 or 7, iii) easy to be cracked for $n \leq 5$

- **Graphical passwords**

Finally, to create a graphical password we have $5 \times 5 = 25$ cells and one pen up event, i.e. 26 different choices. So the ***"full password space"*** is 26^n, where $n \geq 4$ is the number of cells and pen up events to each password. For one more time, we compute the number of combinations for various values of n.

$n=12 \rightarrow 26^{12}$ combinations $\rightarrow \approx (2^{4.7})^{12} \approx 2^{56}$

$n=11 \rightarrow 26^{11}$ combinations $\rightarrow \approx (2^{4.7})^{11} \approx 2^{52}$

$n=10 \rightarrow 26^{10}$ combinations $\rightarrow \approx (2^{4.7})^{10} \approx 2^{47}$

$n=9 \rightarrow 26^9$ combinations $\rightarrow \approx (2^{4.7})^9 \approx 2^{42}$

$n=8 \rightarrow 26^8$ combinations $\rightarrow \approx (2^{4.7})^8 \approx 2^{38}$

$n=7 \rightarrow 26^7$ combinations $\rightarrow \approx (2^{4.7})^7 \approx 2^{33}$

$\Rightarrow$

$n \geq 11$ Difficult password

$8 \leq n \leq 10$ Medium password

$n \leq 7$ Easy password

Correspondingly, we classified graphical passwords to the three categories: i) difficult to be cracked for $n \geq 11$, ii) medium difficulty to be cracked for n=8, 9, or 10, iii) easy to be cracked for $n \leq 7$.

Having analyzed the full password space for each password type, we will figure out on the difficulty to crack the passwords created by the participants.

Regarding text passwords, many participants (40%) use 8 or more characters in their passwords which correspond to difficult passwords (Figure 30). However, 34% of them use 4 or 5 characters, i.e. easy passwords. Figure 31 shows the classification of their text passwords into the three categories.

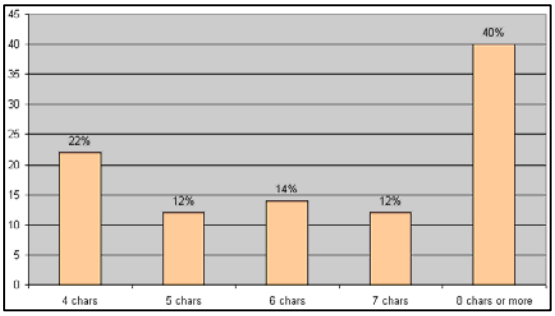

Figure 30: Number of characters in the text passwords.

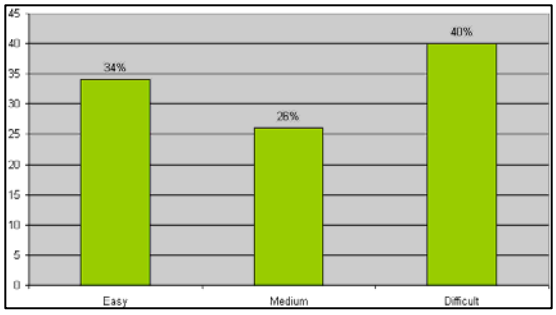

Figure 31: Grouping text passwords in terms of difficulty.

At first look, we would characterize these results quite good in terms of difficulty. However, after examining carefully the text passwords, we found out that 54% of the participants (Figure 32) created passwords that are composed of only names, or only numbers and dates. This makes these passwords really predictable. On the other hand, we found that 34% of them use a mix of

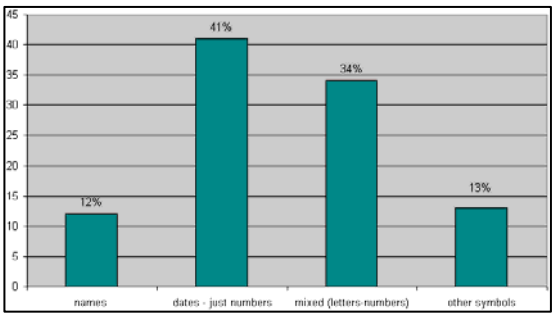

Figure 32: Predictable passwords.

letters and numbers, and only 13% of them use symbols too.

Examining only difficult text passwords, we found out that 42.5% of them are predictable. So, although 97% of the users successfully confirmed their text password, these passwords were predictable and as a result very vulnerable to attacks.

Investigating the password selection for text passwords, with respect to the gender of the participants (Figure 33), we found that more women (39.22%) than men created easy passwords (28.57%). Similarly, more women (41.18%) than men (39.78%) created difficult passwords. However, more men (32.65%) than women (19.61%) created medium difficulty passwords.

Analyzing the text passwords with respect to their ages (Figure 34), we found that most people up to 30 years old created difficult passwords (47.46%), while, most people over 30 years old created easy passwords (over 45%).

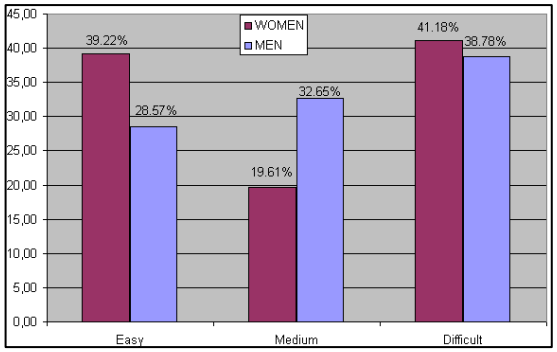

Figure 33: The difficulty of text passwords among the two sexes.

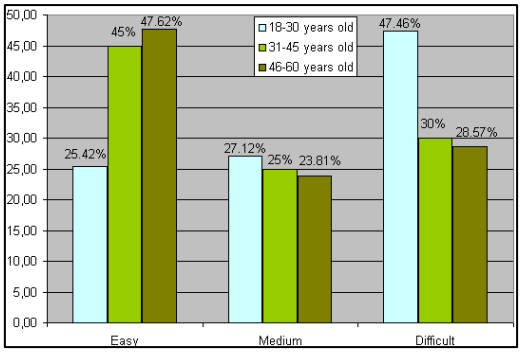

Figure 34: The difficulty of text passwords for each age group.

With the purpose to discover if the difficulty of the text passwords that users choose, depends on their sex or age, we used the SPSS statistical software and we made a chi-square test, which had the following results (Figure 35):

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	2,504[a]	2	,286
Likelihood Ratio	2,522	2	,283
Linear-by-Linear Association	,228	1	,633
N of Valid Cases	100		

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	5,215[a]	4	,266
Likelihood Ratio	5,222	4	,265
Linear-by-Linear Association	4,443	1	,035
N of Valid Cases	100		

Figure 35: Chi-test (relationship between the sex or age of the users and the difficulty of the text passwords that they create).

As we can see from the two tests, and the values that are pointed (>0.05), we can conclude at last that there is no relationship between the sex or age of the users and the difficulty of the text passwords that they create.

Continuing, we examine visual passwords following the same method, with the aim to find out if users created safer visual passwords than text.

Figure 36 shows the number of images that users have selected in their visual passwords. Then, we can construct Figure 37 which classifies the selected visual passwords into the three categories. Most participants (70%) selected 4 or 5 images into their passwords (in general, the average number of selected images is 5.07), which means that their passwords are considered very easy to be cracked. This is even worse if we think the previous successful and unsuccessful visual confirmations. We can now understand how big is the percentage of users who did not confirmed correctly their visual passwords (18%), as at the same time a great number of those passwords consist of 5 or less images.

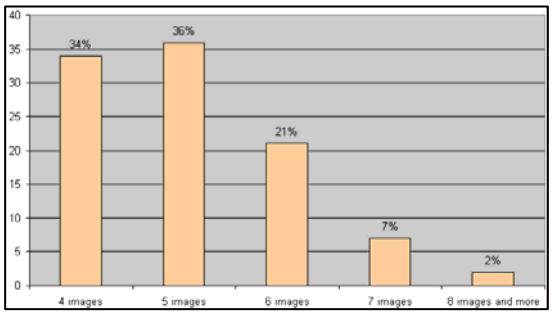

Figure 36: Number of images in visual passwords.

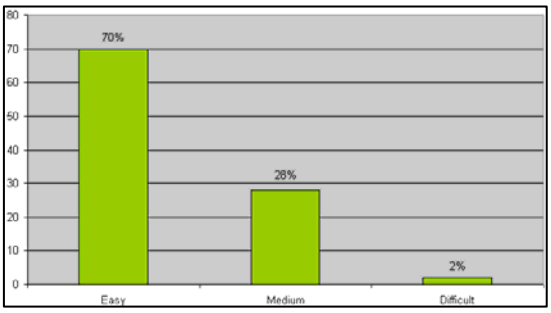

Figure 37: Grouping visual passwords in terms of difficulty.

Comparing men and women (Figure 38), we found that more men (77.55%) than women (62.75%) selected easy visual passwords. On the contrary, much more women (37.25%) than men (18.37%) selected medium difficulty visual passwords. Finally, very few men (4.08%) selected difficult visual passwords.

Regarding the ages of the participants (Figure 39), we found that easy visual passwords were selected by most participants irrespectively of their age. Higher percentages of older people (80.95%) selected easy password, while more young people (32.20%) selected passwords of medium difficulty. Also, only few young participants (3.39%) selected difficult passwords.

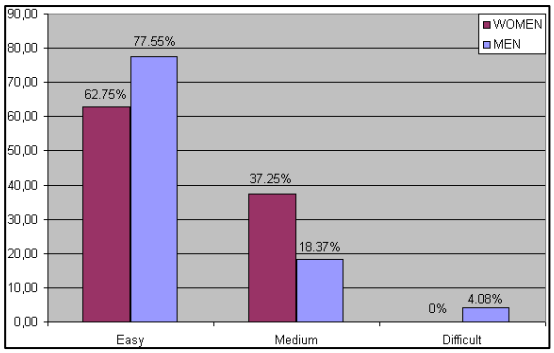

Figure 38: The difficulty of visual passwords among the two sexes.

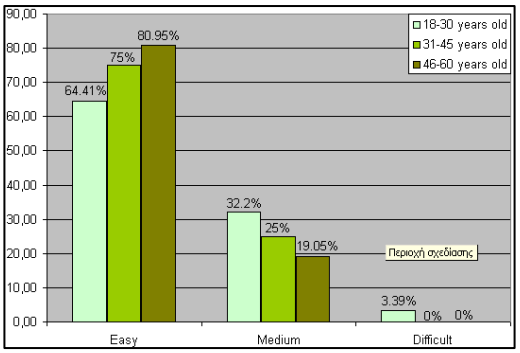

Figure 39: The difficulty of visual passwords for each age group.

Working as with the text passwords, we also tried to find out if there is a relationship between the sex or the age of users and the difficulty of visual passwords that users created. The chi-square results are presented on Figure 40:

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	6,048[a]	2	,049
Likelihood Ratio	6,899	2	,032
Linear-by-Linear Association	1,105	1	,293
N of Valid Cases	100		

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	3,122[a]	4	,538
Likelihood Ratio	3,893	4	,421
Linear-by-Linear Association	2,743	1	,098
N of Valid Cases	100		

Figure 40: Chi-test (relationship between the sex or age of the users and the difficulty of the visual passwords that they create).

According to the two tests, we can see that there is a relationship between users' sex and the difficulty of the visual passwords that they create and no relationship that concerns their age and the corresponding visual passwords.

Finally, we examine the same parameters for graphical passwords. After collecting the passwords that were created by the participants, we calculated the exact number of cells and pen up events that each password had (Figure 41). Transforming these to Figure 42, we found that most people (82%) created graphical passwords that were difficult to be cracked, of more than 11 cells and pen ups. It is also very important that the average number of cells and pen up events is 16.15. This means that even if users were not able to understand it (as they chose visual passwords as the most memorable method, they were able to create more easily really difficult graphical passwords, having a very small percentage of unsuccessful certifications.

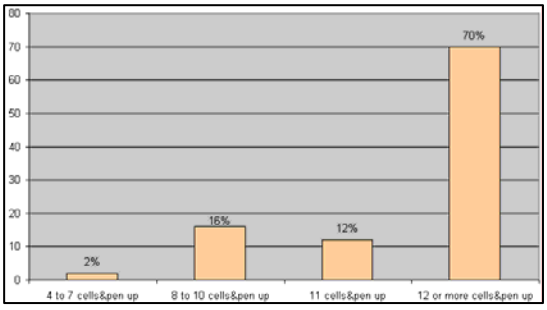

Figure 41: Number of cells and pen up events in graphical passwords.

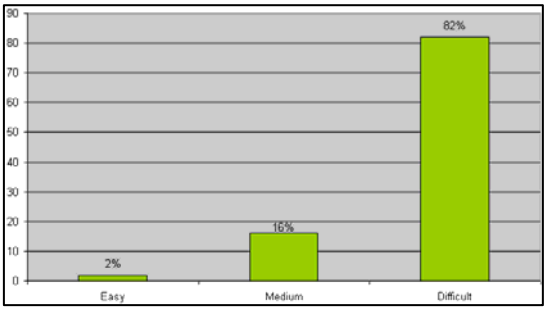

Figure 42: Grouping graphical passwords in terms of difficulty.

Figure 43 shows how is distributed the number of cells and pen up events, regarding the difficulty of graphical passwords. So, the majority of difficult graphical passwords (64.63%) consist of 11 to 18 cells and pen ups. Even better are the results of passwords which consist of 19 to 25 cells and pen ups (23.17%), and 26 to 34 cells and pen ups (12.2%).

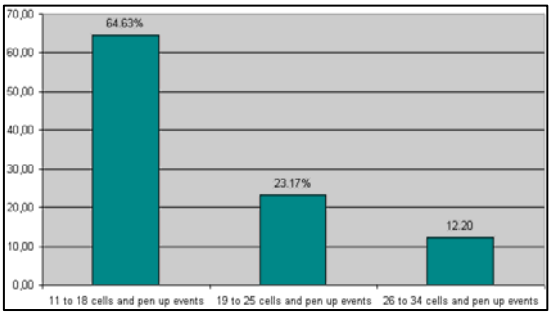

Figure 43: Distribution of the number of cells and pen up events, in difficult graphical passwords.

At the end, analyzing the results with respect to the gender (Figure 44) and the age (Figure 45) of the participants, we conclude that:

- Both men and women and almost equally, created really difficult graphical passwords, but more women than men created graphical passwords of medium difficulty
- Not only young users (86.44%), but even those at the age of over 46 years old (80.95%) were able to create difficult graphical passwords.

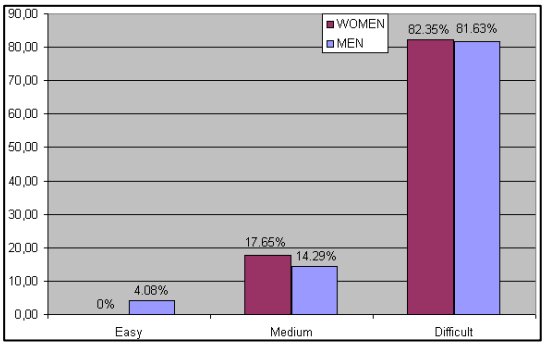

Figure 44: The difficulty of graphical passwords among the two sexes.

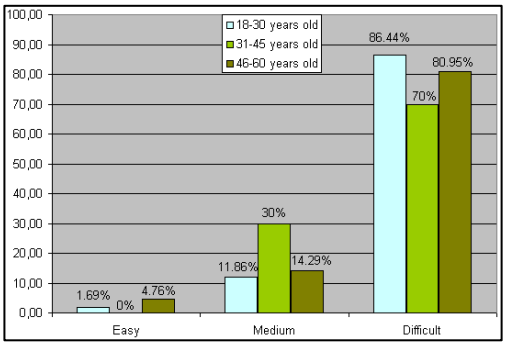

Figure 45: The difficulty of graphical passwords for each age group.

Implementing the chi-square test for graphical passwords, we conclude that neither the sex nor their age have relationship with the difficulty of graphical passwords that they create.

To make things more clear we present some random samples of graphical passwords that the participants created (Figure 46). As we can observe, the first one (Figure 46a) is a really easy password, as it has 8 cells and one pen up event. The second one (Figure 46b) is a bit more difficult, and the third and fourth (Figures 46c and 46d) are even more since they have 2 pen ups. The fifth password (Figure 46e) is a difficult one as it covers 24 cells and has 5 pen up events. The only disadvantage here is that it is symmetrical, which means that it may become a bit vulnerable to attacks that use a dictionary. Finally, the sixth password (Figure 46f) is the most difficult one as it has 7 pen up events, and has none of the characteristics that could make it easy to be cracked (it is not centered or symmetrical).

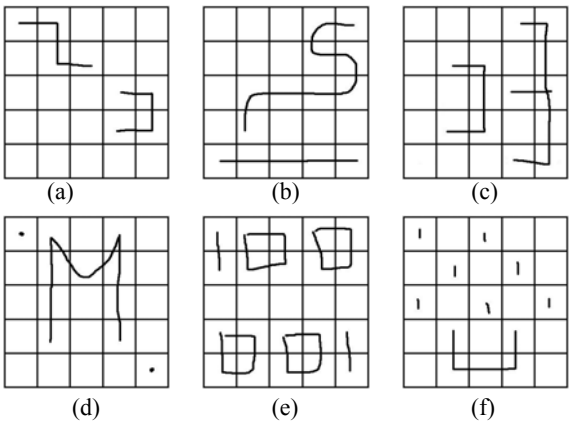

Figure 46: Sample graphical passwords.

5.6 Users' remarks

As we have already referred, the questionnaire included one question where each participant was able to report his personal opinion or whatever he wanted about passwords.

First of all, we must point out that all users understood that the development of new authentication methods that would be safer than text passwords, was an urgent issue. Those who preferred visual passwords mentioned that they are more memorable, as they can make their personal stories and according to them remember easier the right sequence of the images. From the other side, participants that preferred graphical passwords mentioned one main drawback that visual have: even if they are more attractive at the beginning, they can confuse the user very much if the application has many images and as a result become very time-consuming. Moreover they pointed out that it is very difficult to remember more than 5 images, while in graphical passwords it is much easier to pass through many cells and create a difficult password.

Users also reported that both methods are really good, even for persons who are illiterate, as they do not have to write characters, numbers or symbols, but pick images or draw a design. A very good idea that was proposed from a user about graphical passwords was to put a different color to every cell, in order to remember easier the sequence of cells.

Finally, an issue that bothered some users was the hardware that should be added e.g. a pen for graphical passwords and a touch screen for visual. This should not trouble them. Having this development in technology, in a few years it would be very easy to embed this hardware especially in communal machines, such as ATM, where information security is very important issue.

6 Conclusions

We implemented this survey with the purpose to compare the proof by knowledge authentication techniques, i.e. text passwords, visual passwords and graphical passwords. A total of 100 users participated in the survey. First, they were informed about visual and graphical passwords and the problems that text passwords have. Then, they created their own text, visual, and graphical passwords and confirmed them. Finally, they answered to a questionnaire.

Based on the passwords that users created and their answers to the questionnaire, we were able to confirm, that users have problems in remembering their passwords and as a result create text passwords

that are really predictable and vulnerable to attacks. Moreover, they share them with others, write them down or use something already known to remember them easier. Understanding this situation, almost all users were positive in knowing better and using visual and graphical passwords.

According to their answers, users and especially men remembered visual passwords easier, because they had to remember a sequence of images than a sequence of characters. The problem here was that even if visual passwords impressed users very much, the password space remains the same as in text passwords. In addition, most times users make very easy visual passwords and not safe at all.

The second new authentication method, graphical passwords, proved to be the best one. Even if the users reported that they preferred visual passwords, when they were asked to create their own graphical passwords they created more memorable and safer passwords than those when using the other two methods.

Generally, both new methods were characterized as very friendly from all users, but a bit difficult at the beginning, until they learn how to use them. This characterization was pointed out mostly from elder users, when they referred to graphical passwords. These users also found that both new methods waste more time than the text passwords, but they were positive to learn more about them. Having to their minds that these methods are much safer than the traditional ones, they found out that after practice they become really easy in their implementation.

Future research would repeat this survey in various countries. A cross-cultural comparison could be made regarding all factors considered in this study. For example, Chinese people may have different preferences and results in using text, visual and graphical passwords.

Moreover, referring to visual passwords, it would be a good idea to investigate the proper selection of images that would be included in a visual password application. For example, many users would determine their opinion about the images that they would like to be included in the application and be tested on how well they discriminate and remember these pictures.

References

De Angeli A., Coventry L., Johnson G. and Renaud K. (2005). Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems. *International Journal of Human-Computer Studies*, Vol. 63, pp 128-152, July.

Alexiadis A., Chalkias K. and Stephanides G. (2006). Implementing a graphical password scheme that uses nested grids. In *Proceedings International Conference for Internet Technology and Secured Transactions (ICITST 2006)*, London, United Kingdom.

Bauer A. (1998). Gallery of random art, http://andrej.com/art, accessed on 2nd December 2008.

Besnard D. and Arief B. (2004). Computer security impaired by legitimate users, *Computers and Security*, Vol. 23, pp. 253-264.

Birget J.-C., Hong D. and Memon N. (2003). Robust discretization with an application to graphical passwords, In *Cryptology ePrint Archive, Report 2003/168*, http://eprint.iacr.org, accessed on 2nd December 2008.

Blonder E. G. (1996). Graphical passwords, *Lucent Technologies, Inc., Murray Hill, NJ*, U. S. Patent, Ed. United States.

Bolande H. (2000). Forget passwords, what about pictures? http://zdnet.com.com/2102-11-525841.html

Chalkias K., Alexiadis A. and Stephanides G. (2006). A multi-grid graphical password scheme. In *Proceedings 6th International Conference on Artificial Intelligence and Digital Communications*, Thessaloniki, Greece.

Chiasson, S., Forget, A., Stobert, E., van Oorschot, P.C. and Biddle, R. (2009). Multiple password interference in text passwords and click-based graphical passwords. *ACM CCS'09*, November 9–13, 2009, Chicago, Illinois, USA.

Davies H. (2005). Physiognomic access control, *Information Security Monitor*, Vol. 10, no.3, pp 5-8.

Davis D., Monrose F., Reiter M. (2004). On user choice in graphical password schemes. In *Proceedings 13th USENIX Security Symposium*.

Del Luca, Denzel, M. and Hussmann, H. (2009). Look into my eyes!: can you guess my password? *Proceedings of the 5th Symposium on Usable Privacy and Security*. Mountain View, California, USA. ACM. Article No. 9.

Dhamija R., Perrig A. (2000). Déjà Vu: A user study using images for authentication. In *Proceedings 9th USENIX Security Symposium*.

Everitt, K.M., Bragin, T., Fogarty, J. and Kohno, T. (2009). A comprehensive study of frequency, interference, and training of multiple graphical passwords. *Proceedings of the 27th international conference on Human factors in computing systems*. Boston, MA, USA. ACM, pp. 889-898.

Gaw S. and Felten W. E. (2006). Password management strategies for online accounts. In *Proceedings of the second symposium on Usable privacy and security*, pp. 44-55.

Gilhooly K. (2005). Biometrics: Getting back to business. *Computerworld, May 09*.

Goldberg J., Hagman J. and Sazawal V. (2002). Doodling our way to better authentication. *CHI '02 extended abstracts on Human Factors in Computer Systems*, Minneapolis (ACM Press).

Hafiz, M.D., Abdullah, A. H., Ithnin, N. and Mammi, H.K. (2008). Towards identifying usability and security features of graphical password in knowledge based authentication technique. *Second Asia International Conference on Modelling & Simulation*, IEEE, pp. 396-403.

Irakleous I., Furnell M. S., Dowland S. P. and Papadaki M. (2002). An experimental comparison of secret-based user authentication technologies. *Information Management & Computer Security*, Vol. 10, pp. 100-108.

Jansen W. (2003). Authenticating users on handheld devices. *Canadian Information Technology Security Symposium*.

JansenA. W. (2004). Authenticating mobile device users through image selection. *Data Security,* May.

Jansen W., Gavrila S., Korolev V., Ayers and Swanstrom R. (2003). Picture password: A visual login technique for mobile devices, national institute of standards and technology interagency report NISTIR7030, http://csrc.nist.gov/publications/nistir/nistir-7030.pdf,

Jermyn I., Mayer A., Monrose F., Reiter K. M. and Rubin D. A. (1999). The design and analysis of graphical passwords. In *Proceedings of the 8th USENIX Security Symposium*.

Johnson, K. and Werner, S. (2008). Graphical user authentication: A comparative evaluation of composite scene authentication vs. three competing graphical passcode systems. *Human Factors and Ergonomics Society Annual Meeting Proceedings*, Vol. 52, No. 2008, pp. 542-546.

Kim Y. and Kwon T. (2004). An authentication scheme based upon face recognition for the mobile environment. In *International symposium on computational and information science No1*, Shanghai, China.

Klein D. (1990). Foiling the Cracker: A survey of, and improvements to, password security. In *Proceedings 2^{n} USENIX Security Workshop*, pp. 5-14.

Nali D. and Thorpe J. (2004). Analysing user choice in graphical passwords. *Tech. Report TR-04-01, School of Computer Science*, Carleton University, Canada.

van Oorschot C. P., Thorpe J. (2005), On the security of graphical password schemes. *Technical Report TR-05-11. Integration and extension of USENIX Security 2004 and ACSAC 2004 papers*.

Ozok, A.A. and Holden, S. (2008). A strategy for increasing user acceptance of authentication systems: insights from an empirical study of user preferences and performance. *International Journal of Business and Systems Research*, Vol. 2, No. 4, pp. 343-364.

Passlogix, 2006. www.passlogix.com, accessed in 22nd November 2008.

Perrig A. and Song D. (1999). Hash visualization: A new technique to improve real-world security. In *Proceedings of the 1999 International Workshop on Cryptographic Techniques and E-Commerce (CryTEC '99)*.

Por, L.Y. and Lin, X.T. (2008). Multi-grid background Pass-Go. *WSEAS Transactions on Information Science and Applications*, Vol. 7, No. 7, pp. 1137-1148.

Real User Corporation, 2006. About passfaces, http://www.realuser.com/cgi-bin/ru.exe/_/homepages/technology/passfaces.htm, accessed on 20th November 2009

Real User Corporation, 2001. *The Science Behind Passfaces*, Revision 2, September 2001. http://www.realuser.com/published/ScienceBehindPassfaces.pdf

Renaud K. and De Angeli A. (2004). My password is here! An investigation into visuo-spatial authentication mechanisms. *Interacting with Computers,* vol. 16, pp 1017-1041.

Sobrado L., Birget C. J. (2002). Graphical passwords. *The Rutgers Scholar,* vol.4. http://RutgersScholar.rutgers.edu/volume04/contents.htm.

Suo X., Zhu Y. and Owen S. G. (2005). Graphical passwords: A survey. In *Annual Computer Security Applications Conference*, Marriott University Park, Tucson, Arizona.

Tari F., Ozok A. A. and Holden H. S. (2006). A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords. In *ACM International Conference Proceeding Series*, vol. 149, pp. 56-66.

Thorpe J. and van Oorschot P. (2004). Graphical dictionaries and the memorable space of graphical passwords, In *Proceedings of the 13th UNIX Security Symposium,* August.

Tribelhorn B. (2002). End user security. http://www.cs.hmc.edu/~mike/public_html/courses/security/s06/projects/index.html, accessed on 18th November 2008.

Weiss, R. and Del Luca, A. (2008). PassShapes: Utilizing stroke based authentication to increase password memorability. *Proceedings of the 5th Nordic conference on Human-computer interaction: building bridge*s. Lund, Sweden, ACM pp. 383-392.

Wiedenbeck S., Waters J., Birget C. J., Brodskiy A. and Memon N. (2005a). Authentication using graphical passwords: Basic results. In *Human-Computer Interaction International (HCII 2005)*. Las Vegas, NV.

Wiedenbeck S., Waters J., Birget C. J., Brodskiy A. and Memon N. (2005b). Authentication using graphical passwords: Effects of tolerance and image choice. In *Symposium on Usable Privacy and Security (SOUPS)*. Carnegie-Mellon University, Pittsburgh.

Wiedenbeck S., Waters J., Birget C. J., Brodskiy A. and Memon N. (2005c). PassPoints: Design and longitudinal evaluation of a graphical password system. *International Journal of Human Computer Studies (Special Issue on HCI Research in Privacy and Security)* 63, 102-127.

Yan J., Blackwell A., Anderson R and Grant A. (2004). Password memorability and security: Empirical results. *IEEE Security & Privacy*, vol. 2, pp. 25-31, September.