Gkarafli, S. & Economides, A. A. (2010). **Comparing the proof by knowledge authentication techniques**. *International Journal of Computer Science and Security*. Vol. 4, No. 2, pp. 237-255. CSC Press. ISSN: 1985-1553

Comparing the Proof by Knowledge Authentication Techniques

Stamati Gkarafli *gkaraflistamati@yahoo.gr*
Information Systems Department
University of Macedonia
Thessaloniki 54006, GREECE

Anastasios A. Economides *economid@uom.gr*
Information Systems Department
University of Macedonia
Thessaloniki 54006, GREECE

Abstract

This paper presents a survey of proof by knowledge authentication techniques (text passwords, visual passwords and graphical passwords). Both new methods are more memorable, as people have to remember images and not characters and graphical passwords are also more secure. A total of 100 users participated in our survey, who after getting informed about the new authentication methods, they answered the questions of our questionnaire. Based on their answers, all participants have many passwords for their everyday needs and they try to select passwords that are not only memorable, but also secure. Unfortunately, they can not deal with proper password selection and they become victims of dictionary attacks. Understanding this situation, participants were very positive in learning more about the new authentication methods. They found both techniques memorable and friendly – visual passwords at most. However, they found graphical passwords a bit more complex and difficult to learn how to use them, something that they can overcome with small practice.

Keywords: graphical passwords; text passwords; user authentication methods; visual passwords.

1. INTRODUCTION

Access control includes the user's identification and authentication, authorization, audit and accountability. Various access control models have been proposed in the past [e.g. 1-5].

Authentication is the process of confirming or not the user's identity. Jansen [6] distinguished the authentication techniques into the following three categories:

- Proof by knowledge techniques, which are based on specific information that an individual has (e.g. PIN- personal identification number, text-passwords).
- Proof by property techniques, which are based on a certain property that the user has (e.g. biometrics, fingerprint verification, voice verification, iris scanning) [e.g. 7].
- Proof by possession techniques, which are based on the possession of an object that an individual has (e.g. smart cards, digital certificates, security token).

Text passwords represent the authentication method that is mainly used by all users today. Nevertheless, most times users select passwords that are memorable and as a result easy to be cracked [8]. This problem is very serious if one looks at some case studies that were conducted. According to a security team in a large company, they managed to crack 80% of the passwords [9]. Also, based on Klein's case study [10], 25% of 14.000 passwords were cracked using a small dictionary of 3 million words. According to these results one can assume that even if these methods are very popular, they can cause serious problems to the users. Some of the usual problems are the following:

- Users choose passwords that are very short in length.
- Users choose passwords that are easy to remember.
- Users write passwords down or share them with others, in order to remember them easier.
- Users use the same passwords for different applications.

Text passwords are very vulnerable to *"dictionary attacks"* (automated attacks using tools that can crack the passwords that are common words, names or dates).

2. VISUAL AND GRAPHICAL PASSWORDS

Considering all those problems of text passwords, researchers invented other proof by knowledge authentication methods: visual and graphical passwords. These methods have many advantages that are described below [11, 12, 13]:

- A sequence of pictures is more memorable than a sequence of characters.
- Pictures are independent from user's language.
- There do not exist yet special dictionaries for a dictionary attack and it is very difficult to be constructed (especially for graphical passwords that have a very large password space).
- Automated attacks are difficult to take place.

Except from all these advantages Renaud and De Angeli [14] referred the *shoulder surfing problem* as the main disadvantage of the new methods. This happens when someone is looking over someone's shoulders, during the login process [15, 16].

Next, we describe the two new authentication methods and the applications that have been created for each one of them.

2.1 Visual Passwords

Visual passwords are passwords that are created by selecting a sequence of images [5, 17]. Based on this idea, there was developed a number of commercial products that we will refer and analyze in the text below.

a) Passfaces

Real User Corporation developed a product named "Passfaces" [14, 18]. The basic idea is that the user must select four images of human faces, in a specific order, from a database. This sequence of images will be his secret password.

During the login process, the user sees a grid of nine faces, but only one of those faces belongs to the password that he made. He clicks on it, another set of nine images appears and he must again recognize and click on the image that is included

in his password. This procedure is repeated until the user clicks on all four pictures of his password. If he clicks on all four pictures correctly, the system allows him to enter.

The whole idea is based on the fact that people recall much easier human pictures than any other kind. This is especially true if each user has the opportunity to construct his own database with his personal pictures which are familiar to him and much harder to be guessed by an attacker.

FIGURE 1: Passfaces

b) Story Scheme

Story Scheme is an application similar to Passfaces. The only difference is that the images would be not only human faces, but also everyday objects, animals, food, sports, cars, or even people. In this case, the user has to think a story with the pictures that are in his database. Having his story in his mind, he selects a sequence of images [19].

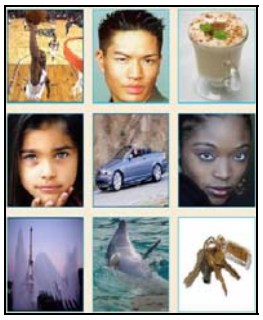

FIGURE 2: Story Scheme

c) Déjà Vu

Dhamija and Perrig developed "Déjà Vu" for user authentication [20]. At the beginning the user creates his *"image portfolio"*, by selecting a set of *p* images out of a much bigger set.

During the login process, the Déjà Vu presents to the user a set of *n* images consisting of:

- *x* images that belong to the users' image portfolio, and
- *y* other images, that we call *"decoy images"*.

At this point the user has to make a click on all images that he recognizes as belonging into his image portfolio. If he succeeds in it, the user will enter the system successfully.

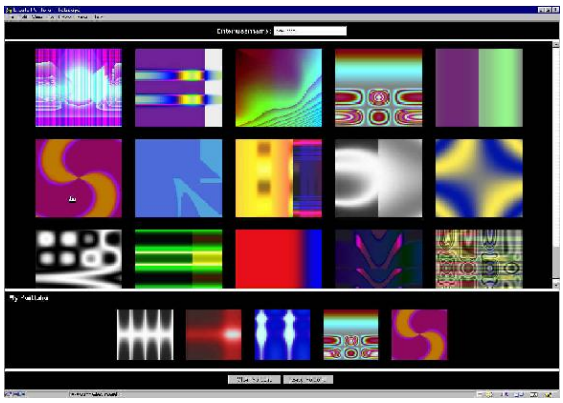

FIGURE 3: Déjà Vu

Something that is very important in Déjà Vu scheme is the type of images that are used. The images are based on Andrej Bauer's Random Art [21], which can generate random abstract images. When the user attempts to make his image portfolio, the system gives to this specific process an initial seed. With this seed, *Random Art* generates a random mathematical formula, which defines the color of each pixel in an image. Therefore, each user has his personal random pictures that were created from the initial seed.

So, it is obvious that this type of images makes the whole system much more secure, since it is very difficult for someone who observes the login process to remember them. Moreover, the system does not have to store each image pixel-by-pixel, but it stores only the initial seed.

d) Picture Password

Picture Password authentication mechanism is another application for visual login, which was developed by Jansen [5, 22].

The images are grouped into different categories according to the theme that they represent. Theme examples include Cats & Dogs, Sea, Landscapes, Sports, Faces, Transportation Means, etc. In order to create a password, the user has to choose one of these themes and afterwards a sequence of images from this theme.

Each image corresponds to an element of an alphabet. However, the user does not have to remember a sequence of random characters, but a sequence of images, something that is much easier to recall.

There are two different ways to choose the sequence of images:

- *Individual Selection:* each image represents one element in the alphabet
- *Paired Selection:* two images are combined (more often with drag and drop) and their coupling represents one element in the alphabet.

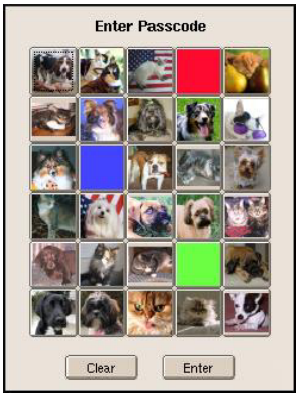

FIGURE 4: Picture Password.

e) Passlogix – Passpoints

Passlogix [23] is based on Blonder's idea [24] who proposed that during authentication, the user must click on several locations in an image. In the Passlogix implementation, the user must click on a sequence of items in the image he sees on his screen in order to create his password. To make a successful login to the system, he has to click on the same items in the correct order. A problem that we face here is how we know if an item is clicked, if we click on its edge. For this reason, there were defined invisible boundaries which indicate whether an item is clicked by the mouse or not.

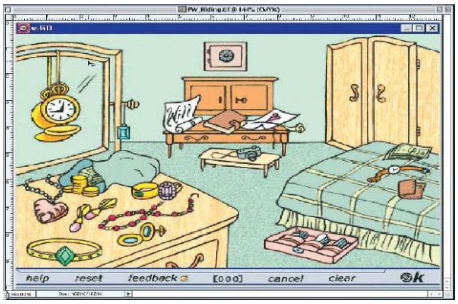

FIGURE 5: Passlogix.

An extension of this idea is the "Passpoint" system developed by Wiedenbeck et al. [25, 26, 27]. In this implementation, the user is able to make a click at any place on an image, and not only on a certain object. To achieve this they eliminated the boundaries between objects and put a tolerance around each pixel that is selected. As a result, the only thing that a user must do to make a login and enter the system is to click within the tolerance of the pixels that he chooses, in the correct order.

It is important to be mentioned here that complex pictures can have hundreds of memorable points. So, with 5 or 6 clicks, a user can make more passwords than that used today with 8 characters. So, the possible password space with this method is very large, and the whole process becomes very safe.

FIGURE 6: Passpoints.

2.2 Solving the Shoulder Surfing problem

As we have already mentioned, one main problem that visual passwords have is the *"shoulder surfing problem"*. That is watching over someone's shoulders as he tries to login a system [16]. Next, we present three methods developed by Sobrado and Birget [15] in order to solve this problem.

a) Triangle Scheme

According to this scheme, the user sees on his screen a set of *N* objects in a random position each time. He creates his password by selecting *K pass-objects* that will consist from now on, the user's portfolio.

During the login process the user is able to see on his screen a set of *L* images with *L<N*. To login correctly he must recognize the 3 pass-objects that are depicted and make a click inside the invisible triangle that is created.

If this process is done only once, then it would be very easy for someone to click inside the triangle by chance. So, the process is repeated for 8 – 10 times for each login, with the purpose to reduce the probability of randomly clicking on the correct region.

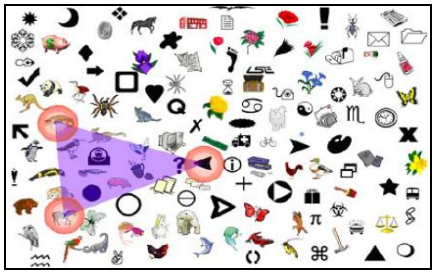

FIGURE 7: Triangle Scheme.

b) Movable Frame Scheme

Based on the same ideas with the previous scheme, in the "Movable Frame Scheme", the user has to recognize 3 of the pass objects that he has already chose. This time, his job is to move the frame around (Figure 8) until the pass object on the frame lines up with the other two.

Of course, the process is again repeated for several times, as it was also mentioned above, in order to avoid lining up the correct items by chance.

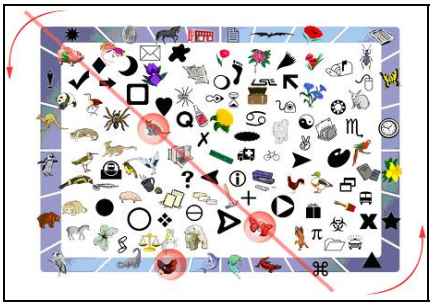

FIGURE 8: Movable Frame Scheme.

c) Other Geometric Configurations

Similarly, the third method follows the same rules. However, in this case the user has to recognize 4 pass objects and make a click at the intersection of the virtual lines that are formed by connecting these objects.

Of course, it is obvious, that there is a tolerance of the pixel that the user clicks, in order not to have arguments about the exact point that he chooses each time.

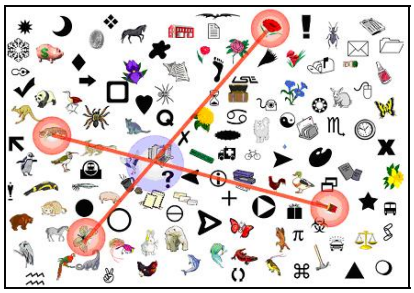

FIGURE 9: Other Geometric configurations.

2.3 Graphical Passwords

In this section, we analyze *graphical passwords*. Here, the user has to draw a personal design that will be from now on his secret password. More precisely, we examine the *DAS* scheme and its extension *Multi-grid Passwords.*

a) Draw-a-Secret (DAS) Scheme

Jermyn et al. [22] proposed a scheme, called DAS (Draw-a-Secret), which allows the user to draw a simple design on a grid. On his screen the user is able to see a rectangular grid of size $G \times G$. Then, he has to draw a sequence of lines in this grid. This drawing will represent his password.

For example, let consider a grid of size 3×3 (Figure 10). In order to create his password, the user has to draw a sequence of lines. Then, at the login process, he must draw the same lines again, in the same order. For this reason the drawing is mapped to a sequence of coordinate pairs by making a list of the cells through which the drawing passes in the correct order, separated by pen-up events, when the user raises his pen and continues from another point. In Figure 10, we have the following sequence that we made by the drawing:

(1,2), (1,1), (2,1), (2,2), (3,2), pen-up, (2,3), (1,3).

According to this, we must underline that what counts for a user in order to make a successful login is not the exact draw that he has made, but the sequence of cells from which his pen passes in combination with the pen-up events.

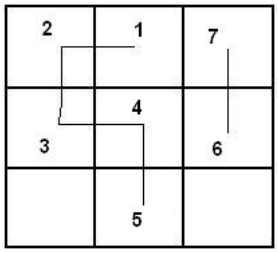

FIGURE 10: DAS Scheme.

In Figure 11 we can see another example of the DAS Scheme, its internal representation, the bit string that is created and an unsuccessful login because of a shift error that was made.

An important point is that a one-way hash function is applied to the bit string that is created and the result is stored to the server of the system. So, when the user tries to login the system, he draws his password, then the hash function is applied to it, and the result is compared with the stored result. If these two are the same, then the login is successful, otherwise it is not.

As we can understand this process makes the whole scheme very safe. The system does not know each user's password and as the hash function is one-way we cannot compute the initial design from the result that is stored.

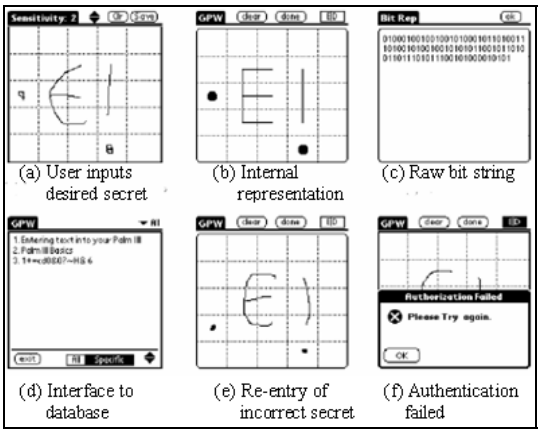

FIGURE 11: DAS Scheme. Internal representation of our draw and a failed login because of a shift error [28].

b) Multi-grid Passwords

Nali and Thorpe [29] performed a survey to investigate the reasons that could make DAS passwords vulnerable to attacks. According to them, this idea could be true if we consider that many users draw passwords with predictable characteristics, which means that these are centered or symmetric. As a result symmetrical or centered DAS passwords can reduce very much the password space and help attackers in

creating dictionaries [30, 31]. Based on this remark, Birget et al. [30] referred problems with the DAS scheme because of uncertainty in the clicking regions.

Chalkias et al. [33] as well as Alexiadis et al. [34] made an extension to the DAS scheme with the aim to reduce these facts that have very serious implications to the security of the system. They proposed multi-grid passwords by using nested grids in the initial one (Figure 12). The main reasons that users fail to confirm their passwords are that they forget their stroke order and they mark adjacent cells instead of the correct ones.

With multi-grid passwords the users are able to create more complicated passwords that at the same time are more memorable. For example, using grids like in Figure 12, the user has more points of focus to do his drawing, and so he does not need to make his design in the center of the grid or symmetrically. With multi-grid passwords the users are able to create more complicated passwords that at the same time are more memorable. This can be explained if we examine Figure 12. With grids like those, we have more points of focus to do our drawing, and so the user does not need to make his design in the center of the grid or symmetrically.

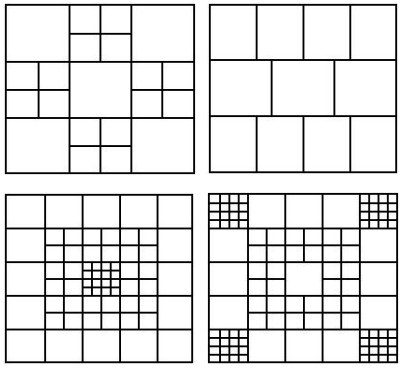

FIGURE 12: Multi-grid passwords [33].

3. RELATED WORK

As we have already mentioned, text passwords nowadays are very unsafe and can cause serious security problems to the users. Based on this fact and taking into account the new authentication methods that were invented, many researchers have worked on them, with the aim to compare them and find what effect they may have in our society.

According to Irakleous et al. [35], 59% of the participants have 2 -5 passwords, while 65% of them use at least one of them daily. Also, Tribelhorn [36] showed that all users are concerning very much for the security of their passwords. For this reason, many users try to create passwords that are difficult to be cracked, by selecting 8 or more characters. But just this effort is not enough, because users want their passwords to be also memorable. So they create passwords that are consisted of ordinary words or dates, making them really vulnerable to dictionary attacks.

All these lead the researchers to the new authentication methods, visual and graphical passwords. Many applications were created based first of all on the image selection of visual passwords. Kim and Kwon [37] found that having in visual

passwords images with known faces, make them more memorable that having landscapes or random faces. Davis et al. [19] examined the images that males and females choose and concluded that females chose animals or food and males choose women and sports. Dhamija and Perrig [20] working on Déjà vu scheme, found out that after some practice, users have very good results in remembering the passwords with simple photos, but also the passwords that are based on random art technique.

Really opposed to these results, Jansen [22] showed that visual passwords are not safer than the text, as users tend to select a small number of images (usually 4 or 5), creating this way passwords easy to be cracked. Wiedenbeck et al. [25, 26, 27] showed that graphical passwords may be more time-consuming or more difficult to be confirmed successfully, but that after some practice the situation changes and above all the passwords that are created are really safe.

Further examining the graphical passwords, Goldberg et al. [38] found out that with practice users can have the best results. They make more successful logins, something that is confirmed by the fact that 72% of them agreed that this method is easier to remember than the text passwords.

Nali and Thrope [29] examined the drawbacks of graphical passwords which include that users draw designs that are centred or symmetrical, something that decreases their security. As a solution to this situation, Chalkias et al. [33] proposed a multi-grid password scheme and they made a comparison for centred and symmetrical drawings, between non-technical and technical users. According to their survey, using a multi-grid scheme fewer participants created centred and symmetrical passwords and as a result, more users were able to create safer passwords. Weiss and Del Luca [39] 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. Also, Eljetlawi and Ithnin [40] designed Jetafida focusing on the usability features of this graphical password system. Everitt et al. [41] 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. [42] 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 [43] compared alphanumeric and graphical passwords. Johnson and Werner [44] found that passcodes are more memorable than alphanumeric passwords over extended retention intervals. Finally, various classification systems of graphical passwords were proposed [45, 46].

In our survey, in opposition to those that we have already mentioned, we made a comparison between the three “proof by knowledge” authentication techniques, text, visual and graphical passwords and not just between two or three specific applications that are listed either in the visual or graphical method. Also 100 users were participated with the aim to obtain results that are significant statistically, while in the other surveys there were participated up to 40 users. Finally, to have more

general results, the users that participated were from 18 to 60 years old (not only students in colleges and universities), in order to find out the impression and the effect that the new methods have in the whole society and not just in a part of it.

Furthermore, we created a comprehensive study, to examine many issues that refer to visual and graphical passwords, comparing them with the traditional authentication method that is text passwords.

4. METHODOLOGY

4.1 Questionnaire

To conduct our survey, we created a questionnaire to obtain users' opinion. Our questionnaire is a completely new questionnaire that is referred to characteristics that text, visual and graphical passwords have. More precisely, the information that we collected with the questionnaire are the following:

- how important are passwords for the users
- what problems do text passwords have
- are they positive in using visual and graphical passwords
- user's personality according to their personal opinion
- users' opinion about text, visual and graphical passwords in terms of memorization, difficulty in learning their use and friendliness.

Analyzing users' answers to the questionnaire, we discovered their opinion about the traditional text passwords and the new visual and graphical passwords. In addition, we examined at what degree our society is able to change its habits and accept without any problems, the new authentication methods that are really safer.

4.2 Participants

In our study 100 people were participated. They already knew and used PINs and text passwords. There were included 49 men and 51 women, from 18 to 60 years old. More precisely, if we divide the users into three categories according to their age, we have: 59 users from 18 to 30 years old, 20 users up to 45 years old and 21 users over 46 years old and until 60. The younger participants were students or post graduated students in the University of Macedonia in Thessaloniki, in the Aristotle University in Thessaloniki and in the TEI of Larissa. The elder ones were teachers in schools and Universities, people that work in public services, in the private sector, in manufactures or in factories, in Thessaloniki and in Larissa. All these users were found in their work, something that made really difficult the whole process of collecting their answers. This is because we had to make the procedure that we will describe analytically below, separately to 3 - 4 users, as it was infeasible to find more people free at the same time, to deal with our questionnaire.

What was very important to us was that from the beginning of our survey every participant was very positive in helping us to carry it out. Especially after listening to a small introduction with information about the new methods and the danger that traditional text passwords hide, they were very willing to participate and in this way help us overcome all these problems.

4.3 Procedures

As we have already mentioned, in order to accomplish our survey, we have created a questionnaire that referred to text, visual and graphical passwords. The whole

procedure of our survey is divided into two different stages. At the first stage, we gave a short seminar (as many of them were in their work) to the participants that included an introduction to the text passwords and their problems and an analysis of the new authentication methods, visual and graphical passwords.

After understanding all these points, all the participants were asked to fill in the questionnaire that we have prepared, with the aim to find out their personal opinion about the three authentication methods. Finally, after collecting all the questionnaires, we analyzed the users' answers and we present the results in the text below.

5. RESULTS

In this section, we present the results of the survey regarding text, visual and graphical passwords. We present the results in six categories: 1) password importance, 2) problems with text passwords, 3) the new authentication techniques, 4) comparison among the three methods, 5) making safer graphical passwords.

5.1 Are passwords important to our life?

First of all, we were interested in identifying the importance of passwords from the users' point of view. We asked participants about the number of passwords they use in their everyday activities. 47% of them have one to four passwords, 34% have 5 to 7 passwords, and 19% have more than 8 passwords.

In Figure 13, we present the percentage of men and women with respect to their number of passwords. Almost the same percentage of men and women has one to four passwords. However, 26.53% of men and 41.18% of women have five to seven passwords. On the contrary, 26.53% of men and 11.78% of women have eight or more passwords. So, we observe a significant difference between men and women who use more than four passwords.

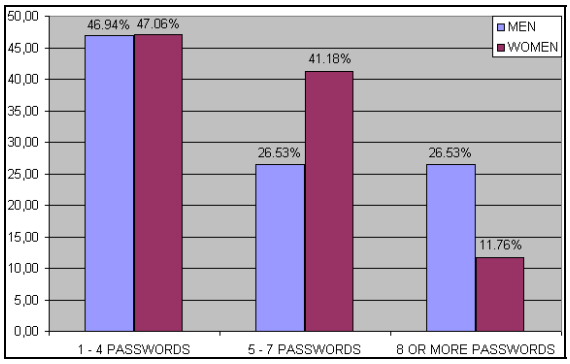

FIGURE 13: Number of passwords that men and women use

Taking into consideration the age of the users, we observe that the majority (76.19%) of people between 46 and 60 years old use up to four passwords, while younger people tend to use many passwords (Figure 14). Five to seven passwords are used by 35.59% of people between 18 and 30 years old, and by 40% of people between 31 and 45 years old. More than eight passwords are used by 27.12% of people between 18 and 30 years old, and by 15% of people between 31 and 45 years old.

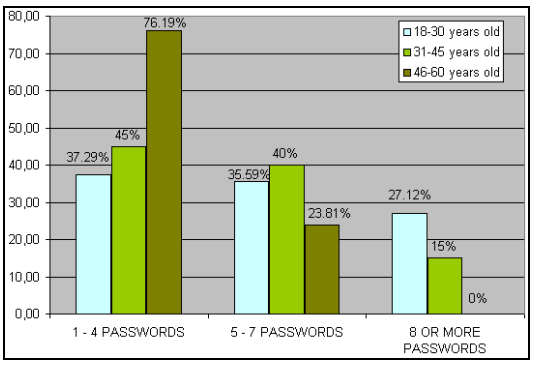

FIGURE 14: Number of passwords that users have, according to their age.

It is also important to examine for what reasons they use those passwords, and how often they really use them. Almost every user has a mobile phone (94%) and ATM cards (88%) with which he uses passwords to verify his identity (Figure 15). Considering the increased use of Internet, we can understand why so many people have passwords for their e-mail (64%), Internet connection (54%) or to make a login to web pages (39%).

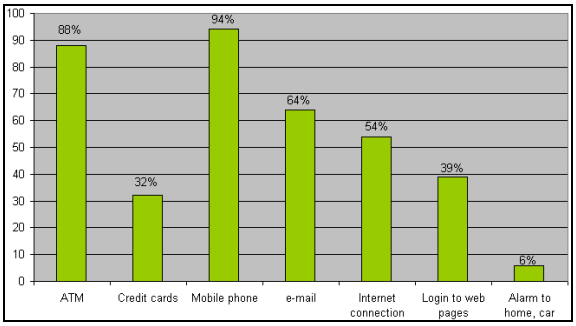

FIGURE 15: The applications where users use passwords.

Finally, we found that 69% of the participants use at least one password every day, and almost all of them use a password once or twice per month. So, we can figure out how important is for everyone to have a memorable and primarily safe password.

5.2 Analyzing text passwords

As we had already referred, text passwords nowadays are very unsafe and can cause many problems to the people that use them. To find out if this situation is really true, we asked the participants what kind of passwords they use for their applications. Their answers are presented in Figure 16.

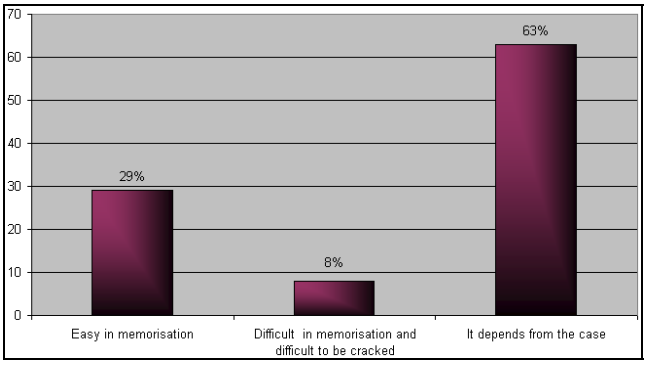

FIGURE 16: Type of passwords that users choose.

The percentage of the users that choose passwords that are easy in memorization is 29%, while just 8% of them choose passwords that are difficult in memorization but also difficult to be cracked and as a result very safe. The rest 63% of the participants chooses both easy and difficult passwords, based on how important are the applications that are applied to.

These percentages are quite good at a first glance. But to make things more clear and to understand if these results are really satisfactory, we have to find out more details about these passwords.

In Figure 17, we can see the number of characters that participants use in their passwords. 41% of them have 4 characters in their passwords, 43% have 5 to 7 characters and 16% have more than 8 characters.

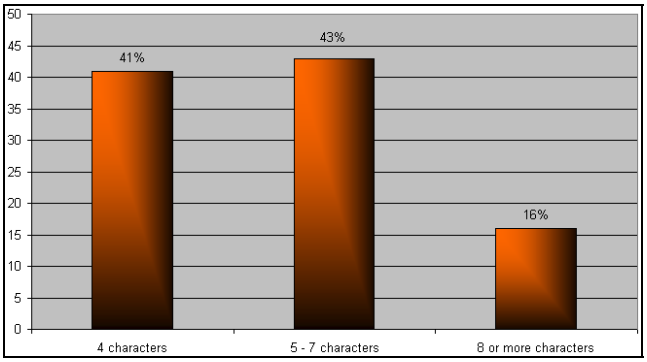

FIGURE 17: Number of characters in a text password.

Carefully looking at these results we can say that they are quite satisfactory as a password of more than 8 characters is characterized very safe and really difficult to be cracked and one with 6 or 7 characters is characterized as a password of medium difficulty. But these results are incomplete, because we have not examined yet what is the exact kind of the characters that these passwords are consisted of. For this reason we have created Figure 18.

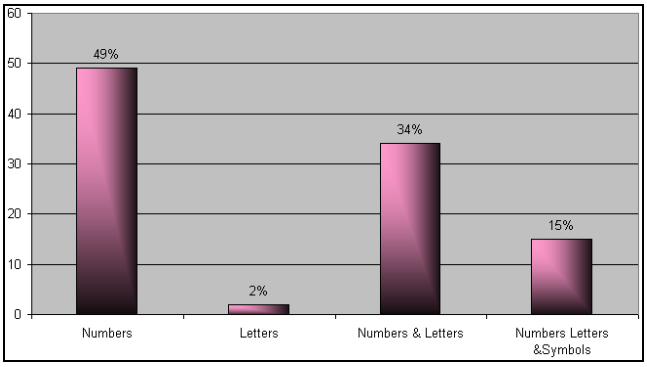

FIGURE 18: The exact kind of characters that the passwords are consisted of.

According to Figure 18, we can see that 49% of the participants use just numbers in their passwords and 2% just letters. This situation is really problematic because most participants that use just numbers or letters in their passwords create passwords with familiar dates or names that consequently are very vulnerable to attacks. Only 15% of these passwords is consisted of numbers, letters and symbols together and are really safe and reliable passwords.

5.3 New authentication techniques: Visual and Graphical passwords

Considering the previous results, we can be sure that most text passwords that were created by users are predictable and really unsafe for them. So, it was inescapable that new authentication methods were needed. These methods are visual and graphical passwords.

Next, after explaining to the users about visual and graphical passwords, we examine at what degree they are positive in further learning and using them. Their answers are divided into five categories (Figure 19), that are “by no means”, “a little”, “enough”, “much”, “very much”.

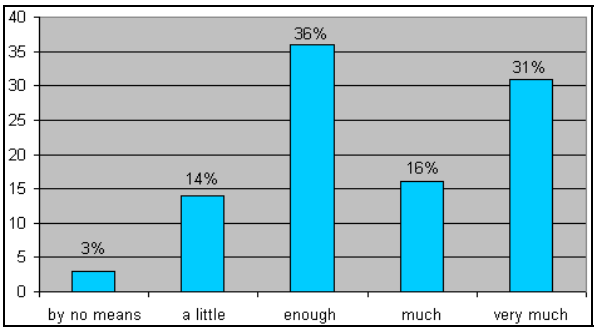

FIGURE 19: Users’ position in accepting or not of visual and graphical passwords

As we can observe in Figure 19, the users that are totally negative or a little interested in learning more about the new authentication methods are very few (3% and 14% correspondingly). In opposition to this, 36% of the users chose “enough” as their answer, 16% “much” and 31% “very much”, a situation that reveals that most of the participants in our survey are positive in learning and also using visual and graphical passwords.

5.4 Analyzing the three authentication methods

In this section we will analyze the two new authentication methods, visual and graphical passwords, with respect to various parameters that will show us if these methods affected participants in a positive way.

Firstly, we will examine the memorability of each method. As we can see in Figure 20, 57% of the users believe that visual passwords are more memorable, while 43% of them prefer graphical passwords.

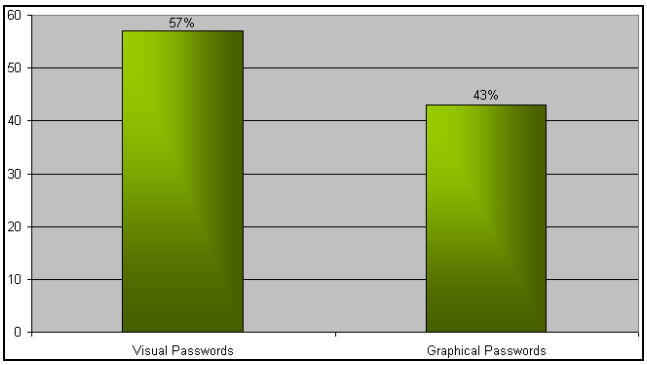

FIGURE 20: Most memorable authentication method

Based on these results we found it very interesting to divide the participants into three categories, describing their personality according to their personal opinion. To answer in this question the participants had to select one out of the three choices that follow:

- Visual, if the user remembers or learns something easier using images
- Acoustic, if the user remembers or learns something easier by listening to it
- Verbal, if the user remembers or learns something easier, when it is written down.

According to their answers, we conclude in Figure 21.

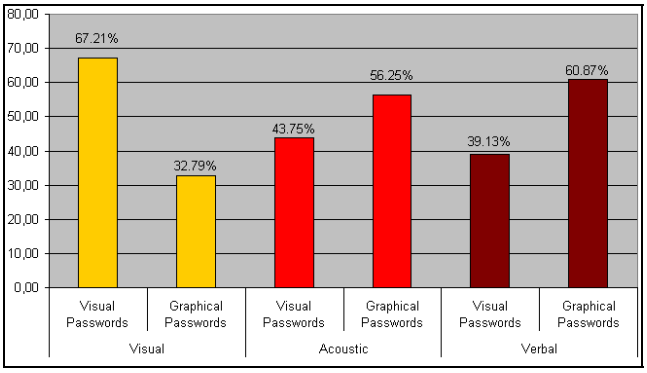

FIGURE 21: Most memorable authentication method based on the kind of person that each user enlists himself.

Here we can see that more users that are visual types of persons prefer Visual Passwords (67.21%), while users that are acoustic and verbal types of persons, prefer mostly Graphical Passwords (56.25% and 60.87% correspondingly).

Next, we will examine and compare all three authentication methods (text, visual and graphical passwords) regarding users' opinion about how easy is it for them to learn how to use each method. Users had to select one out of the five answers that were:

"not at all", "a little", "enough", "much" and "very much", in proportion to how difficult is the whole process for them. Collecting their answers, we conclude in Figure 22.

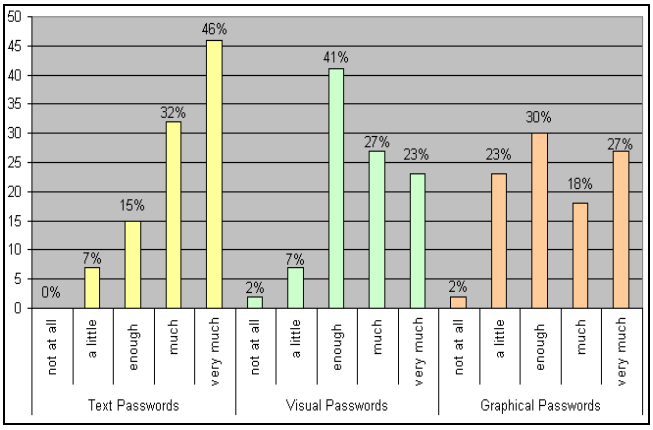

FIGURE 22: How easy is for someone to learn how to use the three authentication methods

According to Figure 22, we can observe that the users that found it very difficult or a little difficult to learn how to use text and visual passwords are very few. Most of them found the two methods really easy, for two different reasons:

- Text passwords, because they are very familiar with them, as they use them almost every day
- Visual passwords, because they are attractive and they have no special rules (the users just have to choose a sequence of images as their password).

On the other side, only 2% of the users find it very easy to learn how graphical passwords are used and 23% of them believe that the whole process is a little easy to be learnt. This percentage is not really problematic, as this method is not so attractive at first side and has also many rules that a user must remember, to create his password. What we have to mention here is that the rest of the participants did not have difficulties in learning the use of graphical passwords and above all they believe that with some practice everyone will be able to overcome any problem he may face.

The last parameter that we examined is how easy is for someone to use the three authentication methods. Users here should again select one of the five given answers that are "not at all", "a little", "enough", "much" and "very much", regarding how friendly they think that each method is for them. The results are depicted in Figure 23.

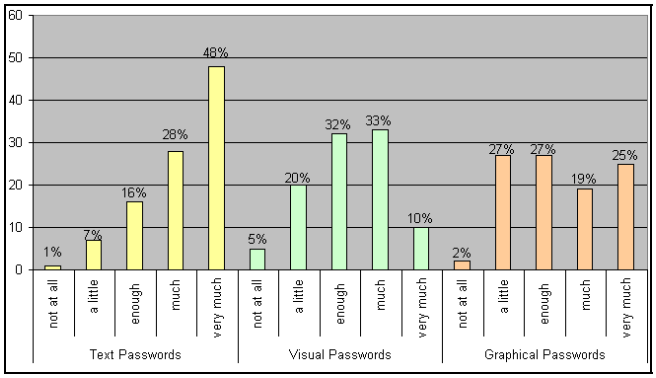

FIGURE 23: User friendliness of the three methods

In Figure 23, we can see that text passwords are considered to be the friendliest method. For visual and graphical passwords 5% and 2% correspondingly believe that they are not friendly at all to the users, 20% and 27% that they are a little friendly, while the rest believe just the opposite. Moreover, we have to say that 25% of the users chose “very much” as their answers for graphical passwords, while the same percentage for visual is 10%. This situation proves us that even if visual passwords impressed the users more at the beginning of the survey, the participants were able to overcome all the difficulties and understand why graphical passwords is the best method out of the three.

5.5 Making more safe graphical passwords

After finishing processing the data, analyzing the results and taking into account other researchers’ results, we conclude that graphical passwords is the safest authentication method. Moreover with some practice by the users, they can become very memorable and ease to be used by the users.

Considering all these, we suggest a set of tips and advices to users, in order to create very difficult passwords and not vulnerable to attacks. These tips are the following:

- do not make symmetrical shapes
- do not make centered shapes
- try to draw more than one lines
- include in your drawing, as much pen up events as you can (the same drawing with more pen up events is much safest)
- avoid starting your drawing from the 4 corners (these cells are very vulnerable)
- if your drawing is simple, try to make a second or even a third, similar to the initial one but covering different cells
- avoid drawing diagonal lines, and as a result lines near the intersection of the lines that create the cells, because it is very easy to get confused and make shift errors.

6. CONCLUSIONS

We conducted our survey with the purpose to compare the proof by knowledge authentication techniques which are text passwords, visual passwords and graphical passwords. A total of 100 users participated in the survey. First, they were informed about the problems that text passwords have and the advantages that visual and

graphical passwords can offer to overcome these problems. Finally, according to what they learnt and their personal opinion, they answered to our questionnaire.

Based on users' answers we are able to confirm that almost every user uses passwords for different applications such as mobile phone, ATM cards, credit cards, e-mails, internet connection etc. From these users, almost half of men and women have 1 – 4 passwords, while about 40% of women have 5 – 7 and 26% of men 8 passwords or more. Indeed, as it was expected, users that have 1 – 4 passwords are the elder ones (46 – 60 years old) and those that have more passwords are the younger.

Analyzing the text passwords that users claim that they create, we see that 30% of them create passwords that are really memorable and as a result easy to be cracked. The encouraging thing is that 63% of them create either easy or difficult passwords (with as many characters as they can), with respect to the application that they are referred to. Unfortunately, this is not enough because many users include only numbers in their passwords, or only letters, or numbers and letters both, creating passwords of familiar dates and names that are vulnerable to dictionary attacks.

That was the main reason that a great percentage of users were very positive in knowing better the new authentication methods. After learning more information about these methods, 57% of them chose visual passwords as the most memorable method, while 43% preferred the graphical passwords. Besides, as we divided the users in three categories, visual, acoustic and verbal, we must say that visual users prefer mainly visual passwords while acoustic and verbal users prefer graphical passwords.

Moreover, we must report that both new methods and especially visual passwords were characterized very friendly by all users. At the same time graphical passwords were characterized a bit difficult until they learn how exactly they are used.

Finally, keeping in mind that graphical passwords is the safest method, we made a small list with tips that users must follow, in order to create really difficult graphical passwords and as a result very hard to be cracked from anyone.

REFERENCES

[1] Bammigatti, P. H., and Rao, P. R. "Delegation in role based access control model for workflow systems". International Journal of Computer Science and Security, 2(2): 1-10, 2008.

[2] Chandrasekar, A., Rajasekar, V. R. and Vasudevan, V. "Improved authentication and key agreement protocol using elliptic curve cryptography". International Journal of Computer Science and Security, 3(4): 325-333, 2009.

[3] Kar, J. and Banshidhar, M. "An efficient password security of multi-party key exchange protocol based on ECDLP". International Journal of Computer Science and Security, 3(5): 405-413, 2009.

[4] Tahir, M. N. “Hierarchies in contextual role-based access control model (C-RBAC)”. International Journal of Computer Science and Security, 2(4): 28-42, 2008.

[5] Tahir, M. N. “Testing of contextual role-based access control model (C-RBAC)”. International Journal of Computer Science and Security, 3(1): 62-75, 2009.

[6] W. Jansen. “Authenticating users on handheld devices”. In Proceedings of the Canadian Information Technology Security Symposium, 2003.

[7] Bhagwat, R. and Kulkarni, A. (2010). “An overview of registration based and registration free methods for cancelable fingerprint template”. International Journal of Computer Science and Security, 4(1): 23-30, 2010.

[8] H. Davies. “Physiognomic access control”. Information Security Monitor, 10(3): 5-8, 2005.

[9] K. Gilhooly. “Biometrics: Getting back to business”. Computerworld, May 2005.

[10] D. Klein. “Foiling the Cracker: a survey of, and improvements to, password security”. In Proceedings of the 2^{n} USENIX Security Workshop, pp. 5-14, 1990.

[11] de A. Angeli, L. Coventry, G. Johnson and K. Renaud. “Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems”. International Journal of Human-Computer Studies, 63: 128-152, July 2005.

[12] H. Bolande. “Forget passwords, what about pictures?”. http://zdnet.com.com/2102-11-525841.html

[13] X. Suo, Y. Zhu and S. G. Owen. “Graphical passwords: A survey”. In Proceedings of the Annual Computer Security Applications Conference, Marriott University Park, Tucson, Arizona, 2005.

[14] K. Renaud and de A. Angeli. “My password is here! An investigation into visuo-spatial authentication mechanisms”. Interacting with Computers, 16: 1017-1041, 2004.

[15] L. Sobrado and C. J. Birget. “Graphical passwords”. The Rutgers Scholar, 4, 2002. http://RutgersScholar.rutgers.edu/volume04/contents.htm.

[16] F. Tari, A. A. Ozok and H. S. Holden “A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords”. In ACM International Conference Proceeding Series, 149: 56-66, 2006.

[17] A. Perrig and D. Song. “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).

[18] Real User Corporation. “About passfaces”, http://www.realuser.com/cgi-bin/ru.exe/_/homepages/ technology/passfaces.htm, accessed in November 2006.

[19] D. Davis, F. Monrose and M. Reiter. “On user choice in graphical password schemes”. In Proceedings of the 13th USENIX Security Symposium, 2004.

[20] R. Dhamija and A. Perrig. “Déjà Vu: A user study using images for authentication”. In Proceedings of the 9th USENIX Security Symposium, 2000.

[21] A. Bauer. “Gallery of random art”, 1998, http://andrej.com/art, accessed in December 2008.

[22] W. Jansen. “Authenticating mobile device users through image selection”. Data Security, May 2004.

[23] Passlogix. www.passlogix.com, accessed in November 2006.

[24] E. G. Blonder. “Graphical passwords”. Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent, Ed. United States, 1996.

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

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

[27] S. Wiedenbeck, J. Waters, C.J. Birget, A. Brodskiy and N. Memon. “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, 2005.

[28] I. Jermyn, A. Mayer, F. Monrose, K. M. Reiter and D. A. Rubin. “The design and analysis of graphical passwords”. In Proceedings of the 8th USENIX Security Symposium. 1999.

[29] D. Nali and J. Thorpe. “Analysing user choice in graphical passwords”. Tech. Report TR-04-01, School of Computer Science, Carleton University, Canada, 2004.

[30] C. P. van Oorschot and J. Thorpe. “On the security of graphical password schemes”. Technical Report TR-05-11. Integration and extension of USENIX Security 2004 and ACSAC 2004 papers.

[31] J. Thorpe and P. Van Oorschot. “Graphical dictionaries and the memorable space of graphical passwords”. In Proceedings of the 13th UNIX Security Symposium, August 2004.

[32] J. C. Birget, D. Hong and N. Memon. “Robust discretization with an application to graphical passwords”. Cryptology ePrint Archive, Report 2003/168, http://eprint.iacr.org,

[33] K. Chalkias, A. Alexiadis and G. Stephanides. “A multi-grid graphical password scheme”. In Proceedings of the 6th International Conference on Artificial Intelligence and Digital Communications, Thessaloniki, Greece, 2006.

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

[35] I. Irakleous, M. S. Furnell, S. P. Dowland and M. Papadaki. “An experimental comparison of secret-based user authentication technologies”. Information Management & Computer Security, 10: 100-108, 2002.

[36] B. Tribelhorn. “End user security”, 2002. http://www.cs.hmc.edu/~mike/public_html/courses/ security/s06/projects/index.html, accessed in November 2008.

[37] Y. Kim and T. Kwon. “An authentication scheme based upon face recognition for the mobile environment”. In Proceedings of the International symposium on computational and information science N°1, Shanghai, China, 2004.

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

[39] R. Weiss and A. del Luca. “PassShapes: Utilizing stroke based authentication to increase password memorability”. In Proceedings of the 5th Nordic conference on Human-computer interaction: building bridges. Lund, Sweden, ACM pp. 383-392, 2008.

[40] A. M. Eljetlawi and N. Ithnin. “Graphical password: Prototype usability survey”. In Proceedings IEEE International Conference on Advanced Computer Theory and Engineering, pp. 351-355, 2008.

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

[42] S. Chiasson, A. Forget, E. Stobert, P. C. van Oorschot and R. Biddle. “Multiple password interference in text passwords and click-based graphical passwords”. ACM CCS’09, November 9–13, 2009, Chicago, Illinois, USA, 2009.

[43] A. A. Ozok and S. Holden “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, 2(4): 343-364, 2008.

[44] K. Johnson and S. Werner. “Graphical user authentication: A comparative evaluation of composite scene authentication vs. three competing graphical passcode systems”. Human Factors and Ergonomics Society Annual Meeting Proceedings, 52: 542-546, 2008.

[45] M. D. Hafiz, A. H. Abdullah, N. Ithnin and H. K. Mammi. “Towards identifying usability and security features of graphical password in knowledge based authentication technique”. In Proceedings of the Second Asia International Conference on Modelling and Simulation, IEEE, pp. 396-403, 2008.

[46] L. Y. Por and X. T. Lin. “Multi-grid background Pass-Go”. WSEAS Transactions on Information Science and Applications, 7(7): 1137-1148, 2008.