International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org, editorijettcs@gmail.com
Volume 4, Issue 3, May-June 2015 ISSN 2278-6856

Graphical Passwords replacing text passwords: Advantages and Cons

[1]Majed SANAN , Mahmoud RAMMAL[2] ,Wassim RAMMAL[3]

[1]Lebanese University, Faculty of Sciences.

[2]Lebanese University, Director of center of Research & Studies
In Legal informatics,

[3]Lebanese University, Faculty of Sciences.

ABSTRACT

The security triad of any company is mainly based on three components: Confidentiality, Integrity and Availability. In other words, this triad is based on keeping the system's data always available when needed while preventing unauthorized individuals from accessing this data or causing harmful modification or destruction to it [1]. Human factors are considered the major threat that could intimidate the security triad of organizations when starting harmful and illegal attacks on the system. But ironically, the attackers depend mainly on the weakest point of any system: the human factor itself. The attackers focus on tricking legitimate users into revealing confidential information in an attempt to gain an unauthorized access to the system depending on some wrong security behavior done by the users. In this work we analyze the main advantages and disadvantages of text passwords and graphical passwords and we explain the reasons of replacement of text passwords by graphical passwords by giving a small algorithm application with its analysis and conclusions.

Keywords: graphical passwords, text passwords.

1. INTRODUCTION

Several challenges are raised when designing user interaction interface, specifically in the case of authentication systems. Such systems should provide an ease of access for all authenticated users and maintain a high level of security.

Security is usually considered a secondary task in the prospect of most users. The main task of the users is to perform the tasks they are paid to do. If the security policies become an obstacle in reaching their primary tasks, the users will try to circumvent the security measures. Due to their poor mental realization of security, users do not realize that their actions are insecure in the first place. They often underestimate the consequences of their actions that could lead to an external leak to attackers [6].

Dr. Karen Reynaud, a computer science lecturer at the University of Glasgow, visualized the authentication process for individuals through three phases:

Identification.

Authentication.

Authorization.

Users must first make some claim of their identity and provide evidence to support this claim, and if successfully authenticated by the system, access rights are granted to the user[8].

2. BACKGROUND

2.1. Text Passwords

Many contributors presented password methods for a secure authentication. Despite the large number of options for authentication, text passwords remain the most common choice for several reasons. Text passwords are inexpensive, easy to implement and friendly to almost all users. It allows users to authenticate themselves without violating their privacy, as biometrics could, since users should select passwords that do not contain personal information. Moreover, text passwords are portable since users simply have to remember or recall them, in contrary to tokens which must be carried [8].

However, in the perspective of security and usability, text passwords have a number of cons. Passwords can be only secure if they are difficult for attackers to guess or predict. Many security policies must be applied to obtain such a deterrent system. An example of these policies according to an article published by Symantec [3] are:

- Length: A password's length should be from 6 to 9 characters
- Width: Complexity should be added to the password. In other words, it should contain letters (both uppercase & lowercase), numerals and special characters.
- Depth: Users should not use complete words; instead, they should use unguessable word-phrases that contain no personal information.
- Changing the Password: The password should be changed every month or two for financial account and every 3 or 4 months for regular users, and the password should not be used twice.

Moreover, many systems sometimes try to provide some help by:

- Giving on-screen advice on how to create more secure passwords.
- Giving a feedback about password choice, such as showing a password strength meter indicating the strength of the password.

- Forcing users to create passwords that comply with specific system-defined policies. [9]

But when such policies are applied, the password does not become only difficult to be stolen by attackers, but also difficult for the authenticated users to remember. This situation is defined as the “Password Problem" where despite the need for both secure and well-memorable passwords, most created passwords are either weak-and-memorable or secure-but-difficult-to-remember [9].

Actually, the password problem is a result of two main reasons:

- The fundamental limitations of human long-term memory.
- The lack of the security foresight in the users' perspective.

➢The fundamental limitations of human long-term memory

Once a password is chosen, the user must be able to remember it every time he wants to access the system. But people tend to forget their passwords due to the nature of the human memory [14]. The passage of time and retroactive interference are two main factors that emphasize this memory weakness, where not using the password for a while will make new items in memory replace or disrupt the existing ones or vice-versa [10].

A user is expected to choose a secure and complex password and learn and memorize it to be able to recall it when required. But by the time he learns such a password, the system will ask him to choose another one according to the security relegations of the system. This causes a disruption in the user’s memory where by the passage of time the memory becomes confused between the previous passwords and the current one, especially if his access of the system is not frequent. Actually, researches have shown that users do not forget the password completely. They tend to recall parts of it correctly, but still the complete password is required to obtain an access to the system [11].

➢ The lack of the security foresight in the users' perspective

Most users lack any security knowledge and they do not know or recognize the threats that online systems face every day. They visualize the password, or any authentication process, as an obstacle that is preventing or slowing them from accomplishing their main tasks. This leads them to try to use insecure methods to overpass the authentication process underestimating the severe results their actions can cause [9].Their created passwords tend to be short and usually contains the name of a family members or pets. Additionally, they tend to write down their passwords and keep it in a suitable place for them, most commonly on a sticker on their screen or on a small paper in the drawer, and give their password to his/her coworkers. Also, users create their own rules by adding a different to the same base word for each new password [12].

Moreover, in the case of multiple systems that require multiple authentication processes users tend to choose one password for all systems, reducing the security level to minimum and putting the user and his organization at risk of widespread damage if the password file of any of the accessed systems is breached [13].

These disadvantages encouraged developers to find new authentication methods. The best systems developed were those which depended on humans’ biometrics, but the main obstacle was its huge cost. So, researches continued until the concept of graphical passwords was introduced. Graphical Passwords replaced the input in text passwords with another input containing images. This implementation was developed from the fact that humans’ brain and their memory can remember images better than text.

2.2 Images vs. Text in Human Memory

One of the most famous quotes of Albert Einstein was “If I can’t picture it, I can’t understand it” [15]. This quote reflects the proposition that gives images and pictures the advantage over text when human interaction is involved.

Imagery is considered a primary sensory connection in the brain. Within our daily lives we are provided with an overflow of visual images from multiple sources such as the television, the Internet, the on-road billboards, and even the illustrations provided in students' textbooks. For example if instead of watching a TV show, we could only read the script, would the images we visualize while reading match those watched on the television? [15]

Through experience and experimentation, the understanding of the visual world and how we are influenced by it has increased. Psychologist Albert Mehrabian demonstrated that 93% of communication is nonverbal. Studies concluded that the human brain tends to receive and decipher images simultaneously, while text is decoded in a linearly, taking more time to process. [19]

Moreover, physically our brain has one memory. But practically it is divided into three sections:

- Sensory Memory
- Short-term Memory
- Long-term Memory

➢ Sensory memory

Sensory memory takes the information provided by the senses and retains it accurately but very briefly. Sensory memory lasts such a short time (from a few hundred milliseconds to one or two seconds). But it still represents an essential step for storing information in short-term memory.

➢ Short-term Memory

Short-term memory is considered as a scratch paper to temporary remembers the information processed at any time. But it can hold a small amount of information for a short duration in an active and ready state, usually not more than seven items for a maximum period of a minute.

This information will quickly disappear if an extra effort is not made towards the next stage of reservation, the long-term memory. [21]

➢ **Long-term Memory**

Long-term memory is for the storage of information over a long period of time. Despite the human's nature of forgetting, long-term memory actually is not destructed easily over time and can store an undefined amount of information. But still, it is not obvious whether we actually ever forget anything at all, or whether it just becomes increasingly difficult to access or retrieve certain items from memory [21].

Words are processed by our short-term memory which has been mentioned before can retain about 7 bits of information. This is why we have 7-digit phone numbers.

On the other hand, Images go directly to our long-term memory where they are usually engraved. Therefore, it is not surprising that it is much easier to show a circle than describe it. [19]

Actually, a study made by Nick Patel, an analytics expert, lead to the following conclusions that support the pre-mentioned proposition:

- Approximately 50% of the human brain is involved in visual processing. [18]
- 65% of people are visual learners that respond better to visual information than plain text. [18]
- High quality infographics are 30 times more likely to be read than text articles.
- The average person only read 20% of the words on a regular web page. [18]
- The use of visualized information has increased 9900% on the Internet between 2007 & 2013. [18]
- People following instructions with a visual element perform 323% better than those without. [18]
- Visual aids in the classroom improve learning up to 400%. [18]
- Moreover, researches made by Mindlab International, an independent research company, on brain waves of people completing certain tasks with the help of visual information lead to the following results:
- Individuals working with visual mapping techniques used on average 19% less cognitive resources. [20]
- They were 17% more productive and 4.5% better able to recall details than when using the equivalent traditional software. [20]
- They were 8% more productive and recalled 6.5% more data when using visual mapping compared with traditional techniques. [20]

2.3 Graphical Passwords

Based on the mentioned scientific researches that concluded that the human mind is more familiar with images than text, more researches were made to invent new authentication systems based on images instead of text. Graphical password was one of the alternatives introduced to replace text passwords.

Graphical passwords are divided into two main categories:

A.Recognition based methods

- Dhamija and Perring implementation
- Sobrado and Birget implementation
- Passfaces

B.Recall based methods

- Pure Recall
- Reproduce a drawing
- Cued Recall
- Repeat a sequence of actions: PassPoints

2.3.1 Recognition based Methods

In recognition based methods, users are given a set of pictures to pick from. Later during the authentication process, they should recognize and identify the pictures picked previously.

Several implementations were made based on the basics of these methods. Below are some examples of these implementations:

➢ **Dhamija and Perring implementation:**

This implementation was made based on the Hash Visualization technique that was based on using images in authentication. Dhamija and Perrig developed this technique trying to introduce a more secure simple authentication system.

The system should initially provide the user with a certain number of images generated randomly. The user is expected to select a certain number of images among those shown to him. This is considered as the registration process.

Later when the user wishes to log in to the system, he is shown again different images. He should recognize and identify the images he previously selected.

After making several studies, the following results were obtained:

- 90% of the participants succeeded logging in using the graphical password technique developed by Dhamija and Perring.
- 70% of the participants succeeded logging in using text passwords and PIN numbers.
- 18% of people use "1234", "0000", or "1111" as their PIN passwords(11% use "1234").[23]
- The average log-in time using graphical passwords is much longer than the time needed using text passwords or PIN numbers.

In case of the graphical password implementation, it is required to store a large amount of images. Also, it is well known that images require more space and capacity more than text. So in addition to the large capacity required on the disks when compared to that required in case of text, another drawback is the delay in the network caused by the time needed to load the images from the database server.

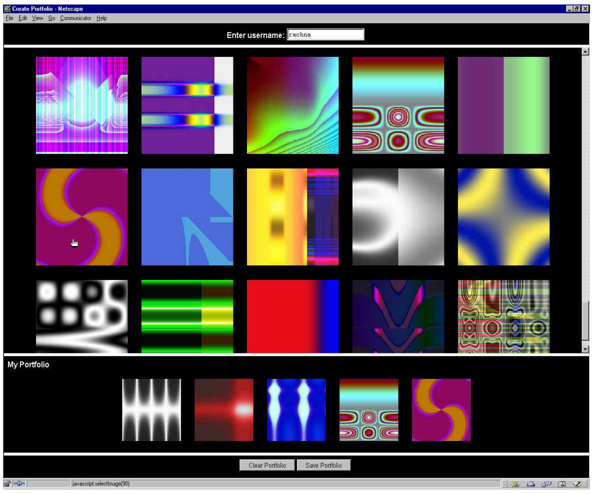

Figure 1: Déjà vu system: an example of Dhamija & Perring implementation

➢ Sobrado and Birget implementation:

To deal with the shoulder-surfing problem, Sobrado and Birget developed a new technique. Their new technique was based on the same concept used in the Dhamija implementation. But instead of using large-sized and limited random images, a large number of relatively smaller passobjects is used. The same instructions are required where the user should choose a certain number of passobjects, and later during authentication he should select these passobjects.

The main idea of this technique is to make the screen so crowded (Sobrado and Birget suggested using 1000 objects). This way, any person sneaking above the user's shoulder be confused and would not be able to concentrate on which objects the user selected. Also, the user should not have any problem finding the object since he should know exactly what to choose and would not be distracted by the crowd of passobjects.

On the other hand, there are still several drawbacks of this implementation:

- There will be delay over the network due to the large number of objects needed to be loaded.
- The log in process could be slow since the user knows the object he needs to select, but might need some time to find them if the objects' places is randomly changed.
- If a small number of objects is shown on the screen, the password space will be smaller leading to security vulnerabilities.

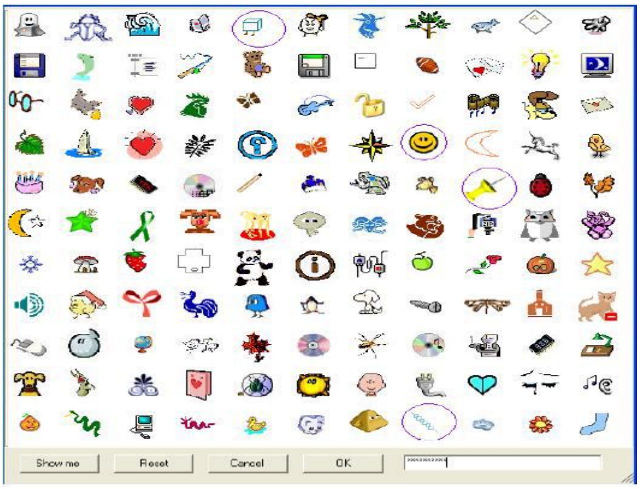

Figure 2:A shoulder surfing resistant scheme developed by Hong.

➢ Passfaces

Passface is another technique that depends on images, but the difference is that these images belong to human faces. It is based on studies that concluded that humans' faces are easier to remember than other images and that they are more memorable over long intervals.

The user is shown a set of images and he should choose a certain number of images. Later during authentication, a random set of human faces' images will be shown on the screen including both the selected images in addition to random false ones.Real Corporation suggested selecting 4 images during registration, and during authentication the user will be shown 4 sets of images. Each set will include 9 images: 1 pre-selected image and 8 decoy ones. The user must select the correct image in each challenge.

The main advantage of this technique is that users can identify human faces easily, but still there are many drawbacks:

- Most users tend to choose faces of people from the same race.
- Female faces were preferred by both male and female users.
- Better looking faces were more likely to be chosen.

These drawbacks forced the created passwords to create a certain pattern making the passwords more predictable.

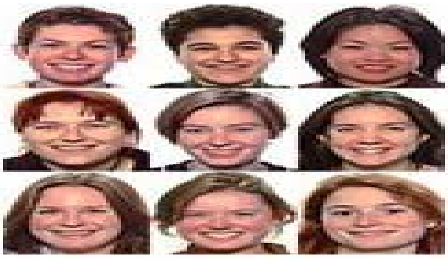

Figure 3: An example of Passfaces

2.3.2. Recall based Methods

➢ Pure Recall Methods

Pure recall based methods are similar to text passwords because users must remember their passwords and reproduce it without any hints or help from the system.

- **Reproducing a drawing: Draw-A-Secret (DAS)**

The user will be shown a new screen which should be divided into 2-dimension grids. Using a mouse or a stylus, the user must draw his unique password on this grid. The password can be drawn using one continuous stroke or multiple separate ones. The system will study the drawing to see in which grids it passed through. These active grids will be considered as the password. During authentication, the same process is repeated where starting from a blank grid the user is asked to reproduce his drawing. The user must not reproduce the same drawing identically, but his drawing must pass through the same previously mentioned grids that represent the password.

But when asking users to use this method by "Nali and Thorpe", the following drawbacks were noticed:

- Users tend to draw symmetric drawings.
- Users tend to produce their drawing in the middle of the grid.
- Users tend to use alphabetical characters and numbers as their drawing.

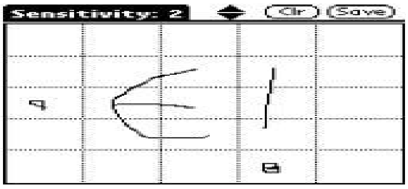

Figure 4: An example of DAS

➢ Cued Recall Methods

Cued recall methods are identical to pure recall methods except for that the user is initially given a cue or hint to start from.

- **Repeating a sequence of actions: PassPoints**

PassPoints is similar to DAS but instead of having a blank gridded screen, an image with no grids is shown. The user must select a set or sequence of click-points. These click-points are considered as the password. When logging in, the system displays the pre-mentioned initial image. The user is expected to click on the previously chosen click-points to authenticate his access.

Several add-ons can be added to this method to increase the security level:

- Force the user during authentication to enter his click-points in the same sequence he initially clicked.
- Adding another authentication phase by displaying several decoy images in addition to the user's image where the user should first choose the correct image before proceeding to the second authentication phase.

➢ Password Spaces

The password space is the set of all password combinations that can be created. In text passwords, systems have a password space that depends on the available characters (small and capital letters), symbolsand numbers which are counted as a total of 95. For example, in the case of an 8-character password, the password space is 95^8or 6.63x 10^{15} possible permutations. But actually, this is only the theoretical password space because not all these permutations have make sense. For example, ***\R9&i8/q***is one of these permutations, but it actually means nothing and it is almost impossible for any user to memorize or remember it. Actually, the meaningful words in English language is approximately 10^6. Moreover and out of these million words, only an approximate of 170000 [26][27] words are used by people. So if we suppose that each password created is made up of 2 paraphrases, the password space would be 2.88x 10^{10}. But in graphical passwords, all images or grids or passpoints are meaningful, so the theoretical permutation is the same as the practical.

3. Our proposed algorithm for graphical password form

- ❖ At first, a welcome screen will be shown on the screen asking the user if he is a new or a registered user.
- ❖ If he/she is a new user:
- A new screen will appear asking the user to enter some personal information in addition to choosing an ID or a username.
- Then the user is asked to create a password and then confirm it again.
- The request of creating a new user accompanied with this user's entered information is sent to the administrator to gain access to the system.
- If the administrator gives permission to this user, the ID, the password and the accompanied information are saved in the database.

Otherwise, the access is denied.

❖ **If he/she is a registered user:**

- A new screen will appear asking the user to enter his ID or a username.
- The system searches for the ID in the database.
  If it does not find the ID, it asks the user to enter it again.
- If the ID is found in the database, the user is asked to authenticate his identity by entering his password.
  If he enter the password incorrectly, he is allowed to enter the password again 2 more times and afterwards his access would be automatically denied.
- If the user enters the password correctly, his access is granted.

4. Our flowchart

See figure 5.

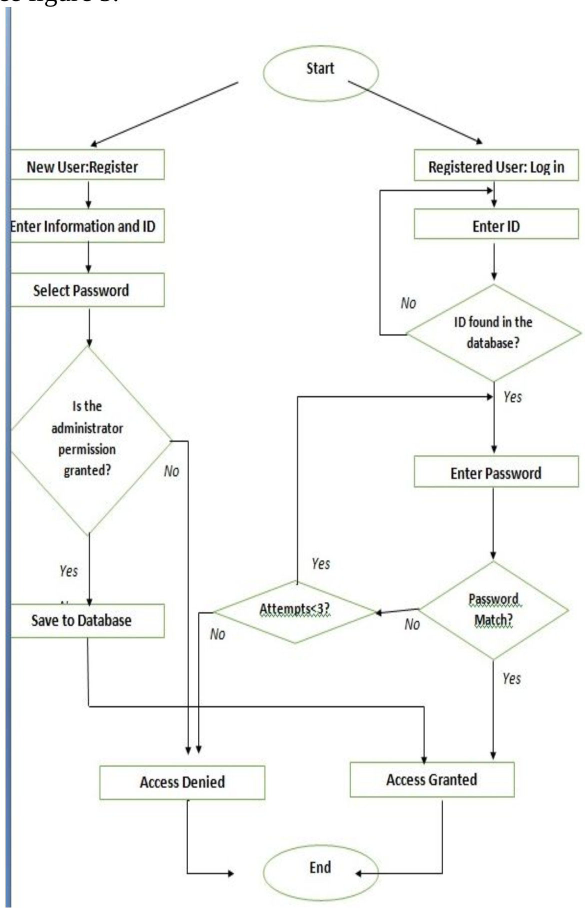

Figure 5 : Our FlowChart

5. Conclusion and Future Work

The past years have showed an interest in the attempt of spreading the graphical password authentication methods in order to replace text passwords. The main argument that such an approach is that the human memory can identify and remember images much better than text. Researches lead to developing many new implementations based on graphical passwords. As stated earlier in this article, many of these implementations have a bigger password than that of text passwords. This factor, one of many, made breaking graphical passwords using traditional attack methods (ex: dictionary attack, brute-force attack…) more difficult. Even some implementations proposed a solution for shoulder surfing. Despite its disadvantage of being a slow log-in operation, graphical passwords appear to be more secure. But this conclusion is not absolute because even though many researches are made continuously on this topic, but its main problems and disadvantages are not obvious yet. This is due to the limit in the number of users which depend on graphical passwords as their authentication methods. Moreover, attackers are now focusing on other authentication methods to breach, text passwords mainly. They will not be interested in giving their time and efforts to breach a method that is still not world widely spread.
In the future work we will test this algorithm on a system and then conclude based on statistics that attacking graphical passwords is not so easy, and memorizing graphical passwords is easier than text passwords.

References

[1]. A Design and Analysis of Graphical Password

[2]. UNDERSTANDING THE SECURITY TRIAD (CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY) BY DARRIL GIBSON MAY 27, 2011 HTTP://WWW.PEARSONITCERTIFICATION.COM/ARTICLES/ARTICLE.ASPX?P=1708668

[3]. The Simplest Security: A Guide To Better Password Practices
by Sarah Granger, last updated 05 Jul 2011 http://www.symantec.com/connect/articles/simplest-security-guide-better-password-practices

[4]. Pictures versus text: Modality effects across three levels of learning and study time Janet M Beagle, Purdue University 2009 http://docs.lib.purdue.edu/dissertations/AAI3402284/

http://search.proquest.com/docview/288429608

[5]. Recognition memory for words and picturesat short and long retention intervals,ROBERTE. GEHRING, MICHAELP. TOGLIA,andGREGORY A. KIMBLE, University ofColorado1976

[6]. USABLE AUTHENTICATION AND CLICKBASED GRAPHICAL PASSWORDS by Sonia Chiasson

A thesis submitted to the Faculty of Graduate Studies and Research in partial fulfillment of the requirements for the degree of DOCTOR OF PHILOSOPHY

School of Computer Science at CARLETON UNIVERSITY

[7]. A Survey of Password Attacks and Comparative Analysis on Methods for Secure Authentication By Mudassar Raza, Muhammad Iqbal, Muhammad Sharif and Waqas Haider Comsats Institute of Information Technology, Wah Cantt., 47040, Pakistan

World Applied Sciences Journal, 2012

[8]. K. Renaud. Evaluating authentication mechanisms. By K. Renaud, 2005In L. Cranor and

[9]. PassPoints: Design and longitudinal evaluation of a graphical password system By Susan Wiedenbecka, Jim Waters, Jean-Camille Birget, Alex Brodskiy, Nasir Memon

[10]. Wixted, J.T., 2004. The psychology and neuroscience of forgetting. Annual Review of Psychology 55, 235–269.

[11]. Sasse, M.A., Brostoff, S., Weirich, D., 2001. Transforming the 'weakest link'—a human/computer

Interaction approach to usable and effective security. BT Technical Journal 19, 122–131.

[12]. Adams, A., Sasse, M.A., 1999. Users are not the enemy. Communications of the ACM 42 (12), 41–46.

Bahrick, H.P., 1984. Semantic memory content in permastore: fifty years of memory for Spanish learned in

School. Journal of Verbal Learning and Verbal Behavior 14, 1–24.

[13]. Ives, B., Walsh, K.R., Schneider, H., 2004. The domino effect of password reuse. Communications of theACM 47 (4), 76–78.

[14]. Bahrick, H.P., 1984. Semantic memory content in permastore: fifty years of memory for Spanish learned in

School. Journal of Verbal Learning and Verbal Behavior 14, 1–24

[15]. Comprehension Strategies Visualizing & Visual Literacy

By Debbie Draper, DECS Curriculum Consultant, Northern Adelaide - 2010

[16]. Brain Rules – John Medina – June 2013

[17]. Infographics and the Science of Visual Communication by Mark Smiciklas

[18]. Your Brain on Visualizationby Neil Patel on August 8, 2013

[19]. The Power of Visual Communication by Mike Parkinson

[20]. Images vs text for getting your message across by Fiona Graham – Technology of Business reporter

[21]. The Brain from Top to Bottom (McGill University)

http://thebrain.mcgill.ca/

[22]. An experimental survey and comparison of proof by knowledge authentication techniques Stamati Gkarafli and Anastasios A. Economides

[23]. http://www.businessinsider.com/too-many-people-still-use-1234-as-pin-code-2013-8

[24]. T. Valentine, "An evaluation of the Passface personal authentication system," Technical Report, Goldsmiths College, University of London 1998.

[25]. T. Valentine, "Memory for Passfaces after a Long Delay," Technical Report,

Goldsmiths College, University of London 1999.

[26]. http://www.lingholic.com/how-many-words-do-i-need-to-know-the-955-rule-in-language-learning-part-2/

[27]. http://www.oxforddictionaries.com/words/the-oec-facts-about-the-language

[28]. http://arstechnica.com/security/2012/12/25-gpu-cluster-cracks-every-standard-windows-password-in-6-hours/

[29]. A VISUAL DICTIONARY ATTACK ON PICTURE PASSWORDS By Amir Sadovnik and Tsuhan Chen; Department of Electrical and Computer Engineering, Cornell University