A survey on usability and security features in graphical user authentication algorithms

ARASH HABIBI LASHKARI and SAMANEH FARMAND

University Malaya (UM), Kuala Lumpur, Malaysia

Summary
Nowadays, user authentication is one of the important topics in information security. Text-based strong password scheme can provide security to a certain degree. However, the fact that strong passwords being difficult to memorize often leads their owners to write them down on papers or even save them in a computer file. Graphical authentication has been proposed as a possible alternative solution to text-based authentication, motivated particularly by the fact that humans can remember images better than text. Recently, many networks, computer system and Internet-based environments try using graphical authentication techniques as their user's authentication. Graphical passwords have two essential aspects, usability and security. Unfortunately till now none of the proposed algorithms were able to cover both of them simultaneously. This paper presents a review on the security and usability features of graphical password authentication schemes. In this study we surveyed 23 papers and explained the problems, solutions, findings and future work recommended in each paper. In the next paper we will cover a new model supporting security and usability together.

Keywords
User Authentication, Graphical User Authentication, Graphical Password, Usability, Security.

1. Introduction

User authentication is one of the important topics in information security to protect users' privacy. Computer security depends on trustworthy user authentication to a degree. There are many authentication schemes in the current state. Some of them are based on user's physical and behavioural properties, and some other are based on user's knowledge such as textual and graphical passwords. Moreover, there are some other important authentication models that are based on what you have, such as smart cards. Among the various authentication designs, textual password and token-based schemes, or the combination of both, are commonly applied. However, as it is explained in the following, both authentication patterns are vulnerable to certain attacks. Nowadays the most common computer authentication method to access to computer networks and systems is based on the use of alphanumerical usernames and passwords. Traditional strong password schemes could provide with certain degree of security; however, the fact that strong passwords being difficult to memorize often leads their owners to write them down on papers or even save them in a computer file. As a result, security becomes greatly compromised.

Conventional passwords have been shown to have significant drawbacks. Users do not follow their requirements, for example; users tend to pick passwords that can be easily guessed (weak password) or choose meaningful words from dictionaries, which make textual passwords easy to break and vulnerable to dictionary or brute force attacks. On the other hand, if a password is hard to guess, then it is often hard to remember. Users have difficulty remembering a password that is long and random appearing. So, they create short, simple, and insecure passwords that are susceptible to attack. Textual-based password authentication scheme tend to be more vulnerable to attacks such as shoulder-surfing, hidden camera, spyware attacks and key-loggers. Moreover, the alphanumeric characters and authentication methods based on passwords and PINs (knowledge-factor authenticators) hold severe problems and still must rely on the limitation of human's capacity of recollection. Forcing the user to memorize different passwords or carrying around different tokens is another sensitivity of traditional methods. Smart cards or tokens can be stolen. On the other hand, many biometric authentications have been proposed; however, users tend to resist using biometrics because of their intrusiveness and the effect on their privacy. Moreover, biometrics cannot be revoked.

To address this problem, some researchers have developed authentication methods that use pictures as passwords and introduced it as possible alternative solutions to text-based scheme. On the other hand, knowing that human beings are predominant visual creatures, many researchers have investigated or developed graphical password schemes recently. Graphical passwords have been designed to try to make passwords more memorable and easier for people to use, to create and, therefore, more usable and secure. Many available graphical passwords have a password space that is less than or equal to the textual password space. Using a graphical password, users click on images to authenticate themselves rather than type alphanumeric strings. This method has been categorised to recognition-based (image selection and click-based) and recall-based. Usability and security should be considered simultaneously to achieve a good authentication system.

Manuscript received September 5, 2009
Manuscript revised September 20, 2009

Usability features are ease of use, ease to create, ease to memorise, ease to learn and satisfaction of the overall system design and layout. User friendliness in both recognition and selection of pass-objects from the given images, familiarization or a lengthy password setup process can be counted under usability.
Common security attacks like brute-force search, spyware, shoulder surfing, social engineering, and forgery. Problems like requiring a large image database, uneasy to repeat mouse clicking at the same position, as well as images being too simple to cause collisions on points selected for different users, storage-efficient as all images are created when needed.
Rather than optimizing the password space and the strength against brute force attacks because proposed graphical passwords are mostly vulnerable to shoulder-surfing overcoming this issue without adding any extra complexity into the authentication procedure is researcher's goal these days.
Simply adopting graphical password authentication also has some drawbacks therefore some hybrid schemes based on graphic and text were developed. Moreover, image based authentication is considered as a promising alternative to traditional textual password for mobile devices, to achieve better trade-off between usability and security. However, previous proposals of graphical password have the limitation of limited entropy. Achieving higher security with compromising user-friendliness for mobile application scenarios and obtaining a significant improvement in terms of system security (both password entropy and shoulder-surfing attacks) are important objectives.
Furthermore, there are many authentication schemes that are currently under study and they may require additional time and effort to be applicable for commercial use.

2. Security

In this part, we will explain eleven articles from security section of graphical password by focusing on problems, solutions and their findings.

Problem [1]: Size of the password space in DAS [1].
Methodology used: They studied the impact of selected parameters on the size of the password space for "Draw-A Secret" (DAS) graphical passwords. They examined the role of and relationships between the number of composite strokes, grid dimensions, and password length in the DAS password space. They showed that a very significant proportion of the DAS password space depends on the assumption that users will choose long passwords with many composite strokes.
To strengthen security, they proposed a technique and described a representative system that may gain up to 16 more bits of security with an expected negligible increase in input time [1].
Findings/Outcome: If users choose passwords having 4 or fewer strokes, with passwords of length 12 or less on a 5 × 5 grid, instead of up to the maximum 12 possible strokes, the size of the DAS password space is reduced from 58 to 40 bits. Additionally, they found a similar reduction when users choose no strokes of length 1.
Their results can be directly applied to determine secure design choices, graphical password parameter guidelines, and in deciding which parameters deserve focus in graphical password user studies They believe that this work significantly extends and compliments existing analysis/understanding of DAS graphical passwords – comparing the bit-size of the probable password space showed that a more viable graphical password attack strategy follows from their present results than that of using symmetry alone. They believe that without taking these results into consideration, the practical security of DAS implementations may be over-estimated [1].
Future Work: Further study is required to determine how complexity properties (e.g. grid dimensions, password length, number and direction of composite strokes) impact memorability and user choice in passwords. Psychological and user studies could be examined for how the complexity properties of drawings affect memorability, giving direction as to which complexity properties may be relaxed to encourage users to choose passwords consisting of more strokes. Alternatively, research is required to determine whether mnemonic strategies exist for graphical passwords to aid memorization of complex graphical passwords. Research to determine how such mnemonic strategies affect memorability would be useful, similar to that performed by Yan et al. for textual passwords [1].

Problem [2]: To overcome the shoulder-surfing attack issue without adding any extra complexity into the authentication procedure [2].
Methodology used: In line with the recent call for technology on Image Based Authentication (IBA) in JPEG committee, they presented a novel graphical password design in this paper. It rests on the human cognitive ability of association-based memorization to make the authentication more user-friendly, comparing with traditional textual password. Based on the principle of zero-knowledge proof protocol, they further improved the primary design (scheme) to overcome the shoulder-surfing attack issue without adding any extra complexity into the authentication procedure. System performance analysis and comparisons were presented to support their proposals [2].
Future Work: The future work includes conducting user studies and experiments to examine the effectiveness of their methods [2].

Problem [3]: Recently, various types of personal authentication methods have been studied to confirm a persons' identity in the on-line system. However, the

alphanumeric characters and authentication methods based on passwords and PINs (knowledge-factor authenticators) hold severe problems and still must rely on the limitation of human's capacity of recollection. Recently, "graphical password", using visual information for authentication methods that utilize photographic image for authentication, has been proposed. However this method holds some problem on security [3].

Methodology used: In this paper, they proposed "COMPASS" (COMmunity Portrait Authentication SyStem) that uses a portrait as the authentication image, to solve the issues of the previous graphical passwords. COMPASS has two features, i.e. use of portrait as the authentication image and the idea of the "community authentication" that a member of a certain community consisting of a party of human can be authenticated. The validity of the proposed method is confirmed by a set of subject experiments [3].

Findings/Outcome: As a result, it is confirmed that outsiders can be excluded effectively, by using the portrait. However, increase in the probability of insider's exclusion was also recognized [3].

Future Work: In the future they plan to make further studies on the applicability of the proposed method. For example, they plan to examine the relationship between the threshold in the elapsed time for answer and characteristics of the authentication, to compare with the other image encoding method, and to investigate the combination with the other information such as hints of the image [3].

Problem [4]: Conventional remote user strong-password authentication schemes have the common drawback that the user has to memorize a hard-to-remember textual password, and therefore their applications are restricted [4].

Methodology used: To solve this problem, they proposed a remote user authentication scheme using strong graphical passwords in this paper. As graphical passwords are easy to remember for the user and conventionally dictionary attacks on graphical passwords are infeasible, the practicability of the proposed scheme is improved. Next, they showed that the proposed scheme can withstand the replay attack, the password- file compromise attack, the denial-of-service attack, the predictable n attack, and the insider attack. In particular, the proposed scheme is easily reparable. Note that this method is secure under the assumption that the easy to-remember DAS password is strong [4].

Future Work: Although conventionally dictionary attacks on graphical passwords are infeasible because there are no existing workable dictionaries for graphical information, its resistance to specific graphical dictionary attacks, has to be analyzed in future research [4].

Problem [5]: virtual three-dimensional environment. To have a scheme that has a huge password space while also being a combination of any existing, or upcoming, authentication schemes into one scheme [5]

Methodology used: Textual passwords and token-based passwords are the most commonly used authentication schemes. However, many different schemes have been used in specific fields. Other designs are under study yet they have never been applied in the real world. In this paper, they proposed and evaluated their contribution which is a new scheme of authentication. This scheme is based on a virtual three-dimensional environment.

The motivation of this work is to have a scheme that has a huge password space while also being a combination of any existing, or upcoming, authentication schemes into one scheme. Users navigate through the virtual environment and interact with items inside the virtual three-dimensional environment. The combination of all interactions, actions and inputs towards the items and towards the virtual three-dimensional environment constructs the user's 3D password. The 3D password combines most existing authentication schemes such as textual passwords, graphical passwords, and biometrics into one virtual three-dimensional environment. The 3D password's main application is the protection of critical resources and systems [5].

Findings/Outcome: The main application domains of 3D Password are critical systems and resources. Critical systems such as military facilities, critical servers and highly classified areas can be protected by 3D Password system with large three-dimensional virtual environment. Moreover, a small three-dimensional virtual environment can be used to protect less critical systems such as handhelds, ATM's and operating system's logins. Acquiring the knowledge of the probable distribution of a user's 3D password might show the practical strength of a 3D password [5].

Future Work: The 3D password is in its infancy. A study on a large number of people is required. They are looking at designing different three-dimensional virtual environments that contain objects of all possible authentication schemes. Moreover, finding a solution for shoulder surfing attacks on 3D passwords and other authentication schemes is also a field of study [5].

Problem [6]: Users tend to pick short passwords or passwords that are easy to remember, which makes the passwords vulnerable for attackers to break. Furthermore, textual password is vulnerable to shoulder-surfing, hidden-camera and spyware attacks. Graphical password schemes have been proposed as a possible alternative to text-based scheme. However, they are mostly vulnerable to shoulder-surfing too [6].

Methodology used: In this paper, they proposed a Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme (S3PAS). S3PAS seamlessly integrates both graphical and textual password schemes and provides nearly perfect resistant to shoulder-surfing,

hidden-camera and spyware attacks. It can replace or coexist with conventional textual password systems without changing existing user password profiles. Moreover, it is immune to brute-force attacks through dynamic and volatile session passwords. S3PAS shows significant potential bridging the gap between conventional textual password and graphical password and can accommodate various lengths of textual passwords, which requires zero-efforts for users to migrate their existing passwords to S3PAS. Further enhancements of S3PAS scheme are proposed and briefly discussed. Theoretical analysis of the security level using S3PAS is also investigated [6].

Findings/Outcome: However, there are still some minor drawbacks in this system similar to other graphical password schemes. The major issues in S3PAS schemes include slightly more complicated and longer login processes. They planned to design a simplified version of S3PAS with a little other security level to ease its adoption [6].

Problem [7]: Current authentication systems suffer from many weaknesses. Textual passwords are commonly used; however, users do not follow their requirements. Users tend to choose meaningful words from dictionaries, which make textual passwords easy to break and vulnerable to dictionary or brute force attacks. Many available graphical passwords have a password space that is less than or equal to the textual password space. Smart cards or tokens can be stolen. Many biometric authentications have been proposed; however, users tend to resist using biometrics because of their intrusiveness and the effect on their privacy. Moreover, biometrics cannot be revoked [7].

Methodology used: In this paper, they presented and evaluated their contribution, i.e., the 3-D password. It is a multifactor authentication scheme. To be authenticated, they presented a 3-D virtual environment where the user navigates and interacts with various objects. The sequence of actions and interactions toward the objects inside the 3-D environment constructs the user's 3-D password. The 3-D password can combine most existing authentication schemes such as textual passwords, graphical passwords, and various types of biometrics into a 3-D virtual environment. The design of the 3-D virtual environment and the type of objects selected determine the 3-D password key space [7].

Findings/Outcome: The 3-D password is a multifactor authentication scheme that combines various authentication schemes into a single 3-D virtual environment. The virtual environment can contain any existing authentication scheme or even any upcoming authentication schemes by adding it as a response to actions performed on an object. Therefore, the resulted password space becomes very large compared to any existing authentication schemes. The design of the 3-D virtual environment, the selections of objects inside the environment, and the object's type reflect the resulted password space. It is the task of the system administrator to design the environment and to select the appropriate object that reflects the protected system requirements. Additionally, designing a simple and easy to use 3-D virtual environment is a factor that leads to a higher user acceptability of a 3-D password system. The choice of what authentication schemes will be part of the user's 3-D password reflects the user's preferences and requirements. A user who prefers to remember and recall a password might choose textual and graphical passwords as part of their 3-D password. On the other hand, users who have more difficulty with memory or recall might prefer to choose smart cards or biometrics as part of their 3-D password. Moreover, users who prefer to keep any kind of biometrical data private might not interact with objects that require biometric information. Therefore, it is the user's choice and decision to construct the desired and preferred 3-D password [7].

Future Work: The 3-D password is still in its early stages. Designing various kinds of 3-D virtual environments, deciding on password spaces, and interpreting user feedback and experiences from such environments will result in enhancing and improving the user experience of the 3-D password. Moreover, gathering attackers from different backgrounds to break the system is one of the future works that will lead to system improvement and prove the complexity of breaking a 3-D password. Moreover, it will demonstrate how the attackers will acquire the knowledge of the most probable 3-D passwords to launch their attacks. Shoulder surfing attacks are still possible and effective against 3-D passwords. Therefore, a proper solution is a field of research [7].

Problem [8]: In click-based graphical password schemes that allow arbitrary click locations on image, a click should be verified as correct if it is close within a predefined distance to the originally chosen location. This condition should hold even when for security reasons the password hash is stored in the system, not the password itself [8].

Methodology used: To solve this problem, a robust discretization method has been proposed, recently. In this paper, they showed that previous work on discretization does not give optimal results with respect to the entropy of the graphical passwords then proposed a new discretization method to increase the password space and optimize the strength against brute force attacks. To improve the security further, they also presented several methods for click-based graphical passwords that use multiple hash computations for password verification. In the first of these methods, by considering each x and y values of user clicks separately, they succeeded in selecting optimum offset values for discretization. The method they have proposed increases the password space by 32c where c is the number of clicks. As a second method, instead of using hash

iterations to slow down the brute force search, they showed that discretization errors can be allowed to have a similar security improvement. They also proved the maximum upper limit for this improvement with methods using discretization errors [8].

Problem [9]: Recognition-Based Graphical password**.**
Methodology used: Most common computer authentication method is traditional 'User Name' and 'password'. Numerous Biometric authentication methods were also proposed. In this paper, they proposed.
In this paper, they conducted an extensive survey of the existing graphical password schemes and proposed a novel and new alternative; Figure as a Password. In this scheme users will get complete freedom to select their Passwords. Entire work can be' divided into three phases- a. sampling of users passwords, processing and storage; b. security on transmission; and. c. Recognition and authentication. They used the Recognition based technique in Graphical Password Scheme. Their work suggested that password is difficult to break. The entire system is checked and tested repeatedly with the desired output. Processing speed also improved in their scheme, because of digitization of data. Issue relating privacy and accuracy are tested. Technical aspects are analyzed and operations are validated and verified with numerous samples [9].
Findings/Outcome: Their scheme supports the application environment and they strongly believe that "User Authentication by Secured Graphical Password Implementation" could be a solid platform for future research and study [9].

Problem [10]: In this paper, they presented and evaluated various methods for purely automated attacks against click-based graphical passwords [10].
Methodology used: Their purely automated methods combine click-order heuristics with focus-of-attention scan-paths generated from a computational model of visual attention.
They provided what appears to be the best automated attack against Pass-Points style graphical passwords to date. Click-order patterns, DIAG and LINE, combined with their laziest relaxation rule, yielded highly effective dictionaries. They were able to further reduce the dictionary size while retaining some accuracy using Ittietal's computational model of bottom-up visual attention [10].
Findings/Outcome: Their method resulted in a significantly better automated attack than previous work, guessing 8-15% of passwords for two representative images using dictionaries of less than 224.6 entries, and about 16% of passwords on each of these images using dictionaries of less than 231.4 entries (where the full password space is 243). Relaxing their click-order pattern substantially increased the efficacy of their attack albeit with larger dictionaries of 234.7 entries, allowing attacks that guessed 48-54% of passwords (compared to previous results of 0.9% and 9.1% on the same two images with 235 guesses). These latter automated attacks are independent of focus-of-attention models, and are based on imagine dependent guessing patterns. Their results showed that automated attacks, which are easier to arrange than human seeded attacks and are more scalable to systems that use multiple images, pose a significant threat [10].
Future Work: Their overall results indicate that although essentially no users choose their click-points in the strict scan-path order of Itti's model of visual attention, when all permutations of points in the scan-path are considered, it models a meaningful percentage (from an attacker viewpoint) of user passwords. This raises interesting questions regarding how visual attention relates to user choice in graphical passwords. Their results would be consistent with the hypothesis that bottom-up visual attention is a factor in user choice for some users (and/or for some images), but not necessarily for all users. It would be interesting to further explore whether there are top-down models under various plausible assumptions, that may more accurately model user choice. For example, might the first point be chosen according to bottom-up visual attention, and then the rest chosen in a top-down manner such that they are somehow similar to the first? Alternately, might the entire process be top-down, based on whether the user can find five objects that are similar in some way? Such a top-down theory would be substantially more difficult to model an attack on, but if possible to implement, its results would offer interesting insight [10].

Problem [11]: Textual-based password authentication scheme tend to be more vulnerable to attacks such as shoulder-surfing and hidden camera. To overcome the vulnerabilities of traditional methods, visual or graphical password schemes have been developed as possible alternative solutions to text-based scheme. Because simply adopting graphical password authentication also has some drawbacks, some hybrid schemes based on graphic and text were developed [11].
Methodology Used: In this paper, they proposed a stroke-based textual password authentication scheme. It uses shapes of strokes on the grid as the origin passwords and allows users to login with text passwords via traditional input devices. The method provides salient features as a secure system for authentication immune to shoulder-surfing, hidden camera and brute force attacks. Moreover, the scheme has flexible enhancements to secure the authentication process. The analysis of the security of this approach is also discussed. It has variants to strengthen to security level through changing the login interface of the system [11].
Findings/Outcome: However, the system still has some drawbacks. Firstly, this method is relativity unfamiliar to the general people so that the users may adopt the simple and weak strokes as their passwords. Secondly, the process of creating original password is more vulnerable than the login step. Thirdly, the login process is longer than other

graphical schemes. To address these issues, they should design more advanced authentication system to improve this method [11].

3. Usability

In this part, we will explain four articles from usability section of graphical password by focusing on problems, solutions and their findings.

Problem [1]: Access to computer networks and systems is most often based on the use of conventional passwords nowadays. However, users have difficulty remembering a password that is long and random appearing. So, they create short, simple, and insecure passwords [12].

Methodology used: Graphical passwords have been designed to try to make passwords more memorable and easier for people to use, create and, therefore, more usable and secure. Using a graphical password, users click on images rather than type conventional passwords.

In this paper, they have designed a usable graphical password system focusing on the usability features to the users, called Jetafida. Its security feature was also an important issue but they did not touch the security point in this design.

The system usability features had been tested by questionnaire survey. This is done by thirty computer students participates who used the system for three times in different times to see the usability features achieved in the system. These features were ease of use, ease to create, ease to memorize, ease to learn and the overall system design and layout [12].

Findings/Outcome: The results showed that the participants found the proposed usable graphical password system has been achieving the usability features built in.

Finally, they can say regarding to the questionnaire results that the Jetafida graphical password system is a usable graphical password system which carries the most important usability features for the users [12].

Future Work: From the viewpoint of security, more study of the new kinds of attacks against this proposed system is needed [12].

Problem [2]: Usability features of the existing recognition base graphical password methods.

Methodology used: Graphical passwords are an alternative authentication method to alphanumeric passwords in which users click on images to authenticate themselves rather than type alphanumeric strings.

In this paper they studied the recognition base graphical password type with the available methods from the usability point of view to extract the usability features from the previous studies and surveys. Then they matched the usability features (General usability features, existing usability features for existing graphical password methods, and ISO usability features) to the existing graphical password methods and made a comparison study between these methods and the usability features. They recommend new features that can be built in the new graphical password systems [13].

Findings/Outcome: They have found that there is no method that has the most important usability features. Thus, by completing this study a set of usability features is suggested to be in one graphical password system. This set includes the ease of use, memorize, creation, learning and satisfaction. They suggested that they should be implemented in any new usable graphical password system [13].

Future Work: This work proposes to build a new system of graphical password system that provides promising usability features [13].

Problem [3]: This paper will provide an analysis of a survey on picture attributes based on user's affinity of choice [14].

Methodology used: In this paper, they conducted a picture attributes survey. Evaluated picture attributes were picture size, picture presentation, and picture category. The objective of this survey was to collect and analyze the affinity of choice as selected by the users. They also conducted a priority test in order to investigate which picture category has the highest interest; which will be included into their graphical password scheme.

There are 63 respondents involved in this survey. The respondents were from the Faculty of Computer Science and Information Systems (FSKSM) of University of Technology Malaysia, including staff members, undergraduate and postgraduate students. The sample involved 27 males and 36 females, with ages ranging from 18 to 30 years. All the respondents were frequent users of personal computers (PCs). The picture attributes information will be analyzed and selected information will be embedded into their graphical password scheme [14].

Findings/Outcome: As a result, three highest categories, which are people, nature and animal, are compulsory to be included in the scheme. The remaining categories which are entertainment and miscellaneous, contain the seven themes, sport, movie, animation, car, food, signage and flag. Arguably, not all of these themes will be selected. Only themes that are highly selected will be used. These are movie, animation, car and food themes. Although these fewer themes are not the highest priority, the themes still need to be included but the quantities are less than the highest priorities [14].

Problem [4]: Usability in Draw a secret Graphical Password.

Methodology used: This paper presents a sketch-based password authentication system called Scribble-a-Secret as a graphical password scheme in which free-form drawings are used as a means to authenticate users. Unlike existing schemes, this approach requires no input of graphical

passwords in particular sequences of strokes. Moreover, the system allows for a modicum of variation when users recreate their passwords. Their technique uses edge orientations extracted from sketch images to discern one user from another [15].

Findings/Outcome: The result of their experiments using data collected from 87 individuals showed that their recognition technique is robust for recognizing sketches while differentiating from others with both a false acceptance rate and false rejection rate of less than 1%. These edge orientation pattern features can robustly distinguish a user's sketches from others, absorbing the variations in a modicum of orientations and positions. Moreover, requesting users to input a few sketches for the creation of template enables the system to absorb the variations, resulting in lower FAR (False Acceptance Rate) and FRR (False Rejection Rate) rates [15].

Future Work: An important future task is to address the problem of shoulder-surfing. With the current work, it remains an open question how forgeable a password is when confronted with either a shoulder-surfing attack or some other mode to infer or steal the password. Another important issue is the ability of users to recall sketches when users are requested to remember them over a period of time and/or to remember multiple drawing passwords for different accounts. In future research, they plan to explore these directions [15].

4. Both security and Usability

In this part, we survey on eight articles which working on both of security and usability features in graphical password by focusing on problems, solutions and their finding.

Problem [1]: The most common computer authentication method is to use alphanumerical usernames and passwords. This method has been shown to have significant drawbacks. For example, users tend to pick passwords that can be easily guessed. On the other hand, if a password is hard to guess, then it is often hard to remember [16].

Aim/Objectives: To address this problem, some researchers have developed authentication methods that use pictures as passwords. In this paper, they conduct a comprehensive survey of the existing graphical password techniques which in the past decade has seen a growing interest in using graphical passwords as an alternative to the traditional text-based passwords [16].

Findings/Outcome: They classified these techniques into two categories: recognition-based and recall based approaches. They discussed the strengths and limitations of each method and point out the future research directions in this area. They also tried to answer two important questions: "Are graphical passwords as secure as text-based passwords?"; "What are the major design and implementation issues for graphical passwords?" This survey will be useful for information security researchers and practitioners who are interested in finding an alternative to text-based authentication methods. At the end a comparison of current graphical password techniques is presented [16].

Future Work: Although the main argument for graphical passwords is that people are better at memorizing graphical passwords than text-based passwords, the existing user studies are very limited and there is not yet convincing evidence to support this argument. Their preliminary analysis suggested that it is more difficult to break graphical passwords using the traditional attack methods such as brute force search, dictionary attack or spyware. However, since there is not yet wide deployment of graphical password systems, the vulnerabilities of graphical passwords are still not fully understood. Overall, the current graphical password techniques are still immature. Much more research and user studies are needed for graphical password techniques to achieve higher levels of maturity and usefulness [16].

Problem [2]: Blonder's graphical passwords generalization robustness problem [17].

Methodology used: This paper generalizes Blonder's graphical passwords to arbitrary images and solves a robustness problem that this generalization entails which made this type of password more usable. The password consists of user-chosen click points in a displayed image. In order to store passwords in cryptographically hashed form, they needed to prevent small uncertainties in the click points from having any effect on the password. They achieved this by introducing a robust discretization, based on multi grid discretization.

Findings/Outcome: This enabled them to produce a unique output of the password, despite the fact that users are not able to input exactly the same graphical password at each login. This enabled the system to store graphical passwords in cryptographically hashed form [17].

Problem [3]: Computer security to a degree depends on trustworthy user authentication; unfortunately currently used passwords are not completely secure or user friendly. One of the main problems with passwords is that good passwords are hard to remember and the ones which are easy to remember are too short to be secure [18].

Methodology used: They have designed a graphical authentication schema with a password, which is easy to remember and can be relatively quickly provided to the system, while at the same time remaining impossible to break with brute force alone. They have also proposed a way to measure password length and compared password space sizes of many popular authentication schemas against the one proposed in this paper [18].

Findings/Outcome: Their comparison results between password space and password length for popular user

authentication schemas and for the approach proposed in this paper shows that the presented approach is both most secured and the easiest to remember. At the same time, it is relatively fast to produce during an authentication procedure. With the goal of total computer and network security user authentication is only the first step. A good intruder detection mechanism is also required to protect the system against those who were able to defeat its identification mechanisms [18].

Future Work: Their previous research [November 4, 2005] presented a system for continuous user verification based on user's behaviour and promises to provide improved system security then coupled with the proposed user authentication approach. Integration of those two methodologies into a single security system is the next step in their continuing quest into making computers and computer networks more secure [18].

Problem [4]: User authentication is one of the important topics in information security. Traditional strong password schemes could provide with certain degree of security; however, the fact that strong passwords being difficult to memorize often leads their owners to write them down on papers or even save them in a computer file. As a result, security becomes greatly compromised [19].

Methodology used: On the other hand, knowing that human beings are predominant visual creatures, many researchers have investigated or developed graphical password schemes recently. In this paper, they proposed a graphical password scheme for user authentication using images with random tracks of geometric shapes (RGGPW). Their method not only is more secure than most of the existing graphical password schemes, it also solves problems like requiring a large image database, uneasy to repeat mouse clicking at the same position, as well as images being too simple to cause collisions on points selected for different users. They showed the images to demonstrate user friendliness in both recognition and selection of pass-objects from the given images [19].

Findings/Outcome: The proposed graphical password random geometric graphical password RGGPW is indeed robust against common security attacks like brute-force search, spyware, shoulder surfing, social engineering, and forgery. In addition, RGGPW is storage-efficient as all images are created when needed [19].

Future Work: They are currently working on how to create images with more complex tracks and easier recognizable objects. They will also implement a website to test the acceptance of this technique [19].

Problem [5]: Text-based passwords are ubiquitous authentication system. This traditional authentication system is well-known for its flaws in the aspects of usability and security issues that bring problems to users. Hence, there is a need for alternative mechanism to overcome these problems [20].

Methodology used: Graphical passwords, which consist of clicking or dragging activities on the pictures rather than typing textual characters, might be the option to overcome the problems that arise from the text-based passwords system.

In this paper, a comprehensive study of the existing graphical password techniques was performed. They compared and categorized (classified) these schemes into two groups; recognition-based scheme and recall based scheme. They also listed out several usability and security features for research continuity in this area. Their approach was to provide a scheme that will be able to satisfy the users' needs and requirements. [20].

Findings/Outcome: They have found that the graphical passwords designs are more difficult to be cracked by using the traditional attack methods such as brute force search, dictionary, social engineering and spyware attack. Some user and empirical study have proven that human are better at memorizing graphical passwords compared to textual characters passwords. They strongly believe that, to achieve such condition that usability and security features should be balanced [20].

Problem [6]: Alphanumeric passwords are widely used in computer and network authentication to protect users' privacy. However, it is well known that long, text-based passwords are hard for people to remember, while shorter ones are susceptible to attack [21].

Methodology used: Graphical password is a promising solution to this problem. Draw-A-Secret (DAS) is a typical implementation based on the user drawing on a grid canvas. Currently, too many constraints result in reduction in user experience and prevent its popularity. A novel graphical password strategy Yet another Graphical Password (YAGP) inspired by DAS was proposed in this paper and some preliminary experiments were carried out. The proposal has the advantages of free drawing positions, strong shoulder surfing resistance and large password space. Experiments illustrated the effectiveness of YAGP. In a 48×64 grid, the secret drawings can be described in detail. The users can concentrate on the drawing to improve user experience because exact positions are not required in YAGP [21].

Findings/Outcome: The results showed that YAGP achieves an encouraging performance in usability and security and possesses a high resistance to shoulder surfing. Meanwhile, the algorithm proposed in YAGP is trend-sensitive which actually reflects drawing trends. Furthermore, user personalities have a great influence on the drawings and therefore make it harder for others to imitate. Additionally, users can draw the secrets small enough to resist shoulder surfing [21].

Future Work: The main drawback of YAGP is that it's hard to redraw the password precisely. The legal user cannot always be assured to login successfully because the gaps between user drawings are uncertain while the

similarity threshold value is fixed. Future research will concentrate on improving YAGP as well as developing a comparison algorithm of higher efficiency in distinguishing the legal user from attackers [21].

Problem [7]: Graphical password (i.e., image based authentication) is considered as a promising alternative to traditional textual password for mobile devices, to achieve better trade-off between usability and security. However, previous proposals of graphical password have the limitation of limited entropy [22].

Methodology used: In this paper, they proposed a new scheme incorporating user face based authentication into the association-based graphical password solution they proposed before, aiming at achieving higher security without compromising user-friendliness for mobile application scenarios. System performance analysis and comparisons with other schemes are presented to validate their scheme [22].

Findings/Outcome: By incorporating human face into the graphical password, they obtained a significant improvement in terms of system security (both password entropy and shoulder-surfing attacks). This novel interactive and secure authentication scheme is for mobile applications [22].

Future Work: Their future work includes conducting the studies and experiments on the robustness of face hash and to examine the effectiveness of their methods [22].

Problem [8]: Overcoming threats such as key-loggers, weak password, and shoulder surfing, forcing the user to memorize different passwords or carrying around different tokens. Familiarization or a lengthy password setup process [23].

Methodology used: In this paper, they proposed a new authentication scheme based on graphical password and multifactor authentication. To that end, they employed the user's personal handheld device as the password decoder and the second factor of authentication. In their methods, a service provider challenges the user with an image password. To determine the appropriate click points and their order, the user needs some hint information transmitted only to her handheld device. Their approach can be effectively and securely used as user-friendly authentication mechanism for public and un-trusted terminals. They showed that their method can overcome threats such as key-loggers, weak password, and shoulder surfing. With the increasing popularity of handheld devices such as cell phones, their approach can be leveraged by many organizations without forcing the user to memorize different passwords or carrying around different tokens [23].

Findings/Outcome: Their proposed solution is unique in many ways:

1. It is the first graphical password solution that employs two-factor authentication.
2. They never assume the handheld device is trusted.
3. Their solution resists screen recording attacks.
4. Their method doesn't need a "familiarization" or a lengthy "password setup" process.
5. Lost or stolen handheld doesn't expose a security risk. They can apply their system to more than just authentication mechanisms: their system is applicable anywhere that there is a need to enter sensitive or private data. For instance, Social Security Number can be entered via their system without leaking or revealing any directly usable information to the terminal or even the handheld device [23].

5. Conclusion

In this study we surveyed 23 papers in three categories: Usability, Security and both security and usability. Totally eleven problems in security, four problems in Usability and eight problems in the category of combination of both have been recognised. With reference to our experience in this survey, we will propose a new recognition-based algorithm that can support usability and security side together. This survey will be useful for information security researchers and practitioners who are interested in finding an alternative to text-based authentication methods.

Acknowledgment

We would like to express our appreciation to our parents and all the lecturers who helped us to understand the importance of knowledge and showed us the best ways to earn it.

References

[1] THORPE, J. & VAN OORSCHOT, P. C., 2004, 'Towards secure design choices for implementing graphical passwords', Computer Security Applications Conference, 20th Annual.

[2] ZHI, L., QIBIN, S., YONG, L. & GIUSTO, D. D., 2005, 'An Association-Based Graphical Password Design Resistant to Shoulder-Surfing Attack', IEEE International Conference on Multimedia and Expo (ICME).

[3] YOKOTA, K. & YONEKURA, T., 2005, 'A proposal of COMPASS (community portrait authentication system)', International Conference on Cyber worlds.

[4] WEI-CHI, K. & MAW-JINN, T., 2005, 'A Remote User Authentication Scheme Using Strong Graphical Passwords', The IEEE Conference on Local Computer Networks, 30th Anniversary.

[5] ALSULAIMAN, F. A. & SADDIK, A. E., 2006, 'A Novel 3D Graphical Password Schema', Proceedings of 2006 IEEE International Conference on Virtual Environments, Human-Computer Interfaces and Measurement Systems.

[6] HUANYU, Z. & XIAOLIN, L., 2007, 'S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme', 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW).

[7] ALSULAIMAN, F. A. & EL SADDIK, A., 2008, 'Three-Dimensional Password for More Secure Authentication', IEEE Transactions on Instrumentation and Measurement, vol.57, pp.1929-1938.
[8] BICAKCI, K., 2008, 'Optimal discretization for high-entropy graphical passwords', 23rd International Symposium on Computer and Information Sciences (ISCIS).
[9] BANDYOPADHYAY, S. K., BHATTACHARYYA, D. & DAS, P., 2008, 'User authentication by Secured Graphical Password Implementation', 7th Asia-Pacific Symposium on Information and Telecommunication Technologies (APSITT).
[10] SALEHI-ABARI, A., THORPE, J. & VAN OORSCHOT, P. C., 2008, 'On Purely Automated Attacks and Click-Based Graphical Passwords', Annual Computer Security Applications Conference (ACSAC).
[11] ZHENG, Z., LIU, X., YIN, L. & LIU, Z., 2009, 'A Stroke-Based Textual Password Authentication Scheme', First International Workshop on Education Technology and Computer Science (ETCS).
[12] ELJETLAWI, A. M. & ITHNIN, N., 2008, 'Graphical Password: Prototype Usability Survey', International Conference on Advanced Computer Theory and Engineering (ICACTE).
[13] ELJETLAWI, A. M. & ITHNIN, N., 2008, 'Graphical Password: Comprehensive Study of the Usability Features of the Recognition Base Graphical Password Methods', Third International Conference on Convergence and Hybrid Information Technology (ICCIT).
[14] ABDULLAH, M. D. H., ABDULLAH, A. H. B., ITHNIN, N. & MAMMI, H. K., 2008, 'Graphical password: User's affinity of choice-an analysis of picture attributes selection', International Symposium on Information Technology (ITSim).
[15] OKA, M., KATO, K., YINGQING, X., LIN, L. & FANG, W., 2008, 'Scribble-a-Secret: Similarity-based password authentication using sketches', 19th International Conference on Pattern Recognition (ICPR).
[16] XIAOYUAN, S., YING, Z. & OWEN, G. S., 2005, 'Graphical passwords: a survey', 21st Annual Computer Security Applications Conference.
[17] BIRGET, J. C., DAWEI, H. & MEMON, N., 2006, 'Graphical passwords based on robust discretization', IEEE Transactions on Information Forensics and Security, vol.1, pp.395-399.
[18] YAMPOLSKIY, R. V., 2007, 'User Authentication via Behaviour Based Passwords', IEEE Long Island Systems, Applications and Technology Conference (LISAT).
[19] LIN, P.-L., WENG, L.-T. & HUANG, P.-W., 2008, 'Graphical Passwords Using Images with Random Tracks of Geometric Shapes', Congress on Image and Signal Processing (CISP).
[20] HAFIZ, M. D., ABDULLAH, A. H., ITHNIN, N. & 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 (AICMS).
[21] HAICHANG, G., XUEWU, G., XIAOPING, C., LIMING, W. & XIYANG, L., 2008, 'YAGP: Yet Another Graphical Password Strategy', Annual Computer Security Applications Conference (ACSAC).
[22] QIBIN, S., ZHI, L., XUDONG, J. & KOT, A., 2008, 'An interactive and secure user authentication scheme for mobile devices', IEEE International Symposium on Circuits and Systems (ISCAS).
[23] SABZEVAR, A. P. & STAVROU, A., 2008, 'Universal Multi-Factor Authentication Using Graphical Passwords', IEEE International Conference on Signal Image Technology and Internet Based Systems (SITIS).

Arash Habibi Lashakri obtained his bachelor degree in software engineering from Azad University of Lahijan, Gilan, Iran, followed by master degree of computer system & technology, faculty of computer science and information technology, University of Malaya (UM), Kuala Lumpur, Malaysia. He is a member of International Association of Computer Science and Information Technology (IACSIT), Microsoft System Engineers Association and Microsoft Database Administrators Association in Singapore. He is also a member of some funded research projects and he has published more than 15 papers in various international and national conferences and journals. He is interested to research in security, cryptography and especially graphical user authentication (GUA) areas. He works on wireless security and optical network bandwidth allocation systems as a research assistant.

Samaneh Farmand received her Bachelor degree in Applied Mathematics in Computer from Azad University in Iran-Isfahan in 2006. She is now doing her masters of Information technology in University of Malaya in Malaysia-Kuala Lumpur. Her research interest includes Graphical Passwords, Wireless and Mobile Security.