International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Secure Graphical Password Requirements

Avinash Balasaheb Anap[1], Abhishek Annasaheb Nibe[2], Vasimraj Siraj Tamboli[3]
[123]*Computer Department, P.Dr.V.V.P. Polytechnic, Loni*

Abstract*: Graphical or visual passwords have been introduced as possible alternatives to authentication using alphanumeric passwords. Human being can remember the graphical things better and for longer periods than alphanumeric passwords. Graphical passwords not yet are readily adopted for use due to the demerits associated with it. There has therefore been a move in literature to discussions on efficient implementation of visual password schemes. This paper analyses the current challenges in the design of graphical password as well as the factors affecting security and usability of these schemes. The paper presents requirements of a graphical password scheme providing a large enough password space, ease of use and secures password images.

Keywords*: Security, graphical passwords, authentication.

I. INTRODUCTION

Authentication process, with alphanumeric passwords being the most common of these password based authentication methods [9]. This method has, however, been shown to have significant drawbacks. For example, users cannot remember meaningless alphanumeric strings with ease and therefore resort to choosing predictable passwords [14], thus making these passwords prone to guessing and brute-force attacks. In an attempt to address these drawbacks, there has been an introduction of and growing interest in using visual passwords, sometimes also referred to as graphical passwords [17].

The move towards visual passwords is mainly supported by the so-called picture superiority effect, as explained in the work of Shepard [15]. According to this effect, people can remember pictures much better and for longer periods than words. Visual password schemes have therefore been proposed as a more user-friendly alternative to alphanumeric password schemes in the attempt to address the uneasy compromise between security and human memory constraints often encountered in authentication systems [9].

Even with the improvement in memorability, visual passwords are not the silver bullet for authentication systems. There are three major problems associated with current implementations of visual passwords that this work notes. Visual passwords are more vulnerable to shoulder-surfing than the conventional alphanumeric passwords as pictures are larger and easier to see from a distance [10]. Due to the picture superiority effect, they can also be remembered more easily than secure alphanumeric passwords. Another drawback is the reduced number of possible passwords, the so-called password space [4]. This is particularly a problem for the class of searchmetric visual password schemes. Searchmetric schemes generally require that a user memorize a number of images when creating their password and then recognize their images from among decoys to log in. All the possible password images and decoys are stored in a database and therefore the password space is dependent on the amount of memory space allocated for password images. Furthermore, drawmetric schemes, which require a user to reproduce a previously drawn image for authentication, have usability problems associated with the accuracy required from the user when reproducing his or her password [4]. More efficient implementations of visual passwords are therefore necessary to render them more useful. Work in the effort of implementing efficient visual password schemes has only been in guiding designers of visual password schemes on considerations to be taken with no study covering the exact rules of implementing an efficient visual password scheme [4], [21], [11]. This is the aim of this work.

Our work contributes towards a clear model for the implementation of visual password offering a secure authentication system in support of the trend towards visual passwords. This study analyses the factors that affect the security and usability of visual authentication schemes and therefore design decisions to be taken for high security and usability returns. We present password formation rules for easy to remember and secure password images.

II. OBJECTIVES

Currently, alphanumeric passwords are the default method of authentication; therefore models have been developed to guide users in safe practices when selecting secure alphanumeric passwords. This has not been the case with visual passwords. As a result, implementing secure and efficient visual password schemes is not straight forward. The move towards visual passwords requires that there be set definitions of secure graphical passwords to enhance the ease of use for users as well as limit the number of successful attacks on such schemes.

Work has been put into the considerations to be taken and guidelines to be followed when developing such a model. There has, however, been no comprehensive study on the requirements of a secure visual password image and the schemes deploying them. This is the objective of this work.

III. METHODOLOGY

We determine from the literature the factors affecting the security and usability of visual password schemes. We firstly examine the current and anticipated challenges when implementing visual password schemes. From these challenges, we define clear requirements for secure and efficient visual password schemes and try to alleviate the three problems associated with visual passwords. This paper therefore addresses implementation issues in the design of a visual password scheme that allows for a large password space, low susceptibility to shoulder-surfing and one that eliminates challenges for drawmetric schemes associated with redrawing passwords exactly as they were originally drawn.

This work is based on a wide range of existing academic literature, with particular attention paid to the work of Thorpe and Oorschot [20], which presents results that, can be used when choosing parameter guidelines for secure graphical passwords. This paper emerges from a Masters study currently under way, which aims at the implementation of an efficient visual password scheme using shape grammars [16].

IV. RELATED WORK

A. *Challenges in the development of visual password authentication schemes*

The main challenge when implementing visual password schemes is finding an efficient solution to what is defined as the "password problem" [23]. This problem, as formulated in Wiedenbeck et. al [22], arises because passwords are expected to comply with two conflicting requirements. Firstly, passwords must be easy to remember and the authentication process must be such that humans can execute it quickly and easily. The second requirement speaks to the security of the passwords. The passwords should look random and be hard to guess; it should not be necessary to write the passwords down or store them, since that would pose a security risk. The answer to these problems requires a scheme that offers a good trade-off between the usability and the security strength of the password scheme. This continues to be a challenge to the Human Computer Interaction and security communities [18].

Visual authentication success is dependent on the type of images that a password scheme uses as well as how the images are encoded and then retrieved when required [19]. According to Renaud and De Angeli [14], the suitability of an image for use in authentication can be associated with three prime aspects. The first relates to how clear the image is to the user, and the second to how memorable it is, i.e. how easy it is for the user to recall it. The last aspect relates to the complexity and therefore security level of the image. The encoding and retrieval of password images for verification also impacts the login process. One major complaint regarding graphical passwords is that the login process, in particular for recall-based schemes where users need to reproduce their password, is long and affects user experience negatively [17]. Text passwords can be typed in a few seconds on a standard keyboard and it is therefore important to consider efficiency in response time when adopting graphical passwords.

There have been implementations of visual password schemes with each of them having some disadvantages associated with them. The first few visual password schemes were introduced around 1999 [2]. Searchmetric schemes had issues in having to store the password images and decoys. Locimetric schemes, which require the user to remember points on an image just like drawmetric systems have problems with the precision in pointing at the points and drawing the password, respectively [2].

In summary, implementation problems are due to the difficulty in design of password images that are memorable and secure and providing a large enough password space.

B. *Context-imposed requirements for visual password schemes*

A substantial amount of work has been done on the analysis of current graphical password schemes as well as the challenges in the implementations of these schemes. The work of De Angeli et al [4], Tsai et al [20] and Liao et al. [11] amongst others, present guidelines to be used in setting requirements for visual password authentication schemes. These authors try to address the issues mentioned in Section 4.1. In summary of their work, and the literature reviewed, Table 1 presents the context-imposed requirements derived from the existing challenges.

Table 1: Summary of context-imposed requirements for graphical authentication schemes

Requirement	Description and Support for Requirement
Secure password image	Secure password schemes require secure password images [4]. The basic aspects of the security of a password image are the ability of an attacker to guess the image (guessability), to view the image (observability) and to record and reproduce the image (recordability) [11]. A password image should exhibit low levels of these three factors to be considered secure [11]
Large password space	Attackers find it substantially more difficult in to exhaustively search through the full password space when there are a large number of possible passwords [9].
Memorable password	For usability, the amount of effort required to remember a password should be minimal for the user [4]. This, however, should take into account that a password image that is easy to remember for the user, is unfortunately also easy to remember for an attacker. There should therefore be a way to minimize the ease of observability and recordability of the attacker.
Reduced susceptibility to shoulder surfing	Visual password schemes predominantly use images as passwords and because they are bigger than text and can be seen from a bigger distance, they are more susceptible to shoulder-surfing [14]. There must be a mechanism to either reduce the observability or to hide the process when a user selects their password or produces it by drawing it.
Ease of use and efficiency	Alphanumeric passwords are currently the most predominantly used method of authentication [21]. People are comfortable with using these and will move to graphical passwords only if such schemes allow for efficient use.

C. Specific design requirements

As presented in Table 1. We explain the properties of such a scheme and the specifications by justification from the analysis done on the DAS scheme by Thorpe and Oorschot [20]. In DAS passwords, a user creates their password on a two-dimensional grid. Each grid is referenced by two-dimensional co-ordinates where G is the numbers of rows and columns of the grid. As the user draws their password on the grid, the sequence of the coordinate pairs through which the drawing device passes is added to the DAS password encoding. We borrow the following terminology from the work of Thorpe and Oorschot [20]

From this we note that shapes can be constructed as a connection of neighbouring points with each shape separated from another by a pen-up event. Thus one can rightfully view a shape as a stroke as by the above definition with the length of each shape being the number of coordinate pairs connected to draw out the shape. Similarly, an image made up of shapes can be defined as one made up of strokes and the number of shapes making up the image is equivalent to the stroke count of an image.

D. Secure Password Image

The security of a password image is measured in terms of its resistance to dictionary attacks and capture attacks, the latter through shoulder-surfing or stealing of recorded passwords [19]. The resistance is determined by the size of the password space and the complexity of the password image used. A secure image is defined as one with low levels of guessability, observability and recordability [21]. These three factors depend on the pattern complexity of the image. Thorpe and Oorschot [19] explain how this complexity can be assessed by the password image length, the number of shapes making up the image and how symmetrical the image is [19]. A complex image is harder to guess or remember for a shoulder-surfer and is therefore more secure. One should, however, remember that a more complex image brings about memory strain for the user when having to recall the password image.

A psychological study conducted by Attneave [1] has shown that people recall on average a maximum of six to eight dots after having viewed them for approximately 1.5 seconds. We assume that a user inputting their password would take around the same amount of time and therefore that would be the amount of time an attacker would have to view the password. We therefore define an image to be secure if it is constructed from a connection of at least 8 dots.

E. Memorable Passwords and Reduced Susceptibility to Shoulder-surfing

A password should be easily memorable to the user; for the password scheme to adhere to the usability requirements [9]. The evaluation of visual password schemes by Renaud and De Angeli [14] found that users find password images that they generated more memorable than those that are system generated. User choice is therefore advised to increase memorability. However, given the choice, users select images that carry some meaning to them or object that they frequently see which are therefore easier to guess [14]. To do away with this, it is important to set rules describing the type of images allowed in the password space.

From the work of Thorpe and Oorschot [20], the password complexity is another property that affects the ease of recall of an image. Properties such as the password length, components making up the image and the surface on which the image is presented all play a role in how the user will imprint the image in memory and therefore how easy it would be to recall [18]. The study conducted by Thorpe and Oorschot [19] also shows that a class of memorable images are those with patterns of symmetry within the image. Thorpe and Oorschot show that when subjects were given random patterns and symmetric patterns of dots, the symmetric patterns were more accurately remembered, particularly when the axis of symmetry is about the horizontal and vertical axes. Another difficulty in the use of visual passwords was found to be that the user was expected to reproduce the password exactly as they had originally drawn it at registration of the password [17]. The dimension of the surface on which the password image is drawn or generated on also affects the memorability. The study presented by Thorpe and Oorschot [19] also found that an image on a larger grid is harder to remember than one on a grid with smaller dimensions. In fact, their study shows that a larger grid does not provide high enough security returns to compensate for the increased difficulty in recalling the password. This same study further shows that users find recognition easier to do than recall. In other words, people prefer identifying their password over having to reproduce it. They also have an easier time recalling objects that they can name, this referred to as the nameability property [11].

Since users prefer recognition over recall, the scheme has the user only draw out their password on registration. For authentication, the user does not have to recall a reproduce the image previously drawn, and but simply recognize it from a set of similar decoys as advised by Hafiz in [6].

V. DESCRIPTION AND ANALYSIS OF VISUAL PASSWORD SCHEME RULES

Each shape that can be used as a component to draw up the password can be defined as a stroke with an associated length, where the length is the number of points a user would have to remember to reproduce the shape. Figure 1 shows these shapes as well as their associated (x, y) points.

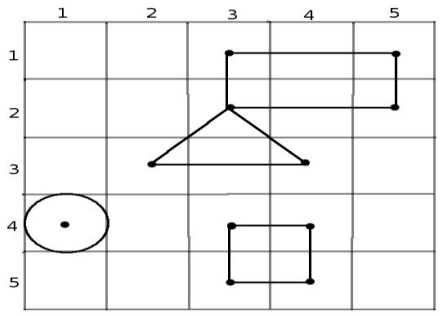

Figure 1: Symmetrical shapes used in construction of password image and associated (x,y) points.

The set minimum length of an allowed password is eight and from the shapes shown in Figure 1, this requires a minimum of three shapes in the image. We set the minimum number of shapes, equal to 3. For a large enough password space we adopt equal to 20, as specified by shorpe and Oorschot [20] with the maximum number of shapes, for these values of and Thorpe and Oorschot [20] calculates the password space to be. This consisting of all passwords of lengths less than or equal to=20 and number of shapes less than or equal to. This value includes even the restricted size, where there are fewer than 3 shapes in a password.

VI. SIGNIFICANCE AND EVENTUAL BENEFITS

Some people are symbolic thinkers, relating most of their thoughts to letters, numbers and other symbols, while other are visual thinkers, their thinking mainly based on shapes colours, graphics and spatial relationships [5]. While symbolic thinkers are more

likely to remember alphanumeric passwords, visual thinkers have difficulty remembering what are considered to be secure alphanumeric passwords. The picture superiority effect also shows that people are generally more likely to remember pictures than words. Furthermore, textual interfaces are unusable for low-literacy users [12]. There is thus a need for both symbolic and visual computations and therefore passwords.

The social benefit of this is in extending the reach of mobile applications requiring passwords for low-literate users who find difficulty in using textual interfaces. For example, mobile applications bringing health, financial and other services to users, require mechanisms to secure the applications as the use of textual passwords remains a problem for low-literate users [12].

This work tries to bridge the gap between advances in symbolic and visual authentication and to support the move towards more visual or icon based computation. It does this by presenting the requirements for an implementation of a secure password scheme and a model that meets the requirements.

VII. CONCLUSION AND RECOMMENDATIONS

Our study analyses the challenges in developing secure graphical password schemes as well as guidelines set in existing literature for secure graphical schemes and from that define a set of rules defining a model for a secure graphical password scheme. We note from literature that for secure and efficient visual password schemes, the allowed passwords should be easy to remember for ease of usability for the user but also be complex to offer resistance to guessing and shoulder-surfing attacks. From this we observe that the success of a visual password scheme is highly dependent on the type of images the password scheme uses. The current implementations of visual passwords have all been shown to be problematic after analysis through user trials. Searchmetric password schemes pose problems in having to allocate memory to store the passwords and their associated decoys while locimetric and drawmetric schemes pose problems for users trying to precisely reproduce their password as originally drawn. All visual password scheme are further shown to be more prone to shoulder-surfing attacks as they are bigger are thus more visible than textual passwords. We conclude that an efficient visual password scheme should therefore take into account properties stated in Table 1.

This work presents requirements to be met to do away with the noted disadvantages of the current visual passwords and address the challenges in implementing visual password schemes. Section 6 gives a description of the requirements such a scheme should meet as well as the rules the password images should adhere to. The work communicates the requirements of such a scheme but does not communicate the implementation of it. An implementation of such a scheme would require a tool that can allow for a rule based design. Such a system could be used for the formal definition of design steps in the creation of a password for a user. For this reason, we suggest implementation of graphical passwords, with shape grammars.

The similarity of the images generated during the authentication is of great importance, since it determines how efficiently the scheme protects the password against shouldersurfing. The images should be similar enough to confuse any attacker looking on, but be distinguishable for the user. Further work in this direction should therefore look at the design of sound measures of perceptual similarity of images used as decoys. These requirements, although sufficient in producing secure schemes, can be strengthened by investigating other mechanisms to reduce shoulder-surfing over and above the use of decoys. An example of this would be to enforce hard-to-see selection methods when the user chooses their password from the given set of selection of different passwords.

This study further notes that an important factor is the amount of time required when users try to authenticate themselves. More detailed studies are required to determine exactly what amount of time users would consider tolerable for the authentication process.

REFERENCES

[1] Attneave, F. (1957). “Physical determinants of the judged complexity of shapes” Journal of Experimental Psychology, 53 (4), 221-227.
[2] Biddle, R., Chiasson, S., & Van Oorschot, P. (2012) “Graphical passwords: Learning from the first twelve years” ACM Computing Surveys (CSUR), 44(4) (19), 1-41.
[3] Collins, A., Joseph, D., & Bielaczyc, K. (2004) “Design research: Theoretical and methodological issues” The Journal of the learning sciences, 13 (1) ,15-42.
[4] De Angeli, A., Coventrya, L., Johnsona, G., & Renaud, K. (2005) “Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems” International Journal of Human- Computer Studies, 63 (1) , 128-152.
[5] Gips, J. (1999) “Computer implementation of shape grammars” MIT Workshop on Shape Computation, MIT.
[6] Hafiz, M.D., Abdullah, A.H., Ithin, N and nammi, H.K., (2008) “Towards identifying Usability and Security Features of Graphical Passwords in Knowledge Based Authentication Technique” In Second Asia International Conference Modelling and Simulation, 396-403
[7] Hevner, A. (2007) “The three cycle view of design science research” Scandinavian journal of information systems, 19 (2), 87--92.
[8] Ichakawa, I. S. (1982) “Measurement of visual memory span by means of the recall of the Dot-inMatrix patterns” Behaviour Research Methods and Instrumentations, 14(3), 309-313
[9] Jermyn, I., Mayer, A., Monrose, F., Reiter, M., & Rubin, A. (1999) “The design and analysis of graphical passwords” In Proceedings of the 8th usenix Security

Symposium (pp. 1--14).
[10] Lashkari, A., Zakaria, D., Farmand, S., Bin, O., & Saleh, R. (2009) "Shoulder Surfing attack in graphical password authentication." International Journal of Computer Science and Information Security, 6 (2), 145-154.Leeds University of. (2008) Design synthesis and shape generation.
[11] Liao, I.-E., Lee, C.-C., & Hwang, M.-S. (2006) "A password authentication scheme over insecure networks" Journal of Computer and System Sciences, 72 (4) , 727-740.
[12] Medhi, I. patnaik, S.,Brunskill,E., Gautama, S.N., Thies,W. &Toyama, K. (2011) "Designing mobile interfaces for novice and low-literacy users" ACM Transactions on Computer-Human Interaction (TOCHI), 18(1), 2.
[13] Peffers, K., Tuunanen, T., Rothenberger, M.A., & Chatterjee, S. (2007) "A design science research methodology for information systems research" Journal of Management Information Systems, 24(3) pp. 45-77.
[14] Renaud, K., & De Angeli, A. (2009) "Visual passwords: cure-all or snake-oil?" Communications of the ACM, 52 (12), 135-140.
[15] Shepard, R. (1967) "Recognition memory for words, sentences, and pictures" Journal of Verbal Learning and Verbal Behaviour, 6 (1), 156-163.
[16] Stiny, G. (1980) "Introduction to shape and shape grammars" Environment and Planning: B, 7(3) 343-351[17] Suo, X., Zhu, Y., & Owen, G. (2005) Graphical passwords: a survey. In Computer Security Applications Conference, 21st annual (p. 10-pp). IEEE.
[17] Tari, F., Ozok, A., & Holden, S. (2006) "A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords" In Proceedings of the second symposium on Usable privacy and security ACM (pp. 56-66) ACM.
[18] Thorpe, J., & Oorschot, P. van. (2004a) "Graphical dictionaries and the memorable space of graphical Passwords" In Usenix security symposium.
[19] Thorpe, J., & Oorschot, P. van. (2004b) "Towards secure design choices for implementing graphical Passwords" In Computer Security Applications Conference (pp. 50-60) IEEE.
[20] Tsai, C., Lee, C., & Hwang, M. S. (2006) "Password Authentication Schemes: Current Status and Key Issues" IJ Network Security, 3 (2), 101-115.
[21] Wiedenbeck, S., Waters, J., Birget, J., Brodskiy, A., & Memon, N. (2005a) "Authentication using graphical passwords: effects of tolerance and image choice" In Proceedings of symposium on Usable privacy and security ACM.
[22] Wiedenbeck, S., Waters, J., Birget, J., Brodskiy, A., & Memon, N. (2005b) "Passpoints: Design and longitudinal evaluation of a graphical password system" International Journal of Human Computer Studies, 63(1), 102-127.