A REVIEW ONSCHEMES FOR USER AUTHENTICATION

Thamraj N. Ghorsad[(1)], R. S. Pippal[(2)], Badri Prasad Patel[(3)]
M.Tech[(1)], Head, Department of C.S.E[(2)],Asst. Prof. Department of CSE[(3)]
RadharamanEngg.College. Bhopal, India (M.P.)[(1,2,3)]
raj.ghorsad@gmail.com[(1)], patel.rec@gmail.com[(3)]

ABSTRACT-*Textual-based password evidence scheme tends to be more accessible to attacks such as shoulder surfing and hidden camera, eves dropping, dictionary attacks, socialengineering. To overcome the vulnerabilities of traditional methods, graphical password schemes have been developed as possible alternative solutions to text-based password schemes.Most of thegraphical schemes are accessible to shoulder surfing. To solve this problem, text can be combinedwith images to generate session passwords for evidence. Session passwords can be usedonly once and every time a new password is generated. In this paper, we introduce a new evidence techniques "authentic recall-based" andComplect recall-based techniques*.

Keywords-*graphical password; evidence; Pass doodle;Grid Selection; Pass-Go; VisKey SFR*

1. INTRODUCTION

Evidence is the first step of information security. Evidence refers to the process of confirming or rejecting an individual's claimed identity. Evidence schemes require users tomemorize the passwords and recall them during log-in time. The most common user evidence method is thetext-based password scheme that a user enters a login nameand a password. The vulnerabilities of this method havebeen well known. Users tend to pick short password orpasswords that are easy to remember, which makes thepasswords accessible for attackers to break. To resist brute forcesearch and dictionary attacks, users are required touse long and random passwords. Unfortunately, such passwordsare hard to remember. Furthermore, textual passwordis accessible to shoulder-surfing, hidden camera and spyware attacks.Graphical password schemes have been proposed as apossible alternative to text-based schemes, motivated partiallyby the fact that humans can remember pictures betterthan text . In addition, the possible password spaceof a graphical password scheme may exceed that of text basedschemes and thus presumably offer higher level ofsecurity. It is also difficult to devise automated attacksfor graphical passwords. As a result, graphical passwordschemes provide a way of making more human-friendlypasswords while increasing the level of security. Due tothese advantages, there is a growing interest in graphicalpassword. However, existing graphical passwords are farfrom perfect. Typically, system requirements and communicationcosts for graphical passwords are significantlyhigher than text-based passwords. In addition, few graphicalsystems support keyboard inputs. More importantly,most current graphical passwords are more accessible toshoulder-surfing attacks than textual passwords. In this paper, Using authentic recall-based techniques and Complect Recall Based Techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage.

2. GRAPHICAL PASSWORDS METHODS

In this section, some graphical password systems based onrecognition and recall-based are discussed. Graphical-basedpassword techniques have been proposed as a solution to theconventional password techniques because graphic pictures are more easily remembered than texts which most ofresearchers

ISSN: 2229-6913 (Print), ISSN: 2320-0332 (Online) -, Web Presence: http://www.ijoes.vidyapublications.com

have nominated them as “Picture superiorityeffect” [18].A literature on most of articles regarding graphicalpassword techniques from 1994 till Jan-2009 shows that thetechniques can be categorized into three groups:

1. Recognition-Based Technique

In this category, users will choose pictures, icons or symbolsfrom a collection of images. In authentication process, theusers need to recognize their registration choice among a setof candidates. The research shows that 90% of users canremember their password after one or two month [15].

2. Pure Recall-Based Technique

In this category, users need to reproduce their passwords
without being given any reminder, hints or gesture. Althoughthis category is easy and convenient but it seems that usershardly can remember their passwords similar to DAS (1999)and Qualitative DAS (2007).

3. Cued Recall-Based Technique

In this category, the technique proposed a framework of
reminder, hints and gesture that help the users to reproducetheir password or help users to make a reproduction moreaccurate similar to Blonder Algorithm (1996) and Passpoint(2005)

3. INTERRELATED WORK

Many graphical evidence schemes have been proposed.
Dhamija and Perrig[1] proposed a graphical evidence scheme where the user has to identify the pre-defined images to prove user’s authenticity. This system is accessible to shoulder-surfing. Jermyn, et al. [3] proposed a new technique called “Draw- a-Secret” (DAS), where the user is required to re-draw the pre-defined picture on a 2D grid. If the drawingtouches the same grids in the same sequence, then the user is authenticated. This evidencescheme is accessible to shoulder surfing.Blonder [5] designed a graphical password scheme where the user must click on theapproximate areas of pre-defined locations. Passlogix [6] extended this scheme by allowing theuser to click on various items in correct sequence to prove their authenticity.Wiedenback et al [8] describes a graphical password entry scheme using convex hull methodtowards Shoulder Surfing attacks. A user needs to recognize pass-objectsand click inside the convex hull formed by all the pass-objects.Passface [2] is a technique where the user sees a grid of nine faces and selects one facepreviously chosen by the user. Here, the user chooses four images ofhuman faces as their password and the users have to select their pass image from eight otherdecoy images. Since there are four user selected images it is done for four times.Haichang et al [7] proposed a new shoulder-surfing resistant scheme in which the user is required to draw a curve across their password images orderly rather thanclicking on them directly. This graphical scheme combines DAS and Story schemes to provideauthenticity to the user.To overcome the shoulder-surfing problem,and hidden camera, eves dropping, dictionary attacks, social engineering two techniques are proposed in this paper i.e.Authentic Recall Based Techniques, and Complect Recall Based Techniques.

4. AUTHENTIC RECALL BASED TECHNIQUES ALGORITHM

Users reproduce their passwords, without having the chance to use thereminder marks of system. Although easy and convenient, it appears that users do notquite remember their passwords. Following are some of the algorithms which werecreated based on this technique.

4.1.Passdoodle

This is a graphical password which is made up ofhandwritten designs or text that is normally drawn with astylus onto a touch sensitive screen. According Jermyn etal. (1999) cracking the doodles is harder because theyhave a theoretically much larger number of possibledoodle passwords than text passwords. A sample of aPassdoodle password is shown in Figure1.

Figure 1.An example of a Passdoodle

Usability wise the Passdoodle is not widely usedbecause it has problems with recognition. What's morethe limits of the system are predefined by the length andidentifiable features of the doodle. In addition to this onlya predetermined amount of computer differentiabledoodles can be created and the doodle is the only meansof identification. In terms of security maintenance, thesystem cannot merely authenticate a user who records avery similar doodle, a minimum threshold of likelinessand similarity must be attained. This enhances securityby preventing evidence of users who use random and obvious guessing.

On the other hand speed and accuracy are still toppriorities for the system. Thus a complex recognitiondesign that needs hundreds of training samples andapproximately one minute of computation to authenticatedoes not justify the purpose of the original pervasivedesign. After careful consideration the proposed systemapplies a combination of doodle velocity and distributionmapping to recognize and authenticate a doodle(Christopher, 2004).

Soundness: According to (Christopher, 2004), people could recall doodle imagesas accurately as they would at alphanumeric passwords. However, such people wouldnot be able to recall the order in which they drew a doodle than the resulting image.On the other hand, users were found to be interest by the doodles drawn by otherusers, and often entered other users' login details simply to discover a variance of theset of doodles from their own (Karen, 2008).

4.2.GridSelection

In 2004, a research was conducted on the complexity of the DAS techniquebased on password length and stroke count by Thorpe and Orschot. Their studyshowed that the item which has the greatest effect on the DAS password space is thenumber of strokes. This means that for a fixed password length, if a few

strokes areselected then the password space will significantly decrease. To enhance security,Thorpe and Orschot created a “Grid Selection” technique. As shown in Figure 2,the selection grid has a large rectangular region to zoom in on, from the grid which the user selects their key for their password. This definitely increases the DASpassword space (Muhammad Daniel *et al.* 2008).

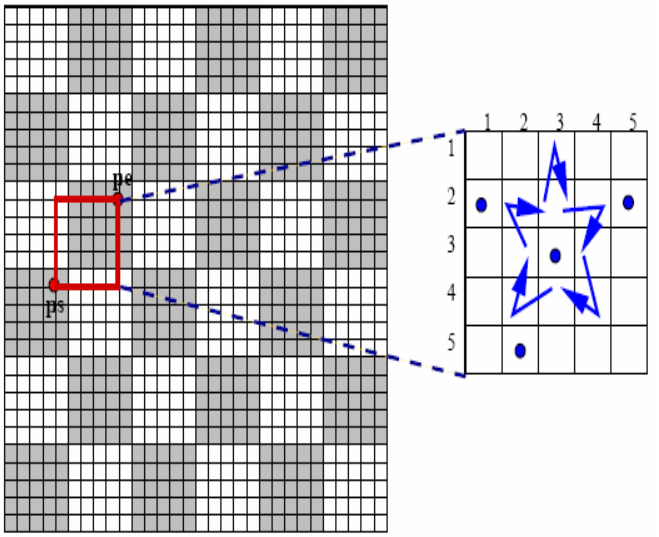

Figure 2. Grid selection

Soundness:Whilst this method significantly increases the DAS password space,the deficiencies in DAS have not been resolved (Muhammad Daniel *et al.* 2008).

4.3.Syukri

The Syukri algorithm proposes a system where evidence is achieved by the user using a mouse todraw their signature as can be seen in Figure 3 (Di et al.,2007).2. This technique is made up of two stages, namely,registration and verification. To start with, during the registration stage the user is requested to draw theirsignature with a mouse, this is then followed by thesystem extracting the signature area and either enlargingor scaling-down signatures, and rotating if required, (alsoknown as normalizing). Subsequent to this, theinformation is stored into the database. The verificationstage begins by obtaining the user input, on which itrepeats the normalization; thereafter it extracts theparameters of the signature. Basically the system usesgeometric average means and a dynamic update of thedatabase for verification purposes. Based on the study(Ali, 2008) undertaken, the rate of successful verificationwas satisfying. The major benefit to this approach is that not only is there no requirement for memorization ofone’s signature but counterfeit signatures is difficult tocome up with.Lack(s): However, since a good number of people areunfamiliar with using the mouse as a writing device; thesignature can therefore prove to be difficult to draw. Toresolve this drawback a pen-like input device could beemployed. Since such devices are not extensively used,adding them as new hardware to the current systemcould turn out to be expensive (Ali,

2008). Althoughresearchers from this study, believe that such atechnique can still be more useful on small devices.

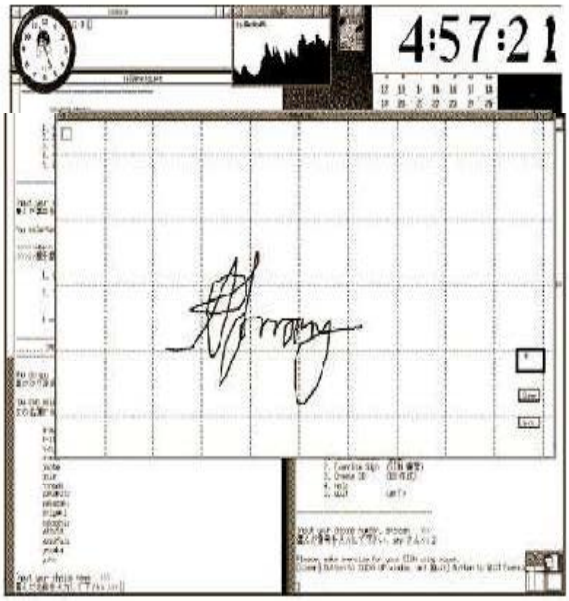

Figure 3. A Sample of Syukri Algorithm

Soundness: However, not everybody is familiar with using mouse as a writing device; the signature can therefore be hard to drawn. One possible solution to this problem would be to use a pen-like input device, but such devices are not widely used, and adding new hardware to the current system can be expensive. In this study, researchers believed such technique is more useful to small devices.

Table 1: The possible attacks in Authentic Recall-Based Techniques

ROW	Authentic Recall-Based Technique	PureRecall Based	CuedRecall Based	Bruteforce	Dictionary	Guessing	Spyware	Shoulder-surfing
1	Passdoodle	•				N		
2	Grid-selection	•				N	N	
3	Syukri	•				N		

5. COMPLECT RECALL BASED TECHNIQUES

Here, the system provides a framework of reminders, hints and gestures forthe users to reproduce their passwords or make a reproduction that would be muchmore accurate. Following are some of the algorithms which were created based onthis technique.

5.1.Passmap

A major drawback to using passwords is that very goodpasswords are difficult to commit to memory and theones that are easy to remember are too short andsimpleto be secure. All in all studies on human memoryindicate that it is quite straightforward to rememberlandmarks on a well-known journey. As such one can optto use a map as an alternative. For instance using themap of Europe a user who has never been to Europebefore should have no difficulty in remembering that hewould like to one day see the Eiffel Tour in Paris, the BigBen in London and the Kremlin in Moscow and his PassMap might be to visit all of them one at a time flying in from his hometown (Roman, 2007).Lack(s): It is obvious that the PassMaptechnology is not very susceptible to "shoulder surfing"attacks. This is due to the fact that the ability to notice asingle new edge or the absence of some edge in a largegraph requires a high level of concentration. HoweverBrute Force attacks are very likely and one has toconsider how good those mechanisms are in terms ofhow easy to remember the PassMap password is(Roman, 2007).

Soundness: This algorithm like the others suffers from some weaknesses. Firstly, when the password is selected by the mouse, it is simple for the attacker to observe the password. The other drawback of this algorithm is the long login time and long process through registration phase which causes this algorithm to be slower than textual password evidence (Furkan*et al*. 2006).

5.2. Pass-Go

In 2006, this scheme being created as an improvement of the DAS algorithm,keeping the advantages of the DAS whilst adding some extra security features. Pass-Go is a grid-based scheme which requires a user to select intersections, instead ofcells, thus the new system refers to a matrix of intersections, rather than cells as in DAS (Figure 4).

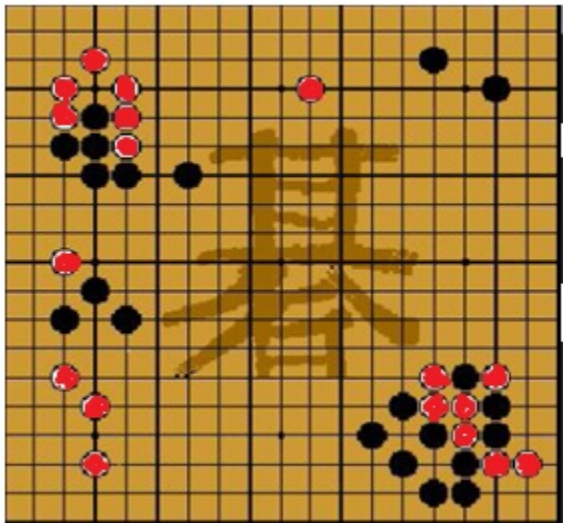

Figure4. Pass-Go Algorithm

5.3.VisKey SFR

A company called SFR from Germany recentlycommercialized the VisKeyscheme which is a recallbasedevidence scheme. The creation of apassword in this scheme requires the user to tap theirspots in sequence (Figure 5) (Muhammad et al., 2008).The VisKey scheme was original purposed for mobiledevices such as PDAs.Lack(s): This scheme's main drawback is the inputtolerance. Pointing to the exact spots on the picture hasproven to be quite hard thusViskey accepts all inputwithin a certain tolerance area around it. It also allowsusers to set the size of this area in advance. However,some caution related to the input precision needs to be taken, since it will directly influence the security and theusability of the password. In order to practically setparameters, a four spot VisKey theoretically providesapproximately 1 billion possibilities for defining apassword. Unfortunately this is not large enough toprevent off-line attacks from a high-speed computer.Therefore no less than seven defined spots are required to overcome the likelihood of brute force attacks(Muhammad et al., 2008).

Figure 5.A Sample of VisKey SFR Algorithm

Soundness*:* The problem with this technique is the input tolerance. Since it is difficult to point to the exact spots on the picture, Viskey permits all input within a certain tolerance area around it. The size of this area can be pre-defined by users. Nonetheless, some precautions related to the input precision needs to be set carefully, as it will directly influence the security and the usability of the password. For a practical setting of parameters, a four spot VisKey can offer theoretically almost 1 billion possibilities to define a password. However, is not large enough to avoid the off-line attacks by a high-speed computer. At least seven defined spots are needed in order to overcome the brute force attacks.

Table 1: The possible attacks in Complect Recall-Based Techniques

ROW	Authentic Recall-Based Technique	Pure Recall	Cued Recall	Brute force	Dictionary	Guessing	Spyware	Shoulder-surfing
1	Passmap		•			Y		Y
2	Viskey SFR		•	Y	N	Y	N	Y
3	Pass -Go		•	Y	N	Y	N	Y

6. COMMON ATTACKS ON GRAPHICAL PASSWORDS

Following aresome of the attacks on Graphical Password.

6.1 Password brute forcing attack

In this attack, which has the attack pattern ID 112, the attacker tries every possible value for a password until they succeed (Common Attack, 2009). A brute force attack, if feasible computationally, will always be successful because it will essentially go through all possible passwords given the alphabet used and the maximum length of the password. A system will be accessible to this type of an attack if it does not have a proper mechanism to ensure that passwords are strong and comply with an adequate password policy. Inpractice, aauthentic brute force attack on passwords is rarely used, unless the password is suspected to be weak. The speed with which an attacker discovers a secret is directly related to the resources that the attacker has. This attack method is resource expensive as the attackers' chance for finding user's password is high only if the resources be as complete as possible.

6.2. Dictionary based password attack

In this attack which has the attack pattern ID 16, an attacker tries each of the words in a dictionary as passwords to gain access to the system via some user's account. If the password chosen by the user was a word within the dictionary, this attack will be successful. This is a specific instance of the password brute forcing attack pattern.

6.3. Spyware attack

Except for a few exceptions, key logging or key listening spyware can not be used to break graphical passwords. It is not clear whether "mouse tracking" spyware will be an effective tool against graphical passwords. However, mouse motion alone is not enough to break graphical passwords. Such information has to be correlated with application information, such as window position and size, as well as timing information.

6.4. Shoulder surfing attack

Like text based passwords, most of the graphicalpasswords are accessible to shoulder surfing. At thispoint, only a few recognition-based techniques aredesigned to resist shoulder-surfing. None ofthe recall-based based techniques are consideredshould-surfing resistant.

6.5. Social engineering attack

In this kind of attack an attacker uses human interaction to obtain or compromise information about an organization or computer systems, while claiming to be one of employees in order to gain identity. On the other hand, the attacker tries to ask many questions in order to infiltrate an organization's security. If an attacker is not able to gather enough information from one source, he or she may contact another source within the same organization and rely on the information from the first source to add to his or her credibility.

7. CONCLUSION

The past decade has seen a growing interest in using graphical passwords as an alternative to the traditional text-based passwords. In this paper, Authentic Recall-Based and Complete Recall-Basedgraphical password evidence algorithms werereviewed. From all these algorithms we were able to come up with a number of shortcomings that can allow attacks to be perpetuated. The current graphical password techniques can be classified into two categories: recognition-based and recall-based techniques.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. Our preliminary analysis suggests 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.

8. ACKNOWLEDGMENTS

We would like to express our appreciation to our parents and all the teachers and lecturers who helped us to understand the importance of knowledge and show us the best way to gain it.

REFERENCES

[1] R. Dhamija, and A. Perrig. “Déjà Vu: A User Study Using Images for Evidence”. In 9thUSENIX Security Symposium, 2000.
[2] Real User Corporation: Passfaces.www.passfaces.com
[3] Jermyn, I., Mayer A., Monrose, F., Reiter, M., and Rubin., “The design and analysis of graphicalpasswords” in Proceedings of USENIX Security Symposium, August 1999.
[4]ArashHabibiLashkari may, 2010 “a new algorithm for graphical user evidence based on rotation and resizing”,
[5] G. E. Blonder, "Graphical Passwords," In *Lucent Technologies, Inc., Murray Hill, Nj*, U. S. Patent,Ed. United States, 1996.
[6] Passlogix, site http://www.passlogix.com.
[7] HaichangGao, ZhongjieRen, Xiuling Chang, Xiyang Liu UweAickelin, “A New Graphical Password SchemeResistant to Shoulder-Surfing.
[8] S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, N. Memon, “Design and longitudinal evaluationof a graphical password system”. International J. of Human-Computer Studies 63 (2005) 102127.
[9]ArashHabibi Lashkari1*, Abdullah Gani1, Leila Ghasemi Sabet2 and Samaneh Farmand1 “A new algorithm on Graphical User Evidence (GUA) based on multi-line grids”.
[10]M Sreelatha1, M Shashi2, M Anirudh1, MD Sultan Ahamer1, V Manoj Kumar, “Evidence Schemes for Session Passwords using Color and Images”.
[11]XiaoyuanSuo Ying Zhu G. Scott. Owen, “Graphical Passwords: A Survey”
[12] D. Hong, S. Man, B. Hawes, and M. Mathews, "Apassword scheme strongly resistant to spyware," in*Proceedings of International conference on securityand management*. Las Vergas, NV, 2004.
[13] S. Man, D. Hong, and M. Mathews, "A shouldersurfing resistant graphical password scheme," in*Proceedings of International conference on securityand management*. Las Vegas, NV, 2003.
[14] GajbhiyeS.K.1* and UlheP.2, “Evidence Schemes For Session Passwords Using Color And Gray-Scale Images”