

A REVIEW ON SCHEMES FOR USER AUTHENTICATION

Thamraj N. Ghorsad

M.Tech., Department of CSE
Radharaman Engg College, Bhopal, India (M.P.)
raj.ghorsad@gmail.com

Ravi Singh Pippal

Head, Department of C.S.E.
Radharaman Engg. College, Bhopal, India (M.P.)
ravesingh@gmail.com

ABSTRACT

Textual-based password evidence scheme tends to be more accessible to attacks such as shoulder surfing and hidden camera, eves dropping, dictionary attacks, social engineering. To overcome the vulnerabilities of traditional methods, graphical password schemes have been developed as possible alternative solutions to text-based password schemes. Most of the graphical schemes are accessible to shoulder surfing. To solve this problem, text can be combined with images to generate session passwords for evidence. Session passwords can be used only once and every time a new password is generated. In this paper, we introduce a new evidence techniques “authentic recall-based” and Complect 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 to memorize the passwords and recall them during log-in time. The most common user evidence method is the text-based password scheme that a user enters a login name and a password. The vulnerabilities of this method have been well known. Users tend to pick short password or passwords that are easy to remember, which makes the passwords accessible for attackers to break. To resist brute force search and dictionary attacks, users are required to use long and random passwords. Unfortunately, such passwords are hard to remember. Furthermore, textual password is accessible to shoulder-surfing, hidden camera and spyware attacks. Graphical password schemes have been proposed as a possible alternative to text-based schemes, motivated partially by the fact that humans can remember pictures better than text. In addition, the possible password space of a graphical password scheme may exceed that of text based schemes and thus presumably offer higher level of security. It is also difficult to devise automated attacks for graphical passwords. As a result, graphical password schemes provide a way of making more human-friendly passwords while increasing the level of security. Due to these advantages, there is a growing interest in graphical password. However, existing graphical passwords are far from perfect. Typically, system requirements and communication costs for graphical passwords are significantly higher than text-based passwords. In addition, few graphical systems support

keyboard inputs. More importantly, most current graphical passwords are more accessible to shoulder-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 on recognition and recall-based are discussed. Graphical-based password techniques have been proposed as a solution to the conventional password techniques because graphic pictures are more easily remembered than texts which most of researchers have nominated them as “Picture superiority effect”. A literature on most of articles regarding graphical password techniques from 1994 till Jan-2009 shows that the techniques can be categorized into three groups:

a. Recognition-Based Technique

In this category, users will choose pictures, icons or symbols from a collection of images. In authentication process, the users need to recognize their registration choice among a set of candidates. The research shows that 90% of users can remember their password after one or two month.

b. Pure Recall-Based Technique

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

c. Cued Recall-Based Technique

In this category, the technique proposed a framework of reminder, hints and gesture that help the users to reproduce their password or help users to make a reproduction more accurate similar to Blonder Algorithm (1996) and Passport (2005).

3. INTERRELATED WORK

Many graphical evidence schemes have been proposed. Dhamija and Perrig 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. 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 drawing touches the same grids in the same sequence, then the user is authenticated. This evidence scheme is accessible to shoulder surfing. Blonde designed a graphical password scheme where the user must click on the approximate areas of pre-defined locations. Passlogix] extended this scheme by allowing the user to click on various items in correct sequence to prove their authenticity. Wiedenback et al describes a graphical password entry scheme using convex hull method towards Shoulder Surfing attacks. A user needs to recognize pass-objects and click inside the convex hull formed by all the pass-objects. Passface is a technique where the user sees a grid of nine faces and selects one face previously chosen by the user. Here, the user chooses four images of human faces as their password and the users have to select their pass image from eight other decoy images. Since there are four user selected images it is done for four times. Haichang et al proposed a new shoulder-surfing resistant scheme in which the user is required to draw a curve across their password images orderly rather than clicking on them directly. This graphical scheme combines DAS and Story schemes to provide authenticity 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 the reminder marks of system. Although easy and convenient, it appears that users do not quite remember their passwords. Following are some of the algorithms which were created based on this technique.

4.1. Passdoodle

This is a graphical password which is made up of handwritten designs or text that is normally drawn with a stylus onto a touch sensitive screen. According Jermyn et al. (1999) cracking the doodles is harder because they have a theoretically much larger number of possible doodle passwords than text passwords. A sample of a Passdoodle password is shown in Figure1.

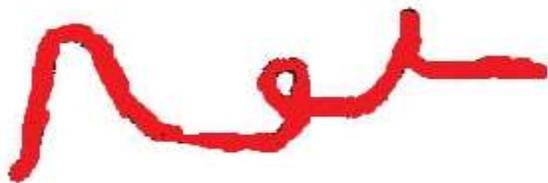


Figure 1. An example of a Passdoodle

Usability wise the Passdoodle is not widely used because it has problems with recognition. What’s more the limits of the system are predefined by the length and identifiable features of the doodle. In addition to this only a predetermined amount of computer differentiable doodles can be created and the doodle is the only means of identification. In terms of security maintenance, the system cannot merely authenticate a user who records a very similar doodle, a minimum threshold of likeliness and similarity must be attained. This enhances security by preventing evidence of users who use random and obvious guessing.

On the other hand speed and accuracy are still top priorities for the system. Thus a complex recognition design that needs hundreds of training samples and approximately one minute of computation to authenticate does not justify the purpose of the original pervasive design. After careful consideration the proposed system applies a combination of doodle velocity and distribution mapping to recognize and authenticate a doodle (Christopher, 2004).

Soundness: According to (Christopher, 2004), people could recall doodle images as accurately as they would at alphanumeric passwords. However, such people would not 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 other users, and often entered other users’ login details simply to discover a variance of the set of doodles from their own (Karen, 2008).

4.2. Grid Selection

In 2004, a research was conducted on the complexity of the DAS technique based on password length and stroke count by Thorpe and Orschot. Their study showed that the item which has the greatest effect on the DAS password space is the number of strokes. This means that for a fixed password length, if a few strokes are selected 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 DAS password space (Muhammad Daniel *et al.* 2008).

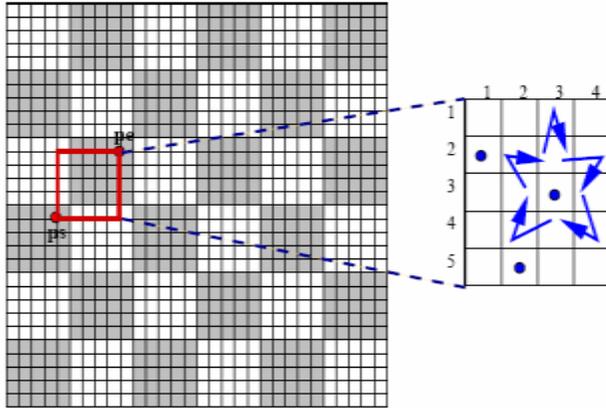


Figure 2. Grid selection

Soundness: Whilst this method significantly increases the DAS password spaces, 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 to draw their signature as can be seen in Figure 3 (Di *et al.*, 2007). 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 their signature with a mouse, this is then followed by the system extracting the signature area and either enlarging or scaling-down signatures, and rotating if required, (also known as normalizing). Subsequent to this, the information is stored into the database. The verification stage begins by obtaining the user input, on which it repeats the normalization; thereafter it extracts the parameters of the signature. Basically the system uses geometric average means and a dynamic update of the database for verification purposes. Based on the study (Ali, 2008) undertaken, the rate of successful verification was satisfying. The major benefit to this approach is that not only is there no requirement for memorization of one's signature but counterfeit signatures is difficult to come up with. Lack(s): However, since a good number of people are unfamiliar with using the mouse as a writing device; the signature can therefore prove to be difficult to draw. To resolve this drawback a pen-like input device could be employed. Since such devices are not extensively used, adding them as new hardware to the current system could turn out to be expensive (Ali, 2008). Although researchers from this study, believe that such a technique can still be more useful on small devices.

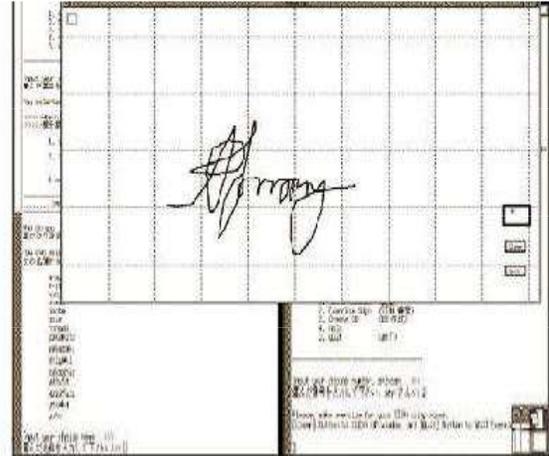


Figure 3. A Sample of Syukri Algorithm

Soundness: However, not everybody is familiar with using mouse as a writing device; the signature can therefore be hard to draw. 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

| R O W | Authentic Recall-Based Technique | Pure Recall Based | Cued Recall Based | Brute force | 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 for the users to reproduce their passwords or make a reproduction that would be much more accurate. Following are some of the algorithms which were created based on this technique.

5.1.Passmap

A major drawback to using passwords is that very good passwords are difficult to commit to memory and the ones that are easy to remember are too short and simple to be secure. All in all studies on human memory indicate that it is quite straightforward to remember landmarks on a well-known journey. As such one can opt to use a map as an

alternative. For instance using the map of Europe a user who has never been to Europe before should have no difficulty in remembering that he would like to one day see the Eiffel Tour in Paris, the Big Ben 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 Passmap technology is not very susceptible to "shoulder surfing" attacks. This is due to the fact that the ability to notice a single new edge or the absence of some edge in a large graph requires a high level of concentration. However Brute Force attacks are very likely and one has to consider how good those mechanisms are in terms of how 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 of cells, thus the new system refers to a matrix of intersections, rather than cells as in DAS (Figure 4).

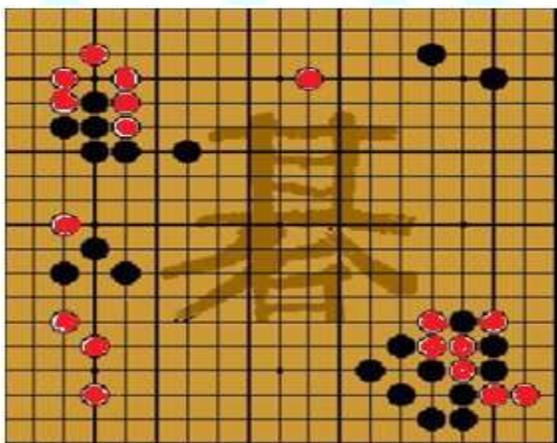


Figure 4. Pass-Go Algorithm

5.3.VisKey SFR

A company called SFR from Germany recently commercialized the VisKey scheme which is a recallbased evidence scheme. The creation of a password in this scheme requires the user to tap their spots in sequence (Figure 5) (Muhammad *et al.*, 2008). The VisKey scheme was original purposed for mobile devices such as PDAs. Lack(s): This scheme’s main drawback is the input tolerance. Pointing to the exact spots on the picture has proven to be quite hard thus Viskey accepts all input within

a certain tolerance area around it. It also allows users 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 the usability of the password. In order to practically set parameters, a four spot VisKey theoretically provides approximately 1 billion possibilities for defining a password. Unfortunately this is not large enough to prevent 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 2: The possible attacks in Complect Recall-Based Techniques

| R O W | 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 are some 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. In practice, a authentic 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 cannot 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 graphical passwords are accessible to shoulder surfing. At this point, only a few recognition-based techniques are designed to resist shoulder-surfing. None of the recall-based based techniques are considered should-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 Complect Recall-Based graphical password evidence algorithms were reviewed. 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. REFERENCES

- [1] R. Dhamija, and A. Perrig. "Déjà Vu: A User Study Using Images for Evidence". In 9th USENIX 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 graphical passwords" in Proceedings of USENIX Security Symposium, August 1999.
- [4] Arash Habibi Lashkari 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] Haichang Gao, Zhongjie Ren, Xiuling Chang, Xiyang Liu Uwe Aickelin, "A New Graphical Password Scheme Resistant to Shoulder-Surfing.
- [8] S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, N. Memon, "Design and longitudinal evaluation of a graphical password system". International J. of Human-Computer Studies 63 (2005) 102127.
- [9] Arash Habibi Lashkari*, Abdullah Gani1, Leila Ghasemi Sabet2 and Samaneh Farmand1 "A new algorithm on Graphical User Evidence (GUA) based on multi-line grids".
- [10] M Sreelatha 1, M Shashi 2, M Anirudh 1, MD Sultan Ahamer 1, V Manoj Kumar, "Evidence Schemes for Session Passwords using Color and Images".
- [11] Xiaoyuan Suo Ying Zhu G. Scott. Owen, "Graphical Passwords: A Survey".

- [12] D. Hong, S. Man, B. Hawes, and M. Mathews, "A password scheme strongly resistant to spyware," in Proceedings of International conference on security and management. Las Vegas, NV, 2004.
- [13] S. Man, D. Hong & M. Mathews, "A shoulder surfing resistant graphical password scheme," in Proceedings of International conference on security and management. Las Vegas, NV, 2003.
- [14] Gajbhiye S.K.1* and Ulhe P.2, "Evidence Schemes For Session Passwords Using Color And Gray-Scale Images".
- [15] Farnaz Towhidi, Maslin Masrom" A Survey on Recognition-Based Graphical User Authentication Algorithms" (IJCSIS) International Journal of Computer Science and Information Security, Vol. 6, No. 2, 2009.
- [16] Zhi Li, Qibin Sun, Yong Lian, and D. D. Giusto "An association-based graphical password design resistant to shoulder-surfing attack" IEEE.
- [17] D.E. Popescu, A.M. Lonea "An Hybrid Text-Image Based Authentication for Cloud Services" April, 2013.
- [18] K.Nivetha, M. Muthumeena, R. Srinivasan "Authentication Mechanisim For Session Passwords By Imposing Color With Text" Vol. 2, Issue 5, September-October 2012.
- [19] Vaishnavi Panchal, Chandan P. Patil," Authentication schemes for session password" International Journal of Scientific & Engineering Research Volume 4, Issue3, March-2013.
- [20] Cormac Herley, Paul C. van Oorschot "A Research Agenda Acknowledging the Persistence of Passwords" 2012.
- [21] Susan Wiedenbeck Jim Waters, "Authentication Using Graphical Passwords:"
- [22] Mr.Jaywant N. Khedkar, Ms.Pragati P. Katalkar, Ms.Shalini V. Pathak, Mrs.Rohini V.Agawane4 Integration of Sound Signature in 3D Password Authentication System International Journal of Innovative Research in Computer and Communication Engineering Vol. 1, Issue 2, April 2013.
- [23] Mihir Bellare Ran Canetty Hugo Krawczyk "Keying Hash Functions for Message Authentication"
- [24] T.Pavan Kumar, Nagesh Vadaparthi, A.Manvi, A.Alekhya Basic Results " Secure Session based Authentication Schemes" Vol. 3, Issue 2, March -April 2013.
- [25] H. Zhao and X. Li, "S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme," in 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW 07), vol. 2. Canada, 2007, pp. 467-472.