User Authentication by Secured Graphical Password Implementation

Ankesh Khandelwal[1]
Department of Information Technology and Engineering

Shashank Singh[1]
Department of Computer Science and Engineering

Niraj Satnalika[1]
Department of Electronics and Instrumentation Engineering

1- Heritage Institute of Technology
Anandapur
Kolkata-700107

ABSTRACT:

For the vast majority of computer systems, passwords are the method of choice for authenticating users. The most widely and commonly used authentication is traditional "Username" and "Password". For such authentication generally text (alphanumeric) is used. It is well-known, however, that passwords are susceptible to attack: users tend to choose passwords that are easy to remember, and often this means that they are also easy for an attacker to obtain by searching for candidate passwords. On the other hand, if a password is hard, then it is often hard to remember. Keeping these things in mind we propose a novel, innovative and more secure way of selecting passwords: Graphical Passwords.

In this paper we explore an approach to user authentication that generalizes the notion of a textual password and that, in many cases, improves the security of user authentication over that provided by textual passwords. We design and analyze *graphical passwords*, which can be input by the user to any device with a graphical input interface.

We also try to answer two most important questions:

- "Are graphical passwords as secure and easy to use as text-based passwords"?
- "Major design and implementation issues for graphical passwords"?

INTRODUCTION:

Patrick, et al. [1] pointed out that there are three major areas where human computer interaction is important: *authentication, security operations and developing secure systems.*

A graphical password is a secret that a user inputs to a computer with the aid of the computers' graphical input (e.g., mouse, stylus, or touch screen) and output devices. Graphical Password can be formed in the combination of Image Icons or Pictures. In other words, graphical password is an authentication system that works by having the user select from images, in a specific order, presented in a graphical user interface (GUI). For this reason, the graphical-password approach is sometimes called graphical user authentication (GUA).

Computer and Information security is very much dependent on password for the authentication of the users and are common in practice. The password design methods include text method, Biometrics. Biometrics scheme cannot be used widely. Text method is most widely used, since it is easy to implement and use.

Three basic features of PASSWORD:
1. Passwords should be easy to remember.
2. User authentication protocol should be executed quickly and easily.
3. Passwords should be secure (random, hard to guess and not in plain text).

One of the main pitfalls in text-based password is the difficulty of remembering it. Studies have shown that users tend to pick short and easy passwords that can be used by them easily [2]. But, these passwords can also be easily guessed or broken. Text based password scheme is lacking the above essential points mostly. Graphical based passwords might be a solution to the problems. Greg Blonder pioneered the idea of graphical passwords in 1996. His idea is to let the user click (with a mouse or stylus) on a few chosen (predesigned) regions in (pre-processed) an image that appears on the screen.

Generally the text based passwords follow the following guidelines:

1. At least 8 characters long and alphanumeric.
2. Should not be easy to relate to the user (e.g. last name, phonenwnber, birth year).
3. Should not be a word that can be found in a dictionary or public dictionary.
4. Should combine upper and lower case letters and digits.

Because of the above mentioned guidelines the text based password scheme has many problems and difficulties which the user will have to face. The following are some of the difficulties faced by the user using text based password scheme:

1. User may forget the password if it is too long or complicated or the password remain unused for a long time.
2. Watching a user log on as they type their password.
3. Dictionary attacks.

Considering the above problems faced by the user using text based password scheme it has been found that graphical password scheme is a better alternative to this. It has the following advantages:

1. Pictures are generally easier to be remembered than text.
2. If the number of pictures is sufficiently large, the possible password space of a graphical password scheme may exceed that of text based schemes and hence may prove to offer better resistance to dictionary attacks.

3. Examples include places we visited, faces of people and things we have seen which are easy to reframe.
4. Difficult to implement automated attacks (such as dictionary attacks) against graphical passwords.

GRAPHICAL AUTHENTICATION TECHNIQUE

Three main authentication techniques are:

- Token based authentication
- Biometric based authentication
- Knowledge based authentication

Knowledge based technique include both text based and picture based technique.
The picture based techniques can further be divided into two categories of graphical techniques:

- Recognition based
- Recall based

Recognition based technique: Dhamija and Perrig [3] proposed a graphical authentication scheme based on the Hash Visualization Technique [4]. In the system developed by them the user is asked to select a certain number of images from a set of random pictures which are generated by some program. Later, the user will be required to identify the pre-selected images in order to be authenticated. The results showed that 90% of all participants succeeded in the authentication using this technique, while only 70% succeeded using text based passwords. A weakness is that the server needs to store the seeds of the portfolio images of each user in plain text. Also, it can be tedious and time consuming.

Figure 1: Random Images used by Dhamija and Perrig

Akula and Devisetty's algorithm [5] is similar to the technique proposed by *Dhamija and Perrig*. The difference is that by using hash function SHA-1, which produces a 20 byte output, the authentication is secure and require less memory. This could be deployed on the Internet, cell phones and PDA's.
Weinshall and Kirkpatrick [6] sketched several authentication schemes, such as picture recognition, object recognition, and pseudo word recognition, and conducted a number of user studies. After studying the users for some time it was found that users were able to recognize over 90% of the images in training set. This study showed that the pictures are the most effective among the three proposed schemes.
Sobrado and Birget [7] developed a graphical password technique that deals with the *Shoulder-Surfing Problem*. In the first scheme, the system will display a number of pass-objects (pre-selected by the user) among many others. To be authenticated, a user needs to recognize pass-objects and click inside the convex hull formed by all pass-objects. Man et al [8] proposed another Shoulder-surfing resistant algorithm where the selected pass-objects have variants. Hong, et al. [10] later extended this approach to allow the user to assign their own codes to pass-object variant.
Other works include *Real User Corporation's "Preface"* [11] where the user will be asked to choose four faces from a face database as their password. Later on *Davis* [9] improved this technique. *Jansen* [12-14] proposed a graphical password model for mobile devices, which was also discussed by *Takada and Koike* [16].

RECALL BASED TECHNIQUE: We would discuss two types of picture password technique in this section:

- *Reproducing a drawing*
- *Repeating a selection*

Reproduce a Drawing: Jermyn [15] proposed a technique, called "Draw-A-Secret (DAS)", which allows the user to draw their unique password. The basic concept behind Draw a Secret (DAS) [Figure 2, 3, 4] is that humans excel at image recognition and memory, so "passwords" should be designed to leverage that ability. Initial implementations simply tracked the ability of people to use a stylus to draw a free-form shape on a touch-sensitive screen. But the people behind the new work have previously refined the technique by parsing the shapes with a flexible grid, which allowed them to more accurately recognize key features such as changes in the stroke's direction. The primary limitation of this DAS system is the user's ability to accurately redraw a complex shape from memory.

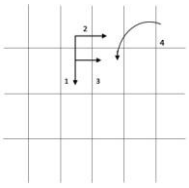

Figure 2: 4x6 DAS password

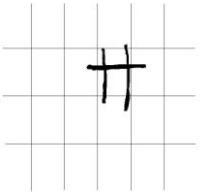

Figure 3: Centered Password

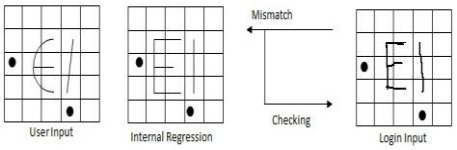

Figure 4: DAS Checking Scheme

The revised version of DAS, which the authors termed Background Draw a Secret, seems to work. Tests, users created BDAS passwords that contained an extra 10 bits of extractable data compared to those who did not use a background image. A week later, 95 percent of the subjects were able to recall their password drawings within three attempts.

Thorpe and Van Oorschot [17] analyzed the password space of the graphical password scheme by Jermyn [15]. They introduced the concept of graphical dictionaries and studied the possibility of a brute force attack using such dictionaries. They further studied [18] the impact of password length and stroke-count as a complexity property f the DAS scheme Thorpe and van Oorschot proposed a "Grid Selection" Technique which would increase the DAS password space.
Goldberg [19] did a user study in which they used a technique called "Passdoodle". This is a graphical password comprised of handwritten designs or text, usually drawn with a stylus onto a touch sensitive screen. *Nali and Thorpe* [21] conducted further analysis of DAS scheme. However, this user study only asked the users to draw a memorable password, but did not do any recall-test on whether or not the passwords were really memorable.

Figure 5: PassFace, an example

Repeating a Selection: *Blonder* [24] designed a graphical password scheme in which a password is created by having the user click on several locations on an image. During authentication, the user must click on the approximate areas o those locations. *Passlogix* [23] has developed a graphical password system based on this idea. In their implementation the users must click on various items of the image in the correct sequence in order to be authenticated. The "PassPoint" system by Wiendenback [26-27] extended Blonder's idea by eliminating the predefined boundaries and allowing arbitrary imagesto be used. As a result, a user can click on any place on an image (as opposed to some pre-defined areas) to create a password. This technique is based on the discretization method proposed by *Birget* [28]. *Adrian Perrig* was reported to be working on a system (called *Map Authentication*) that was based on navigating through a virtual world [25]. In this system the user can build their own virtual world.

IS GRAPHICAL PASSWORD AS SECURE AS TEXT-BASED PASSWORD?

Since graphical passwords are not widely used in practice, very little research has been done to study the difficulty of cracking graphical passwords. But considering some points, as discussed below, we can see that with respect to some points graphical passwords can be considered a good option to be used for authentication. And at some places graphical passwords outclass the text based passwords. Let us examine some of the points to do comparison study of graphical passwords with text-based passwords.

DICTIONARY ATTACKS: One of the problems with text based passwords is dictionary attacks. Since recognition based graphical passwords involve the user to input using mouse instead of keyboard, it is impractical to carry out dictionary attacks against this type of graphical passwords. For some recall based graphical passwords, it is possible to have a dictionary attack, but it will be more complex. So, we can say that graphical passwords are less vulnerable to dictionary attacks than text-based passwords.

GUESSING: This is the weakest part existing in graphical passwords. Unfortunately, it seems that graphical passwords are often predictable, serious problem typically associated with text-based passwords. Studies on the Passface technique have shown that people often choose predictable graphical passwords. *Nali and Thorpe's* study revealed similar predictability among the graphical passwords created with the DAS technique.

BRUTE FORE SEARCH: The main defense against the *brute force search or exhaustive search* is to have a sufficiently large password space. In case of text based passwords, the password space is 94^N, where N is the length of the password, 94 is the number of printable characters excluding SPACE. It has been seen that some graphical password techniques have a password space similar to or larger than that of text-based passwords. It is more difficult to carry out a brute force search against graphical password than text-based passwords. Hence, we believe a graphical password is less vulnerable to brute force search than text-based password.

SOME OTHER POINTS: In computer security, *shoulder-surfing* refers to using direct observation techniques, such as looking over someone's shoulder, to get information. Like text based passwords graphical passwords are also vulnerable to *Shoulder-Surfing*. 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. Comparing to text-based password it is difficult for a user to give a graphical password to another person. For example, giving the graphical password through phone is difficult.]

So we see that it is more difficult to crack graphical passwords than text-based passwords using the conventional attack methods like the dictionary attack, brute force search and spyware. But some points also make graphical passwords less usable. Therefore, more research needs to be done to investigate possible attack methods for graphical passwords.

MAJOR DESIGN AND IMPLEMENTATION ISSUES:

1. SECURITY: We have briefly examined the security issues in the above section.
2. USABILITY: One of the main points which favors graphical password is that it is easier to remember pictures than text strings. A major complaint of the users using graphical passwords is that the password registrations and log-in process take too long.
3. RELIABILITY: It is the major design issue related to graphical password technique, especially for recall-based methods. In this type of method, the error tolerances have to be set carefully.

4. STORAGE AND COMMUNICATION: It also requires much more storage space than text-based passwords. Thousands and thousands of pictures have to be stored in the centralized database. Network transfer delay is yet another problem arousing out of it.

CONCLUSION:

The past decade has seen a growing interest in understanding and implementing graphical password as an alternative to the traditional text-based passwords. Although the main argument for graphical passwords is that people are better at memorizing graphical passwords than text-based passwords. 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. Much more research and user studies are needed for graphical password techniques to reach higher levels of usefulness.

Password Scheme	Paswword Input	Recapitulation Power	Processing Speed	Authentication
Text Based	Fast	Depend on length and type of character combination.	Fast; Complexity,N	Low
Birget	Fast Input	Low; when large number of objects involved	Slow; Complexity depends in size and type of pictures. Can be given as N!/K!(N-K)! (N is the total number of picture objects; K is the number of pre-registered objects)	High
PassFace	Take longer than Text Based	Easier to remember, but, prediction.	N^K(K is the number of rounds of authentication, N is the total number pf pictures at each round.)	High, but, chance of dictionary attack.
Glodberg	Draw with stylus on touch sensitive screen; time taking	Depends on drawing complicacy.	High Password Space	Guess dictionary attack
DAS	Depends on type of input; Draw with stylus on touch sensitive screen.	Depends on drawing complicacy.	Space consuming	Dcitionary attack
User Authentication by Secured Graphical Password Implementation.	Depends on size of password.	Easy to remember	Minimum consumption due to digitization.	Totally secured; Handwritten Characters are varied from person to person Forgery Detection can be incorporated.

Table 1: Comparison between different methods

REFERENCES:

[1] A S. Patrick, A C. Long, and S. Flinn, "HCI and Security Systems", presented at Cm, Extended Abstracts (Workshops). Ft Lauderdale, Florida, USA., 2003.

[2] A. Adams and M. A. Sasse, "Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures," *Communications of th ACM*, vol. 42 pp. 41-46, 1999.

[3] R. Dhamija and A Perrig, "Deja Vu: A User Study Using Images For Authentication", 9th USENIX Security Symposium, 2000.

[5] S. Akula and V. Devisetty, "Image Based Registration and Authentication System," in *Proceedings of Midwest Instruction and Computing Symposium*, 2004.

[4] A. Perrig and D. Song, "Hash Visualizations: A New Technique To Improve Real-World Security," in

Proceedings of the 1999 International Workshop on Cryptographic Techniques and E-Commerce, 1999.

[6] D. Weinshall and S. Kirkpatrick, "Passwords You'll Never Forget, but Can't Recall," *in Proceedings of Conference on Hman Factors in Computing Systems (CHI),* Vienna, Austria: ACM, 2004.

[7] L. Sabrado and J. C. Birget, "Graphical passwords", *The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research*, vol 4, 2002.

[8] S. Man, D. Hong, and M. Mathews, "A Shoulder-Surfing resistant graphical password scheme," in *Proceedings of International Conference on security and management* Las Vegas, NV, 2003.

[9] D.Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes," in *Proceedings of the 13th Usenix Security Symposium*, San Diego, CA, 2004.

[10] 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, 2003.

[11] RealUser, www.realuser.com. last accessed in June, 2005.

[12] W. Jansen, "Authenticating Mobile Device Users Through Image Selection," in *Data Security*, 2004.

[13] W. Jnasen, S. Gavrila, V. Korolev, R. Ayers, and R. Swanstrom, "Picture Password:A Visual Login Technique for Mobile Devices," National Institute of Standards and Technology Interagency Report NISTIR 7030, 2003.

[14] W. Jansen, "Authenticating Users on Handheld Devices," *in Proceedings of Canadian Information Technology Security Symposium*, 2003.

[15] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The Design and Analysis of Graphical Passwords," in Proceedings of the 8th USENIX Security Symposium, 1999.

[16] T. Takada and H. Koike, "Awase-E: Image-based Authentication for Mobile Phones using User's Favorite Images," in Human-Computer Interaction with Mobile Devices and Services, vol. 2795/2003: Springer-Verlag GmbH, 2003, pp. 347-351.

[17] J. Thorpe and P. C. v. Oorschot, "Graphical Dictionaries and the Memorable Space of Graphical Passwords," in *Proceedings of the 20th Annual Computer Security Applications Conference* Tueson, Arizona, 2004.

[18] Julie Thorpe and P.C. van Oorschot, "Towards Secure Design Choices for Implementing Graphical Passwords", *IEEE CS Proceedings of the 20th Annual Computer Security Applications Conference (ACSAC'04)*.

[19] J. Goldberg, J. Hagman, V. Sazawal, "Doodling Our Way To Better Authentication", CHI '02 extended abstracts on Human Factors in Computer Systems, 2002.

[20] J. Thorpe and P. C. v. Oorschot, "Towards Secure Design Choices for Implementing Graphical Passwords," in *20th Annual Computer Security Applications Conference (ACSAC)* Tueson, USA.: IEEE, 2004.

[21] Nali and J. Thorpe, "Analysing User Choice in Graphical Passwords", Technical Report TR-04-o1, School of Computer Science, Carleton University, Canada, 2004.

[22] A. F. Syukri, E. Okamoto, and M. Mambo, "A User Identification System Using Signature Written With Mouse," in *Third Australasian Conference on Information Security and Privacy (ACISP*): Springer-Verlag Lecture Notes in Computer Science (1948), 1998, pp. 403-441.

[23] Passlogix, "www.passlogix.com," last accessed in June 2005.

[24] G. E. Blonder, "Graphical Passwords," in *Lucent Technologies, Inc., Murray Hill, NJ*, U. S. Patent, Ed. United States, 1996.

[25] L. D. Paulson, "Taking a Graphical Appraoch to the Password," *Computer*, vol. 35, pp. 19, 2002.

[26] Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy and Nasir Memon, "Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice", SOUPS'05 Conference, July 6-8, 2005, Pittsburgh, PA, USA.

[27] Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy and Nasir Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system", *International Journal of Human-Computer Studies* (Special Issue on HCI Research in Privacy and Security) 63, 102-127, 2005. - Elsevier Ltd, http://www.science<tirect.com.

[28] Jean-Camille Birget, Dawei Hong and Nasir Memon, uGraphical Passwords Based on Robust Discretization", IEEE Transactions on Information Forensics and Security, Vol. 1, No.3, September 2006.