International Journal of Advanced Science and Research
ISSN: 2455-4227, Impact Factor: RJIF 5.12
www.allsciencejournal.com
Volume 1; Issue 11; November 2016; Page No. 15-18

Authentication using graphical passwords

Priyanka Garg

Dept. of Computer Science & Engg. Gian Jyoti Group of Institution, Patiala, Punjab, Inida

Abstract
The most common computer authentication method is to use alphanumerical usernames and passwords. This method has been shown to have significant drawbacks. For example, users tend to pick passwords that can be easily guessed. On the other hand, if a password is hard to guess, then it is often hard to remember due to long random appearing. To address this problem, some researchers have developed authentication methods that use graphics as passwords. Graphical passwords have been designed to try to make passwords more memorable and easier for people to use and, therefore, more secure. In this paper, we conduct a survey of the existing graphical password techniques. We classify these techniques into two categories: recognition-based and recall-based approaches. We discuss the strengths and limitations of each method and point out the future research directions in this area. We also try to answer two important questions: "Are graphical passwords as secure as text-based passwords?"; "What are the major design and implementation issues for graphical passwords?" This survey will be useful for information security researchers and practitioners who are interested in finding an alternative to text-based authentication methods.

Keywords: graphical passwords, alphanumerical

1. Introduction
Human factors are often considered the weakest link in a computer security system. Patrick, *et al.* [1] point out that there are three major areas where human computer interaction is important: authentication, security operations, and developing secure systems. Here we focus on the authentication problem. The most common computer authentication method is for a user to submit a user name and a text password. The vulnerabilities of this method have been well known. One of the main problems is the difficulty of remembering passwords. Studies have shown that users tend to pick short passwords or passwords that are easy to remember [2]. Unfortunately, these passwords can also be easily guessed or broken

The problem arises because passwords are expected to comply with two fundamentally conflicting requirements:

1) Passwords should be easy to remember, and the user authentication protocol should be executable quickly and easily by humans.
2) Passwords should be secure, i.e., they should look random and should be hard to guess; they should be changed frequently, and should be different on different accounts of the same user; they should not be written down or stored in plain text.

According to a recent Computerworld news article, the security team at a large company ran a network password cracker and within 30 seconds, they identified about 80% of the passwords [3]. On the other hand, passwords that are hard to guess or break are often hard to remember. Studies showed that since user can only remember a limited number of passwords, they tend to write them down or will use the same passwords for different accounts [4, 5]. To address the problems with traditional username password authentication, alternative authentication methods, such as biometrics [3, 6], have been used. In this paper, however, we will focus on another alternative: using pictures as passwords. 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; psychological studies supports such assumption [7]. Pictures are generally easier to be remembered or recognized than text. In addition, if the number of possible pictures is sufficiently large, the possible password space of a graphical password scheme may exceed that of textbased schemes and thus presumably offer better resistance to dictionary attacks. Because of these (presumed) advantages, there is a growing interest in graphical password. In addition to workstation and web log-in applications, graphical passwords have also been applied to ATM machines and mobile devices. In this paper, we conduct a comprehensive survey of the existing graphical password techniques. We will discuss the strengths and limitations of each method and also point out future research directions in this area.

In conducting this survey, we want to answer the following questions:

- Are graphical passwords as secure as text passwords?
- What are the major design and implementation issues for graphical passwords?

This paper will be particularly useful for researchers who are interested in developing new graphical password algorithms as well as industry practitioners who are interested in deploying graphical password techniques.

2. Overview of the Authentication Methods
Current authentication methods can be divided into three main areas:

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

Token based techniques, such as key cards, bank cards and smart cards are widely used. Many token-based authentication systems also use knowledge based techniques to enhance

security. For example, ATM cards are generally used together with a PIN number. Biometric based authentication techniques, such as fingerprints, iris scan, or facial recognition, are not yet widely adopted. The major drawback of this approach is that such systems can be expensive, and the identification process can be slow and often unreliable. However, this type of technique provides the highest level of security. Knowledge based techniques are the most widely used authentication techniques and include both text-based and picture-based passwords. The picture-based techniques can be further divided into two categories: recognition-based and recall-based graphical techniques. Using recognition-based techniques, a user is presented with a set of images and the user passes the authentication by recognizing and identifying the images he or she selected during the registration stage. Using recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage.

3. The survey

3.1 Recognition Based Techniques

We developed a graphical password scheme based on Blonder's original idea that overcomes its limitations of needing simple, artificial images, predefined regions, and consequently many clicks in a password. Our scheme: (1) allows any image to be used and (2) does not need artificial predefined click regions with well-marked boundaries – a password can be any arbitrarily chosen sequence of points in the image (Birget, Hong, & Memon, 2003). Complex images can have hundreds of memorable points, so for example, with 5 or 6 click points one can make more passwords than 8-character Unix-style passwords. In order to log in, the user has to click close to the chosen click points, within some set tolerance distance, e.g., within .25 to .50 cm from the user's click point. The tolerance is needed because the user's click point literally is a single pixel, which is too precise for a user to click on successfully. The tolerance, which is adjustable in the system, gives a margin of error around the click point, in which the user's click is recognized as correct. In Wiedenbeck *et al.* (2005) we compare the password space of Pass Points with alphanumeric passwords, for various parameter settings. The password space is the set of all passwords that are possible for a given password scheme and for a given setting of parameters. For example, for alphanumeric passwords of length 8 over a 64- character alphabet, the number of possible passwords is 648 = 2.8 x 1014. In Pass Points if the image size is 1024 x 752 (i.e., roughly the full screen), with a tolerance around the click point of 20 x 20 pixels, and with passwords consisting of 5 clicks, the password space will have size 2.6 x 1016.

3.2 Recall Based Techniques

In this section we discuss two types of picture password techniques: reproducing a drawing and repeating a selection.

3.2.1 Reproduce a Drawing

Jermyn, *et al.* [8] proposed a technique, called "Draw - a - secret (DAS)", which allows the user to draw their unique password (figure 6). A user is asked to draw a simple picture on a 2D grid. The coordinates of the grids occupied by the picture are stored in the order of the drawing. During authentication, the user is asked to re-draw the picture. If the drawing touches the same grids in the same sequence, then the user is authenticated. Jermyn, *et al.* suggested that given reasonable-length passwords in a 5 X 5 grid, the full password space of DAS is larger than that of the full text password space.

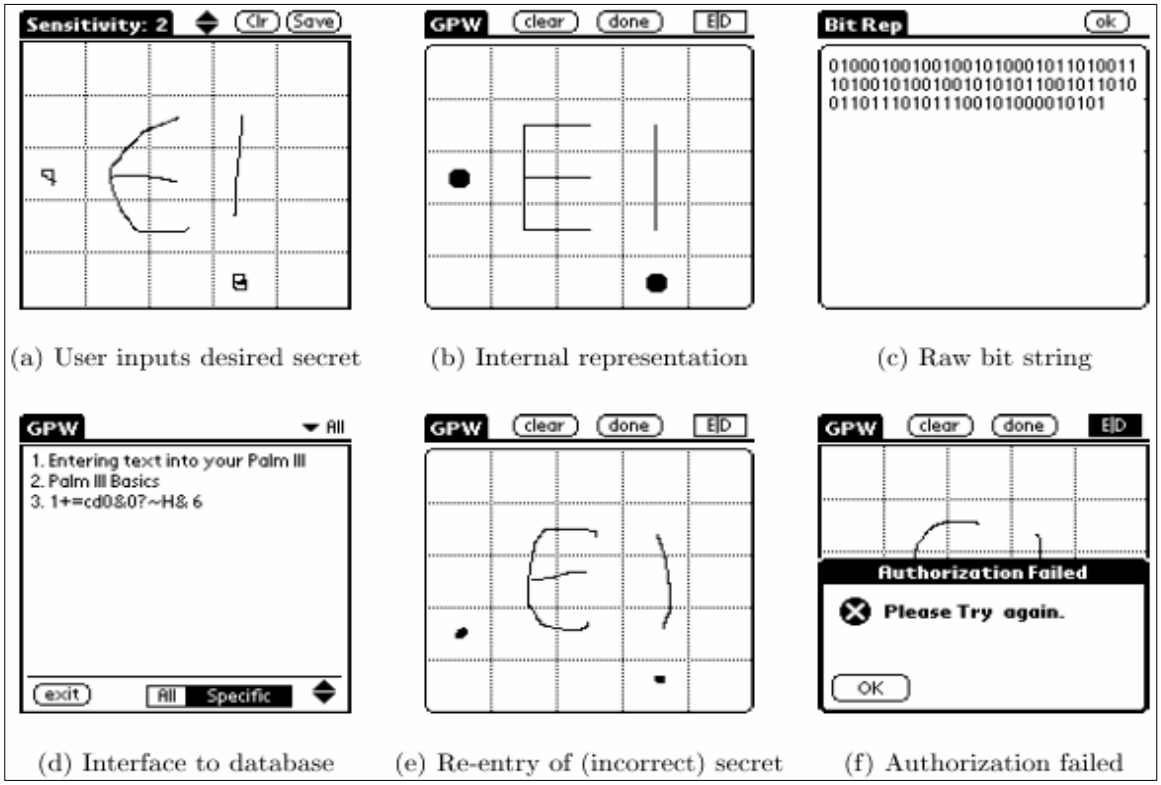

Fig 6: Draw-a-Secret (DAS) technique proposed by Jermyn, *et al.* [24]

Thorpe and van Oorschot [9] analyzed the memorable password space of the graphical password scheme by Jermyn *et al.* [8]. They introduced the concept of graphical dictionaries and studied the possibility of a brute-force attack using such dictionaries. They defined a length parameter for the DAS type graphical passwords and showed that DAS passwords of length 8 or larger on a 5 x 5 grid may be less susceptible to dictionary attack than textual passwords. They also showed that the space of mirror symmetric graphical passwords is significantly smaller than the full DAS password space. Since people recall symmetric images better than asymmetric images, it is expected that a significant fraction of users will choose mirror symmetric passwords. If so, then the security of the DAS scheme may be substantially lower than originally believed. This problem can be resolved by using longer passwords. Thorpe and van Oorschot showed that the size of the space of mirror symmetric passwords of length about L + 5 exceeds that of the full password space for corresponding length L <= 14 on a 5 x 5 grid. Thorpe and van Oorschot [10] further studied the impact of password length and stroke-count as a complexity property of the DAS scheme. Their study showed that stroke-count has the largest impact on the DAS password space - The size of DAS password space decreases significantly with fewer strokes for a fixed password length. The length of a DAS password also has a significant impact but the impact is not as strong as the stroke-count. To improve the security, Thorpe and van Oorschot proposed a "Grid Selection" technique. The selection grid is an initially large, fine grained grid from which the user selects a drawing grid, a rectangular region to zoom in on, in which they may enter their password (figure 7). This would significantly increase the DAS password space. Goldberg *et al.* [11] 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. Their study concluded that users were able to remember complete doodle images as accurately as alphanumeric passwords. The user studies also showed that people are less likely to recall the order in which they drew a DAS password. However, since the user study was done using a paper prototype instead of computer programs, with verifications done by a human rather than computer, the accuracy of this study is still uncertain.

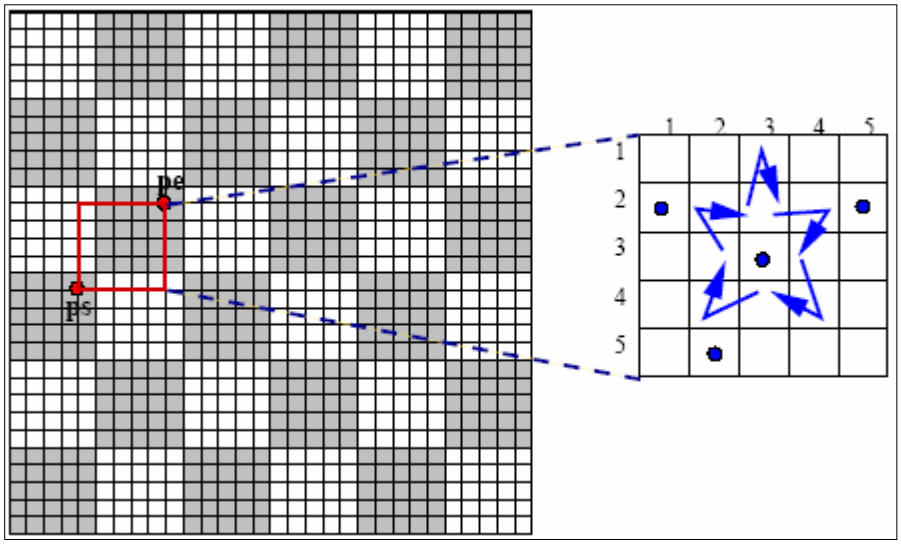

Fig 7: Grid selection: user selects a drawing grid. (Source: Thorpe and Van Oorschot [28])

3.2.2 Repeat a sequence of actions

Blonder [12] 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 of those locations. The image can assist users to recall their passwords and therefore this method is considered more convenient than unassisted recall (as with a text-based password). Passlogix [13] has developed a graphical password system based on this idea. In their implementation (figure 9), users must click on various items in the image in the correct sequence in order to be authenticated. Invisible boundaries are defined for each item in order to detect whether an item is clicked by mouse. A similar technique has been developed by sfr [14]. It was reported that Microsoft had also developed a similar graphical password technique where users are required to click on pre-selected areas of an image in a designated sequence [15]. But details of this technique have not been available.

4. What are the major design and implementation issues of graphical passwords?

Security: In the above section, we have briefly examined the security issues with graphical passwords. Usability

One of the main arguments for graphical passwords is that pictures are easier to remember than text strings. Preliminary user studies presented in some research papers seem to support this. However, current user studies are still very limited, involving only a small number of users. We still do not have convincing evidence demonstrating that graphical passwords are easier to remember than text based passwords. A major complaint among the users of graphical passwords is that the password registration and log-in process take too long, especially in recognition-based approaches. For example, during the registration stage, a user has to pick images from a large set of selections. During authentication stage, a user has to scan many images to identify a few pass-images. Users may find this process long and tedious. Because of this and also because most users are not familiar

with the graphical passwords, they often find graphical passwords less convenient than text based passwords. Reliability The major design issue for recall-based methods is the reliability and accuracy of user input recognition. In this type of method, the error tolerances have to be set carefully – overly high tolerances may lead to many false positives while overly low tolerances may lead to many false negatives. In addition, the more error tolerant the program, the more vulnerable it is to attacks. Storage and communication Graphical passwords require much more storage space than text based passwords. Tens of thousands of pictures may have to be maintained in a centralized database. Network transfer delay is also a concern for graphical passwords, especially for recognition-based techniques in which a large number of pictures may need to be displayed for each round of verification.

5. 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, we have conducted a comprehensive survey of existing graphical password techniques. The current graphical password techniques can be classified into two categories: recognition-based and recall-based techniques. A comparison of current graphical password techniques is presented in Table 1. Although the main argument for graphical passwords is that people are better at memorizing graphical passwords than text-based passwords, the existing user studies are very limited and there is not yet convincing evidence to support this argument. Our preliminary analysis suggests that it is more difficult to break graphical passwords using the aditional 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. User authentication is a fundamental component in most computer security contexts. In this extended abstract, we proposed a simple graphical password authentication system. The system combines graphical and text-based passwords trying to achieve the best of both worlds. It also provides multi-factor authentication in a friendly intuitive system. We described the system operation with some examples, and highlighted important aspects of the system.

6. References

1. Patrick AS, Long AC, Flinn S. HCI and Security Systems, presented at CHI, Extended Abstracts (Workshops). Ft. Lauderdale, Florida, USA, 2003.
2. Adams A, Sasse MA. Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures, Communications of the ACM. 1999; 42:41-46.
3. Gilhooly K. Biometrics: Getting Back to Business, in Computerworld. 2005.
4. Dhamija R, Perrig A. Deja Vu: A User Study Using Images for Authentication, in Proceedings of 9th USENIX Security Symposium, 2000.
5. Kotadia M. Microsoft: Write down your passwords, in ZDNet Australia, 2005.
6. Jain A, Hong L, Pankanti S. Biometric identification, Communications of the ACM. 2000; 33:168-176.
7. Shepard RN. Recognition memory for words, sentences, and pictures, Journal of Verbal Learning and Verbal Behavior. 1967; 6:156-163.
8. Jermyn I, Mayer A, Monrose F, Reiter MK, Rubin AD. The Design and Analysis of Graphical Passwords, in Proceedings of the 8th USENIX Security Symposium, 1999.
9. Thorpe J, Oorschot PCV. Graphical Dictionaries and the Memorable Space of Graphical Passwords, in Proceedings of the 13th USENIX Security Symposium. San Deigo, USA: USENIX, 2004.
10. Thorpe J, Oorschot PCV. Towards Secure Design Choices for Implementing Graphical Passwords, in Proceedings of the 20th Annual Computer Security Applications Conference. Tucson, Arizona, 2004.
11. Goldberg J, Hagman J, Sazawal V. Doodling Our Way to Better Authentication, presented at Proceedings of Human Factors in Computing Systems (CHI), Minneapolis, Minnesota, USA, 2002. [31] G. E. Blonder, Graphical passwords, in Lucent Technologies, Inc., Murray Hill NJ, US. Patent, Ed. United States, 1996.
12. Blonder GE. Graphical passwords, in Lucent Technologies, Inc., Murray Hill, NJ, US. Patent, Ed. United States, 1996.
13. Passlogix, www.passlogix.com, last accessed in June 2005.
14. Sfr www.viskey.com/tech.html, last accessed in, 2005.
15. Paulson LD. Taking a Graphical Approach to the Password, Computer. 2002; 35:19.