Graphical Passwords: A Survey

Xiaoyuan Suo Ying Zhu G. Scott. Owen
Department of Computer Science
Georgia State University
xsuo@student.gsu.edu, yzhu@cs.gsu.edu, owen@siggraph.org

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. To address this problem, some researchers have developed authentication methods that use pictures as passwords. In this paper, we conduct a comprehensive 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.

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. 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, 7], 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 [8]. 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 text-based 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

Dhamija and Perrig [4] proposed a graphical authentication scheme based on the Hash Visualization technique [9]. In their system, the user is asked to select a certain number of images from a set of random pictures generated by a program (figure 1). 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 and PINS. The average log-in time, however, is longer than the traditional approach. A weakness of this system is that the server needs to store the seeds of the portfolio images of each user in plain text. Also, the process of selecting a set of pictures from the picture database can be tedious and time consuming for the user.

Akula and Devisetty's algorithm [10] is similar to the technique proposed by Dhamija and Perrig [4]. The difference is that by using hash function SHA-1, which produces a 20 byte output, the authentication is secure and require less memory. The authors suggested a possible future improvement by providing persistent storage and this could be deployed on the Internet, cell phones and PDA's.

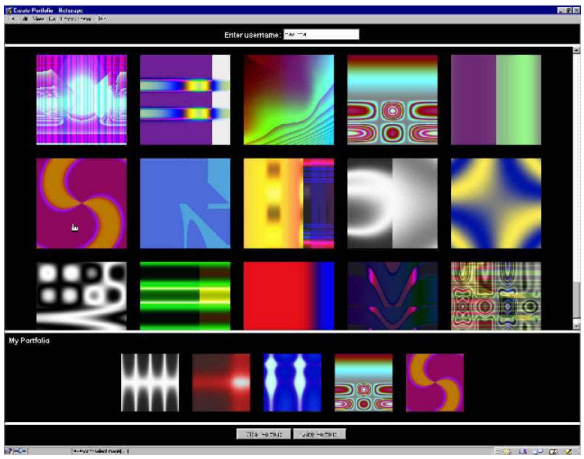

Figure 1.Random images used by Dhamija and Perrig [4]

Weinshall and Kirkpatrick [11] sketched several authentication schemes, such as picture recognition, object recognition, and pseudo word recognition, and conducted a number of user studies. In the picture recognition study, a user is trained to recognize a large set of images (100 – 200 images) selected from a database of 20,000 images. After one to three months, users in their study were able to recognize over 90% of the images in the training set. This study showed that pictures are the most effective among the three schemes tested. Pseudo codes can also be used, but require proper setting and training.

Sobrado and Birget [12] 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 user) among many other objects. To be authenticated, a user

needs to recognize pass-objects and click inside the convex hull formed by all the pass-objects (figure 2). In order to make the password hard to guess, Sobrado and Birget suggested using 1000 objects, which makes the display very crowded and the objects almost indistinguishable, but using fewer objects may lead to a smaller password space, since the resulting convex hull can be large. In their second algorithm, a user moves a frame (and the objects within it) until the pass object on the frame lines up with the other two pass-objects. The authors also suggest repeating the process a few more times to minimize the likelihood of logging in by randomly clicking or rotating. The main drawback of these algorithms is that the log in process can be slow.

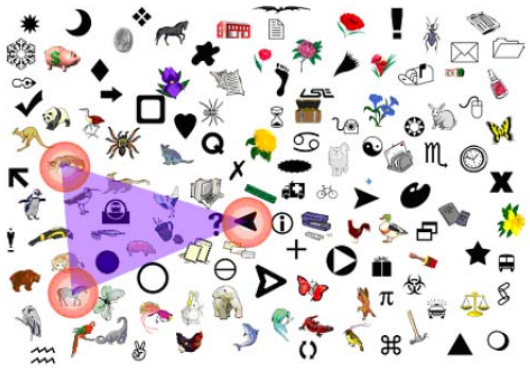

Figure 2. A shoulder-surfing resistant graphical password scheme [12]

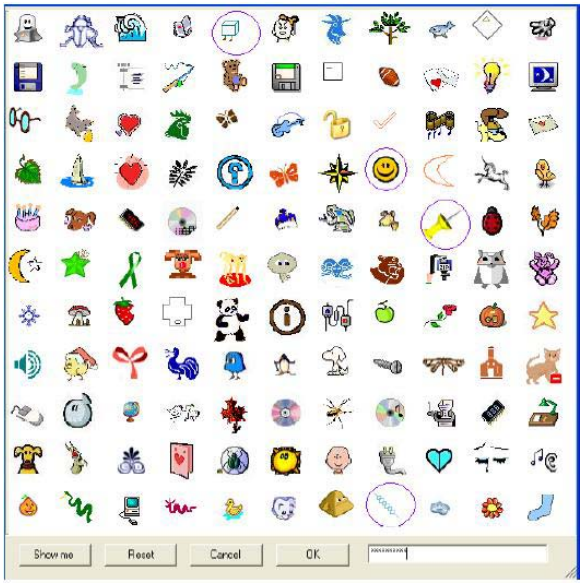

Figure 3. Another shoulder surfing resistant scheme developed by Hong, et al. [13]. The pass-string is 99dc815lup

Man, et al. [14] proposed another shoulder-surfing resistant algorithm. In this algorithm, a user selects a number of pictures as pass-objects. Each pass-object has several variants and each variant is assigned a unique code. During authentication, the user is challenged with several scenes. Each scene contains several pass-objects (each in the form of a randomly chosen variant) and many decoy-objects. The user has to type in a string with the unique codes corresponding to the pass-object variants present in the scene as well as a code indicating the relative location of the pass-objects in reference to a pair of eyes. The argument is that it is very hard to crack this kind of password even if the whole authentication process is recorded on video because where is no mouse click to give away the pass-object information. However, this method still requires users to memorize the alphanumeric code for each pass-object variant. Hong, et al. [13] later extended this approach to allow the user to assign their own codes to pass-object variants. Figure 3 shows the log-in screen of this graphical password scheme. However, this method still forces the user to memorize many text strings and therefore suffer from the many drawbacks of text-based passwords.

Figure 4. An example of Passfaces (source: www.realuser.com)

"Passface" is a technique developed by Real User Corporation [15]. The basic idea is as follows. The user will be asked to choose four images of human faces from a face database as their future password. In the authentication stage, the user sees a grid of nine faces, consisting of one face previously chosen by the user and eight decoy faces (figure 4). The user recognizes and clicks anywhere on the known face. This procedure is repeated for several rounds. The user is authenticated if he/she correctly identifies the four faces. The technique is based on the assumption that people can recall human faces easier than other pictures. User studies by Valentine [16, 17] have shown that Passfaces are very memorable over long intervals. Comparative studies conducted by Brostoff and Sasse [18] showed that Passfaces had only a third of the login failure rate of text-based passwords, despite having about a third the frequency of use.

Their study also showed that the Passface-based log–in process took longer than text passwords and therefore was used less frequently by users. However the effectiveness of this method is still uncertain. Davis, et al. [19] studied the graphical passwords created using the Passface technique and found obvious patterns among these passwords. For example, most users tend to choose faces of people from the same race. This makes the Passface password somewhat predictable. This problem may be alleviated by arbitrarily assigning faces to users, but doing so would make it hard for people to remember the password.

Jansen et al. [20-22] proposed a graphical password mechanism for mobile devices. During the enrollment stage, a user selects a theme (e.g. sea, cat, etc.) which consists of thumbnail photos and then registers a sequence of images as a password (figure 5). During the authentication, the user must enter the registered images in the correct sequence. One drawback of this technique is that since the number of thumbnail images is limited to 30, the password space is small. Each thumbnail image is assigned a numerical value, and the sequence of selection will generate a numerical password. The result showed that the image sequence length was generally shorter than the textural password length. To address this problem, two pictures can be combined to compose a new alphabet element, thus expanding the image alphabet size.

Figure 5. A graphical password scheme proposed by Jansen, et al. [20]

Takada and Koike discussed a similar graphical password technique for mobile devices. This technique allows users to use their favorite image for authentication [23]. The users first register their favorite images (pass-images) with the server. During authentication, a user has to go through several rounds of verification. At each round, the user either selects a pass-image among several decoy-images or chooses nothing if no pass-image is present. The program would authorize a user only if all verifications are successful. Allowing users to register their own images makes it easier for user to remember their pass-images. A notification mechanism is also implemented to notify users when new images are registered in order to prevent unauthorized image registration. This method does not necessarily make it a more secure authentication method than text-based passwords. As shown in the studies by Davis [19], users' choices of picture passwords are often predictable. Allowing users to use their own pictures would make the password even more predictable, especially if the attacker is familiar with the user.

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. [24] 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.

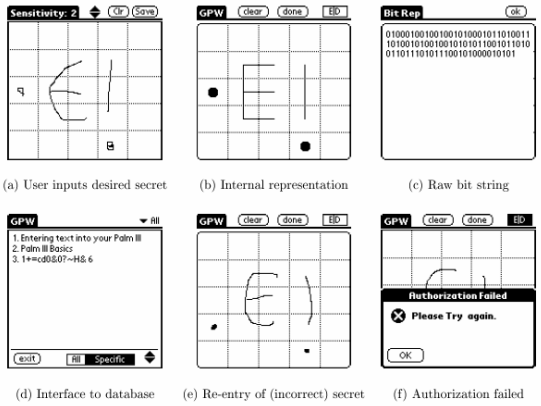

Figure 6. Draw-a-Secret (DAS) technique proposed by Jermyn, et al. [24]

Thorpe and van Oorschot [25] analyzed the memorable password space of the graphical password scheme by Jermyn et al. [24]. 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 [26] 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. [27] 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.

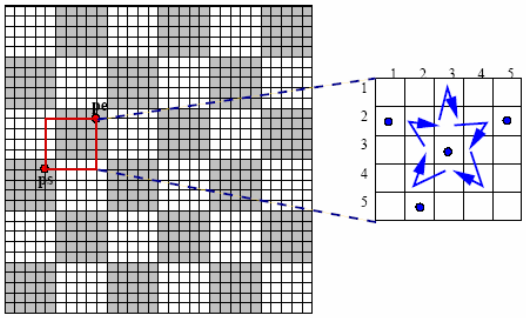

Figure 7. Grid selection: user selects a drawing grid. (Source: Thorpe and Van Oorschot [28])

Nali and Thorpe [29] conducted further analysis of the “Draw-A-Secret (DAS)” scheme [24]. In their study, users were asked to draw a DAS password on paper in order to determine if there are predictable characteristics in the graphical passwords that people choose. The study did not find any predictability in the start and end points for DAS password strokes, but found that certain symmetries (e.g. crosses and rectangles), letters, and numbers were common. This study showed that users choose graphical passwords with predictable characteristics, particularly those proposed as "memorable". If this study is indicative of the population, the probability in which some of these characteristics occur would reduce the entropy of the DAS password space. 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.

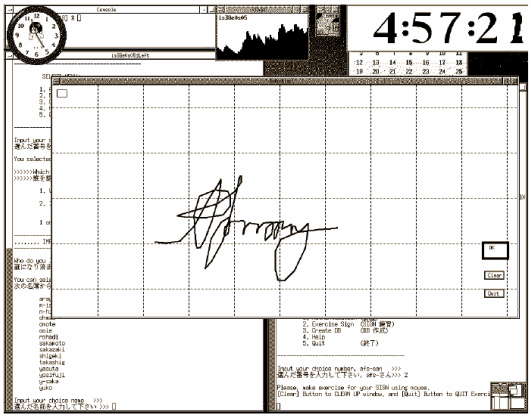

Figure 8. A signature is drawn by mouse. Syukri, et al. [30]

Syukri, et al. [30] proposes a system where authentication is conducted by having the user drawing their signature using a mouse (figure 8). Their technique included two stages, registration and

verification. During the registration stage: the user will first be asked to draw their signature with a mouse, and then the system will extract the signature area and either enlarge or scale-down the signature, and rotates if needed, (also known as normalizing). The information will later be saved into the database. The verification stage first takes the user input, and does the normalization again, and then extracts the parameters of the signature. After that, the system conducts verification using geometric average means and a dynamic update of the database. According to the paper the rate of successful verification was satisfying. The biggest advantage of this approach is that there is no need to memorize one's signature and signatures are hard to fake. However, not everybody is familiar with using a 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. We believe such a technique is more useful for small devices such as a PDA, which may already have a stylus.

3.2.2 Repeat a sequence of actions

Blonder [31] 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 [32] 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* [33]. 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 [34]. But details of this technique have not been available.

The "PassPoint" system by Wiedenbeck, et al. [35-37] extended Blonder's idea by eliminating the predefined boundaries and allowing arbitrary images to 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. A tolerance around each chosen pixel is calculated. In order to be authenticated, the user must click within the tolerance of their chosen pixels and also in the correct sequence (figure 10). This technique is based on the discretization method proposed by Birget, et al. [38]. Because any picture can be used and because a picture may contain hundreds to thousands of memorable points, the possible password space is quite large. Wiedenbeck, et al. conducted a user study [37], in which one group of participants were asked to use alphanumerical password, while the other group was asked to use the graphical password. The result showed that graphical password took fewer attempts for the user than alphanumerical passwords. However, graphical password users had more difficulties learning the password, and took more time to input their passwords than the alphanumerical users.

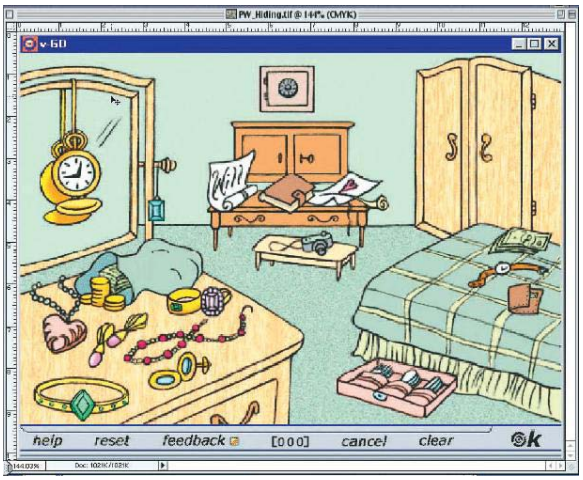

Figure 9. A recall-based technique developed by Passlogix [34]

Figure 10. An image used in the Passpoint Sytem, Wiedenbeck, et al. [35]

Later Wiedenbeck, et al. [36] also conducted a user study to evaluate the effect of tolerance of clicking during the re-authenticating stage, and the effect of image choice in the system. The result showed that memory accuracy for the graphical password was

strongly reduced by using a smaller tolerance for the user clicked points, but the choices of images did not make a significant difference. The result showed that the system works for a large variety of images.

Passlogix [32] has also developed several graphical password techniques based on repeating a sequence of actions. For example, its v-Go includes a graphical password scheme where users can mix up a virtual cocktail and use the combination of ingredients as a password. Other password options include picking a hand at cards or putting together a "meal" in the virtual kitchen. However, this technique only provides a limited password space and there is no easy way to prevent people from picking poor passwords (for example, a full house in cards).

Adrian Perrig was reported to be working on a system (called Map Authentication) that was based on navigating through a virtual world [34]. In this system, users can build their own virtual world. The authentication is carried out by having users navigate to a site that is randomly chosen each time they log on. However, the details of this system are not available.

Table 1 contains a more detailed comparison of all the above techniques.

4. Discussion

4.1 Is a graphical password as secure as text-based password?

Very little research has been done to study the difficulty of cracking graphical passwords. Because graphical passwords are not widely used in practice, there is no report on real cases of breaking graphical passwords. Here we briefly exam some of the possible techniques for breaking graphical passwords and try to do a comparison with text-based passwords.

Brute force search
The main defense against brute force search is to have a sufficiently large password space. Text-based passwords have a password space of 94^N, where N is the length of the password, 94 is the number of printable characters excluding SPACE. Some graphical password techniques have been shown to provide a password space similar to or larger than that of text-based passwords [24 - 27, 30, 38]. Recognition based graphical passwords tend to have smaller password spaces than the recall based methods.

It is more difficult to carry out a brute force attack against graphical passwords than text-based passwords. The attack programs need to automatically generate accurate mouse motion to imitate human input, which is particularly difficult for recall based graphical passwords. Overall, we believe a graphical password is less vulnerable to brute force attacks than a text-based password.

Dictionary attacks
Since recognition based graphical passwords involve mouse input instead of keyboard input, it will be impractical to carry out dictionary attacks against this type of graphical passwords. For some recall based graphical passwords [24][30], it is possible to use a dictionary attack but an automated dictionary attack will be much more complex than a text based dictionary attack. More research is needed in this area. Overall, we believe graphical passwords are less vulnerable to dictionary attacks than text-based passwords.

Guessing
Unfortunately, it seems that graphical passwords are often predictable, a serious problem typically associated with text-based passwords. For example, studies on the Passface technique have shown that people often choose weak and predictable graphical passwords [19]. Nali and Thorpe's study [29] revealed similar predictability among the graphical passwords created with the DAS technique [24]. More research efforts are needed to understand the nature of graphical passwords created by real world users.

Spyware
Except for a few exceptions [13][14], 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.

Shoulder surfing
Like text based passwords, most of the graphical passwords are vulnerable to shoulder surfing. At this point, only a few recognition-based techniques are designed to resist shoulder-surfing [13][14]. None of the recall-based based techniques are considered should-surfing resistant.

Social engineering
Comparing to text based password, it is less convenient for a user to give away graphical passwords to another person. For example, it is very

difficult to give away graphical passwords over the phone. Setting up a phishing web site to obtain graphical passwords would be more time consuming.

Overall, we believe it is more difficult to break graphical passwords using the traditional attack methods like brute force search, dictionary attack, and spyware. There is a need for more in-depth research that investigates possible attack methods against graphical passwords.

4.2 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 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.

References

[1] A. S. Patrick, A. C. Long, and S. Flinn, "HCI and Security Systems," presented at CHI, 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 the ACM*, vol. 42, pp. 41-46, 1999.

[3] K. Gilhooly, "Biometrics: Getting Back to Business," in *Computerworld, May 09*, 2005.

[4] R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in *Proceedings of 9th USENIX Security Symposium*, 2000.

[5] M. Kotadia, "Microsoft: Write down your passwords," in *ZDNet Australia, May 23*, 2005.

[6] A. Gilbert, "Phishing attacks take a new twist," in *CNET News.com, May 04*, 2005.

[7] A. Jain, L. Hong, and S. Pankanti, "Biometric identification," *Communications of the ACM*, vol. 33, pp. 168-176, 2000.

[8] R. N. Shepard, "Recognition memory for words, sentences, and pictures," *Journal of Verbal Learning and Verbal Behavior*, vol. 6, pp. 156-163, 1967.
[9] A. Perrig and D. Song, "Hash Visualization: A New Technique to Improve Real-World Security," in *Proceedings of the 1999 International Workshop on Cryptographic Techniques and E-Commerce*, 1999.
[10] S. Akula and V. Devisetty, "Image Based Registration and Authentication System," in *Proceedings of Midwest Instruction and Computing Symposium*, 2004.
[11] D. Weinshall and S. Kirkpatrick, "Passwords You'll Never Forget, but Can't Recall," in *Proceedings of Conference on Human Factors in Computing Systems (CHI)*. Vienna, Austria: ACM, 2004, pp. 1399-1402.
[12] L. Sobrado and J.-C. Birget, "Graphical passwords," *The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research*, vol. 4, 2002.
[13] 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 Vergas, NV, 2004.
[14] 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.
[15] RealUser, "www.realuser.com," last accessed in June 2005.
[16] T. Valentine, "An evaluation of the Passface personal authentication system," Technical Report, Goldsmiths College, University of London 1998.
[17] T. Valentine, "Memory for Passfaces after a Long Delay," Technical Report, Goldsmiths College, University of London 1999.
[18] S. Brostoff and M. A. Sasse, "Are Passfaces more usable than passwords: a field trial investigation," in *People and Computers XIV - Usability or Else: Proceedings of HCI*. Sunderland, UK: Springer-Verlag, 2000.
[19] 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.
[20] W. Jansen, "Authenticating Mobile Device Users Through Image Selection," in *Data Security*, 2004.
[21] W. Jansen, 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.
[22] W. A. Jansen, "Authenticating Users on Handheld Devices," in *Proceedings of Canadian Information Technology Security Symposium*, 2003.
[23] 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. pp. 347 - 351.
[24] 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.
[25] J. Thorpe and P. C. v. Oorschot, "Graphical Dictionaries and the Memorable Space of Graphical Passwords," in *Proceedings of the 13th USENIX Security Symposium*. San Deigo, USA: USENIX, 2004.
[26] J. Thorpe and P. C. v. Oorschot, "Towards Secure Design Choices for Implementing Graphical Passwords," in *Proceedings of the 20th Annual Computer Security Applications Conference*. Tucson, Arizona, 2004.
[27] J. Goldberg, J. Hagman, and V. Sazawal, "Doodling Our Way to Better Authentication," presented at Proceedings of Human Factors in Computing Systems (CHI), Minneapolis, Minnesota, USA., 2002.
[28] J. Thorpe and P. C. v. Oorschot, "Towards Secure Design Choices for Implementing Graphical Passwords," in *20th Annual Computer Security Applications Conference (ACSAC)*. Tucson, USA.: IEEE, 2004.
[29] D. Nali and J. Thorpe, "Analyzing User Choice in Graphical Passwords," Technical Report, School of Information Technology and Engineering, University of Ottawa, Canada May 27 2004.
[30] 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 (1438), 1998, pp. 403-441.
[31] G. E. Blonder, "Graphical passwords," in *Lucent Technologies, Inc., Murray Hill, NJ*, U. S. Patent, Ed. United States, 1996.
[32] Passlogix, "www.passlogix.com," last accessed in June 2005.
[33] sfr, "www.viskey.com/tech.html," last accessed in June 2005.
[34] L. D. Paulson, "Taking a Graphical Approach to the Password," *Computer*, vol. 35, pp. 19, 2002.
[35] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Basic results," in *Human-Computer Interaction International (HCII 2005)*. Las Vegas, NV, 2005.
[36] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Effects of tolerance and image choice," in *Symposium on Usable Privacy and Security (SOUPS)*. Carnegie-Mellon University, Pittsburgh, 2005.
[37] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system," *International Journal of Human Computer Studies*, to appear.
[38] J.-C. Birget, D. Hong, and N. Memon, "Robust discretization, with an application to graphical passwords," Cryptology ePrint archive 2003.

Techniques	Usability		Security issues	
	Authentication process	Memorability	*Password space*	*Possible attack methods*
Text-based password	Type in password, can be very fast	Depends on the password. Long and random passwords are hard to remember	94^K (there are 94 printable characters excluding SPACE, N is the length of the password).The actual password space is usually much smaller.	Dictionary attack, brute force search, guess, spyware, shoulder surfing, etc.
Perrig and Song [9]	Pick several pictures out of many choices. Takes longer to create than text password	Limited user study showed that more people remembered pictures than text-based passwords	N!/K!(N-K)! (N is the total number of pictures; K is the number of pictures in the graphical password)	Brute force search, guess, shoulder-surfing
Sobrado and Birget [12]	Click within an area bounded by pre-registered picture objects, can be very fast	Can be hard to remember when large numbers of objects are involved.	N!/K!(N-K)! (N is the total number of picture objects; K is the number of pre-registered objects)	Brute force search, guess
Man, et al. [14] Hong, et al. [13]	Type in the code of pre-registered picture objects; can be very fast	Users have to memorize both picture objects and their codes. More difficult than text-based password	Same as the text based password	Brute force search, spyware
Passface [15]	Recognize and pick the pre-registered pictures; takes longer than text-based password	Faces are easier to remember, but the choices are still predictable	N^K (K is the number of rounds of authentication, N is the total number of pictures at each round)	Dictionary attack, brute force search, guess, shoulder surfing
Jansen et al. [20-22]	User register a sequence of images; slower than text-based password	Pictures are organized according to different themes to help users remember	N^K (N is the total number of pictures, K is the number of pictures in the graphical password. N is small due the size limit of mobile devices)	Brute force search, guess, shoulder surfing
Takada and Koike [23]	Recognize and click on the pre-registered images; slower than text-based password. Slower than text-based password	Users can use their favorite images; easy to remember than system assigned pictures	(N+1)^K (K is the number of rounds of authentication, N is the total number of pictures at each round)	Brute force search, guess, shoulder surfing
Jermyn, et al. [24], Thorpe and van Oorschot [25-26]	Users draw something on a 2D grid	Depends on what users draw. User studies showed the drawing sequence is hard to remember	Password space is larger than text based password. But the size of DAS password space decreases significantly with fewer strokes for a fixed password length	Dictionary attack, shoulder surfing
Syukri, et al. [30]	Draw signatures using mouse. Need a reliable signature recognition program.	Very easy to remember, but hard to recognize	Infinite password space	Guess, dictionary attack, shoulder surfing
Goldberg et al. [27]	Draw something with a stylus onto a touch sensitive screen	Depends on what users draw	Infinite password space	Guess, dictionary attack, shoulder surfing
Blonder [31], Passlogix [32], [33], [34] , Wiedenbeck, et al. [35-37]	Click on several pre-registered locations of a picture in the right sequence.	Can be hard to remember	N^K (N is the number of pixels or smallest units of a picture, K is the number of locations to be clicked on)	Guess, brute force search, shoulder surfing

Table 1. Comparison of major graphical password techniques