VOLUME-9, ISSUE-2, FEBRUARY-2020 • PRINT ISSN No. 2277 - 8160 • DOI : 10.36106/gjra

Original Research Paper

Education

GRAPHICAL PASSWORD AUTHENTICATION - SURVEY

Jasmin P. Bhootwala Research Scholar Calorx Teacher's University Navrangpura, Ahmedabad

Dr. Pravin H. Bhathawala* Research Guide Calorx Teacher's University Navrangpura, Ahmadabad
*Corresponding Author

ABSTRACT The most common computer authentication approach is to use alphanumerical usernames and passwords. This method has been proven to have vast drawbacks. For example, users tend to choose passwords that can be easily guessed. On the other hand, if a password is difficult to guess, then it is frequently difficult to remember. To address this problem, some researchers have developed authentication strategies that use images as passwords. In this paper, we conduct a complete survey of the current graphical password techniques. We classify these strategies into two categories: recognition-based and recall-based approaches. We discuss the strengths and barriers of each technique and point out the future research instructions in this area. We also try to answer two necessary questions: "Are graphical passwords as secure as text-based passwords?"; "What are the important design and implementation issues for graphical passwords?" This survey will be useful for data protection researchers and practitioners who are involved in finding an choice to text-based authentication methods.

KEYWORDS : Graphical Password, Recognition Based Techniques, Recall Based Techniques

1. INTRODUCTION

Human factors are frequently regarded the weakest link in a computer security system. Patrick, et al. [1] point out that there are three important areas the place human-computer interaction is important: authentication, security operations, and creating invulnerable systems. Here we focal point on th e authentication problem. The most common computer authe ntication method is for a user to put up a consumer title and a text password. The vulnerabilities of this technique have been properly known. One of the primary issues is the difficulty of remembering passwords. Studies have shown that users tend to choose short passwords or passwords that are handy to be aware. Unfortunately, these passwords can also be effortlessly guessed or broken.

According to a latest Computerworld information article, the safety group at a massive organization ran a network password cracker and within 30 seconds, they recognized about 80% of the passwords . On the other hand, passwords that are difficult to guess or destroy are often hard to remember. Studies showed that due to the fact user can only keep in mind a confined number of passwords, they have a tendency to write them down or will use the same passwords for different accounts. To address the troubles with ordinary username-password authentication, alternative authentication methods, such as biometr ics , have been used. In this paper, however, we will focus on another alternative: using images as passwords.

Graphical password schemes have been proposed as a possible alternative to text-based schemes, motivated partially by way of the reality that human beings can remember pictures better than text; psychological studies supports such assumption [8]. Pictures are normally simpler to be remembered or identified than text. In addition, if the wide variety of feasible pictures is sufficiently large, the possible password area of a graphical password scheme can also exceed that of text-based schemes and hence possibly provide better resistance to dictionary attacks. Because of these (presumed) advantages, there is a growin g activity in graphical password. In addition to computer and web log-in applications, graphical passwords have also been applied to ATM machines and mobile devices. In this paper, we habits a complete survey of the current graphical password techniques. We will talk about the strengths and barriers of every technique and additionally point out future research instructions 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 primary design and implementation problems for graphical passwords?

This paper will be especially useful for researchers who are involved in developing new graphical password algorithms as properly as enterprise practitioners who are involved 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 broadly used. Many token-based authentication systems additionally use knowledge based techniques to enhance security. For example, ATM cards are commonly used together with a PIN number.

Biometric based authentication techniques, such as fingerprints, iris scan, or facial recognition, are not yet broadly adopted. The main drawback of this method is that such systems can be expensive, and the identification technique can be slow and frequently unreliable. However, this kind of approach presents the best level of security.

Knowledge based techniques are the most widely used authentication methods and consist of both text-based and picture-based passwords. The picture-based techniques can be in addition divided into two categories: recognition-based and recall-based graphical techniques. Using recognition-based techniques, a user is introduced with a set of pictures and the user passes the authentication by means of recognizing and identifying the pictures he or she selected during the registration stage. Using recall-based techniques, a user is requested to reproduce something that he or she created or selected earlier in the course of the registration stage.

3. THE SURVEY

3.1 RECOGNITION BASED TECHNIQUES

Akula and Devisetty's algorithm [2] is similar to the technique proposed by means of Dhamija and Perrig [3]. The difference

is that through using hash feature SHA-1, which produces a 20 byte output, the authentication is invulnerable and require less memory. The authors recommended a feasible future enchancment through offering persistent storage and this could be deployed on the Internet, cell phones and PDA's.

Dhamija and Perrig [3] proposed a graphical authentication scheme based on the Hash Visualization method . In their system, the user is asked to choose a certain variety of images from a set of random images generated through a program (figure 1). Later, the user will be required to identify the pre-selected pictures in order to be authenticated. The effects showed that 90% of all members succeeded in the authentication the use of this technique, while only 70% succeeded the usage of text-based passwords and PINS. The average log-in time, however, is longer than the typical approach. A weak point of this system is that the server desires to keep the seeds of the portfolio pictures of every user in plain text. Also, the procedure of choosing a set of pictures from the image database can be tedious and time consuming for the user.

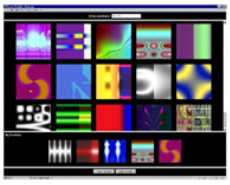

Figure 1. Dhamija and Perrig [3]

Sobrado and Birget [4] 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 way of user) amongst many different objects. To be authenticated, a person wants to recognize pass-objects and click inner the convex hull formed by using all the pass-objects (figure 2). In order to make the password challenging to guess, Sobrado and Birget suggested the use of one thousand objects, which makes the display very crowded and the objects almost indistinguishable, however the usage of fewer objects might also lead to a smaller password space, seeing that the ensuing convex hull can be large. In their 2nd algorithm, a person moves a body (and the objects inside it) until the skip object on the frame lines up with the different two pass-objects. The authors also recommend repeating the process a few more instances to limit the possibility of logging in by way of randomly clicking or rotating. The fundamental disadvantage of these algorithms is that the log in system can be slow.

Weinshall and Kirkpatrick [5] sketched countless authenti cation schemes, such as picture recognition, object recognition, and pseudo word recognition, and carried out a variety of user studies. In the picture recognition study, a user is trained to recognize a large set of pictures (100 – 200 images) selected from a database of 20,000 images. After one to three months, users in their study had been capable to recognize over 90% of the images in the training set. This study showed that images are the most tremendous amongst the three schemes tested. Pseudo codes can also be used, however require proper putting and training.

Figure 2. A shoulder-surfi ng resistant graphical pass word scheme [4]

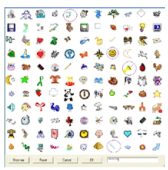

Figure 3. Another shoulder surfing resistant scheme developed by Hong, et al. [13]. The pass-string is 99 dc815lup

Hong, et al. [6] later extended this method to permit the person to assign their personal codes to pass-object variants. However, this method nonetheless forces the person to memorize many textual content strings and therefore go through from the many drawbacks of text-based passwords.

Figure 4. Passfaces[7]

"Passface" is a scheme developed through using Real User Corporation [7]. The fundamental concept is as follows. The person will be asked to select 4 images of human faces from a face database as their futur e password. In the authentication stage, the person sees a grid of nine faces, consisting of one face until now chosen by way of the person and eight decoy faces (figure 4). The person recognizes and clicks anywhere on the recognized face. This process is repeated for numerous rounds. The user is authenticated if he/she effectively identifies the four faces. The approach is based on the assumption that humans can recall human faces less difficult than different pictures. User studies through Valentine have proven that Passfaces are very memorable over long intervals. Comparative studies carried out through Brostoff and Sasse showed that Passfaces had only a third of the login failure fee of text-based passwords, in spite of having about a third the frequency of use.

Their study also showed that the Passface-based log–in manner took longer than textual content passwords and therefore was once used much less often through users. However the effectiveness of this approach is nevertheless uncertain.

Davis, et al. [8] studied the graphical passwords created the usage of the Passface method and determined obvious patterns amongst these passwords. For example, most customers have a tendency to select faces of people from the same race. This makes the Passface password particularly predictable. This problem can also be alleviated by way of arbitrarily assigning faces to users, but doing so would make it challenging for human beings to remember the password.

Man, et al. [9] proposed some other shoulder -surfing resistant algorithm. In this algorithm, a person selects a range of pictures as pass-objects. Each pass-object has a number of variations and every variant is assigned a unique code. During authentication, the person is challenged with quite a few scenes. Each scene carries a number of pass-objects (each in the form of a randomly chosen variant) and many decoy-objects. The person has to kind in a string with the unique codes corresponding to the pass-object versions current in the scene as properly as a code indicating the relative place of the pass-objects in reference to a pair of eyes. The argument is that it is very difficult to crack this form of password even if the entire authentication method is recorded on video due to the fact where is no mouse click on to provide away the pass-object information. However, this technique still requires users to memorize the alphanumeric code for each pass-object variant.

Jansen et al. [10] proposed a graphical password method for mobile devices. During the enrollment stage, a person selects a theme (e.g. sea, cat, etc.) which consists of thumbnail pictures and then registers a sequence of picture as a

password (figure 5).During the authentication, the person should enter the registered images in the correct sequence. One disadvantage of this technique is that due to the fact that the quantity of thumbnail images is restricted to 30, the password space is small. Each thumbnail image is assigned a numerical value, and the sequence of choice will generate a numerical password. The end The result showed that the photo sequence size used to be typically shorter than the textural password length. To address this problem, two images can be mixed to compose a new alphabet element, as a result increasing the photo alphabet measurement.

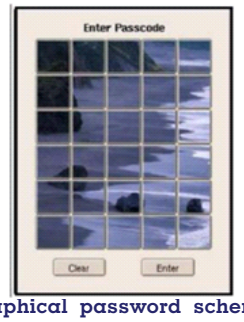

Figure 5. A graphical password scheme proposed by Jansen, et al. [10]

Takada and Koike mentioned a comparable graphical password method for mobile devices. This method allows users to use their preferred image for authentication [11]. The users first register their preferred pictures (pass-images) with the server. During authentication, a user has to go through various rounds of verification. At each round, the person both selects a pass-image among various decoy-images or chooses nothing if no pass-image is present. The program would authorize a user solely if all verifications are successful. Allowing users to register their very own images makes it less difficult for person to be aware their pass-images. A notification mechanism is also implemented to notify users when new pictures are registered in order to prevent unauthorized image registration. This technique does not always make it a more invulnerable authentication approach than text-based passwords. As shown in the studies through Davis, users' options of image passwords are often predictable. Allowing users to use their very own images would make the password even extra predictable, specially 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 Jermyn, et al. [12] proposed a technique, referred to as "Draw - a - secret (DAS)", which approves the user to draw their unique password (figure 6). A user is requested to draw a easy image on a 2D grid. The coordinates of the grids occupied by the photo are stored in the order of the drawing. During authentication, the user is requested to re-draw the picture. If the drawing touches the identical grids in the equal 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 textual content password space.

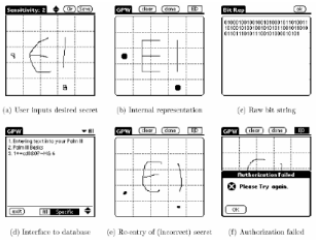

Figure 6. Draw-a-Secret (DAS) technique proposed by Jermyn, et al. [12]

Thorpe and van Oorschot [13] analyzed the memor capable password space of the graphical password scheme through Jermyn et al. [12]. They introduced the idea of graphical dictionaries and studied the possibility of a brute-force attack the usage of such dictionaries. They described a length parameter for the DAS kind graphical passwords and showed that DAS passwords of length eight or lar ger on a 5 x 5 grid may also be much less inclined to dictionary attack than textual passwords. They also showed that the space of replicate symmetric graphical passwords is substantially smaller than the full DAS password space. Since people recall symmetric pictures higher than asymmetric images, it is expected that a large fraction of users will choose replicate symmetric passwords. If so, then the protection of the DAS scheme may additionally be significantly decrease than initially believed. This problem can be resolved by means of using longer passwords. Thorpe and van Oorschot showed that the size of the space of reflect symmetric passwords of size about L + 5 exceeds that of the full password area for correspondin g length L < = 14 on a 5 x 5 grid.

Goldberg et al. [14] did a person study in which they used a method referred to as "Passdoodle". This is a graphical password comprised of handwritten designs or text, typically drawn with a stylus onto a touch sensitive screen. Their study concluded that users have been capable to remember entire doodle pictures as precisely as alphanumeric passwords. The person studies additionally showed that humans are much less probable to recall the order in which they drew a DAS password. However, because the user study was once done the usage of a paper prototype alternatively of computer programs, with verifications achieved by way of a human rather than computer, the accuracy of this study is nonetheless unsure.

Thorpe and van Oorschot [15] similarly studied the have an effect on of password length and stroke-count as a complexity property of the DAS scheme. Their find out about showed that stroke-count has the biggest have an effect on on the DAS password area -- The measurement of DAS password area decreases significantly with fewer strokes for a constant password length. The length of a DAS password also has a huge affect however the impact is not as sturdy as the stroke-count. To develop the security, Thorpe and van Oorschot anticipated a "Grid Selection" method. The decision grid is an in the beginning large, best grained grid from which the person selects a drawing grid, a rectangular region to zoom in on, in which they can also enter their password (figure 7). This would extensively expand the DAS password space.

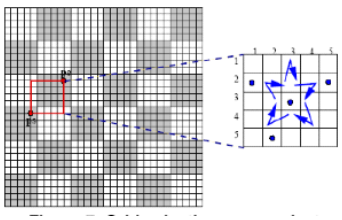

Figure 7. Grid selection: (Source: Thorpe and Van Oorschot [15])

Nali and Thorpe [16] conducted further evaluation of the "Draw-A-Secret (DAS)" scheme . two In their study, users have been asked to draw a DAS password on paper in order to decide if there are predictable characteristics in the graphical passwords that humans choose. The study did now not locate any predictability in the begin and give up factors for DAS password strokes, however located that sure symmetries (e.g. crosses and rectangles), letters, and numbers have been common. This study showed that users select graphical passwords with predictable characteristics, particularly these proposed as "memorable". If this learn about is indicative of

the population, the chance in which some of these charact eristics appear would decrease the entropy of the DAS password space. However, this person study only requested the users to draw a memorable password, but did no longer do any recall-test on whether or no longer the passwords have been surely memorable.

Figure 8. A signature is drawn by mouse. Syukri, et al. [18]

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 andSyukri, et al. [18] proposes a system where authentication is conducted by having the user drawing their signature the usage of a mouse (figure 8). Their approach protected 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 device will extract the signature area and both expand or scale-down the signature, and rotates if needed, (also acknowledged as normalizing). The records will later be saved into the database. The verification stage first takes the person input, and does the normalization again, and then extracts the parameters of the signature. After that, the system conducts verification using geometric common ability and a dynamic update of the database. According to the paper the charge of successful verification used to be satisfying. The biggest benefit of this approach is that there is no want to memorize one's signature and signatures are challenging to fake. However , no longer all people is familiar with using a mouse as a writing device; the signature can consequently be hard to draw. One possible solution to this problem would be to use a pen-like input device, but such devices are now not extensively used, and including new hardware to the current system can be expensive. We trust such a approach is more beneficial for small devices such as a PDA, which may additionally already have a stylus.

3.2.2 REPEAT A SEQUENCE OF ACTIONS

Blonder [19] designed a graphical password scheme in which a password is created by way of having the user click on on various places on an image. During authentication, the person need to click on on the approximate areas of those locations. The picture can help users to recall their passwords and consequently this approach is regarded greater convenient than unassisted recall (as with a text-based password).

Passlogix [20] has developed a graphical password device primarily based on this idea. In their implementation (figure 9), users have to click on a number of items in the picture in the right sequence in order to be authenticated. Invisible boundaries are described for each item in order to discover whether or not an item is clicked by using mouse. A similar technique has been developed through sfr . It used to be said that Microsoft had also developed a similar graphical pass word approach the place users are required to click on on pre-selected areas of an picture in a certain sequence. But important points of this method have not been available.

The "PassPoint" system by way of Wiedenbeck, et al. [35] extended Blonder's concept via removing the predefined boundaries and permitting arbitrary images to be used. As a result, a person can click on any area on an picture (as opposed to some pre-defined areas) to create a password. A tolerance round each chosen pixel is calculated. In order to be authenticated, the person need to click inside the tolerance of their chosen pixels and lso in the right sequence (figure 10). This method is based totally on the discretization method proposed by means of Birget, et al. Because any photo can be used and because a picture may additionally include hundreds to thousands of memorable points, the possible password space is quite large. Wiedenbeck, et al. conducted a person study , in which one team of participants had been requested to use alphanumerical password, while the different group used to be requested to use the graphical password. The end result showed that graphical password took fewer tries for the user than alphanumerical passwords. However, graphical password users had more difficulties learning the password, and took more time to enter their passwords than the alphanumerical users.

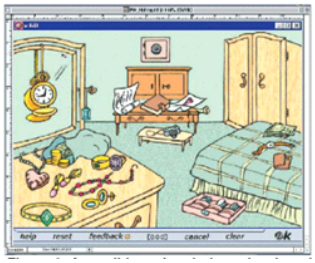

Figure 9. A recall-based technique developed by Passlogix [20]

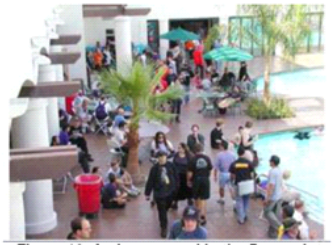

Figure 10. An image used in the Passpoint Sytem, Wiedenbeck, et al. [22]

Later Wiedenbeck, et al. [23] also carried out a user study to consider the impact of tolerance of clicking at some point of the re-authenticating stage, and the impact of photo desire in the system. two The result showed that reminiscence accuracy for the graphical password was once strongly decreased through using a smaller tolerance for the person clicked points, but the selections of pictures did not make a extensive difference. The result showed that the device works for a massive variety of images. two Passlogix has additionally developed numerous graphical password techniques primarily based on repeating a sequence of actions. For example, its v-Go includes a graphical password scheme the place users can combine up a digital cocktail and use the mixture of components as a password. . Other password alternative s consist of selecting a hand at cards or putting together a "meal" in the virtual kitchen. However, this technique only presents a constrained password space and there is no convenient way to prevent humans from choosing bad passwords (for example, a full residence in cards). Adrian Perrig used to be mentioned to be working on a system (called Map Authentication) that was once primarily based on navigating via a virtual world . In this system, users can construct their personal virtual world. The authentication is carried out by way of having user s navigate to a web site that is randomly chosen every time they log on. However, the details of this system are no longer available. Table 1

includes a more specific assessment of all the above techniques.

4. DISCUSSION

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

Very little research has been accomplished to learn about the issue of cracking graphical passwords. Because graphical passwords are not extensively used in practice, there is no report on actual cases of breaking graphical passwords. Here we quickly exam some of the feasible techniques for breaking graphical passwords and try to do a evaluation with text-based passwords.

BRUTE FORCE SEARCH
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 passw ords. For some recall based graphical passwords , 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 appears that graphical passwords are regularly predictable, a serious problem generally related with text-based passwords. For example, studies on the Passface approach have shown that people regularly select vulnerable an d predictable graphical passwords. Nali and Thorpe's learn about revealed comparable predictability among the graphical passwords created with the DAS method. More research efforts are wished to recognize the nature of graphical passwords created through real world users.

SPYWARE

Except for a few exceptions, key logging or key listening spyware can not be used to destroy graphical passwords. It is not clear whether or not "mouse tracking" spyware will be an tremendous device towards graphical passwords. However, mouse movement by myself is no longer sufficient to break graphical passwords. Such records have to be correlated with application information, such as window role and size, as properly as timing information.

SHOULDER SURFING

Like text based passwords, most of the graphical passwords are prone to shoulder surfing. At this point, only a few recognition-based techniques are calculated to resist shoulder-surfing. None of the recall-based based totally methods are viewed should-surfing resistant.

SOCIAL ENGINEERING

Comparing to text based password, it is less convenient for a person to provide away graphical passwords to any other person. For example, it is very hard to provide away graphical passwords over the phone. Setting up a phishing web page to achieve graphical passwords would be more time consuming. Overall, we consider it is extra hard to break graphical passwords using the normal attack methods like brute force search, dictionary attack, and spyware. There is a want for greater in-depth research that investigates feasible attack strategies towards graphical passwords.

5. CONCLUSION

The previous decade has viewed a growing pastime in the use of graphical passwords as an alternative to the common text-based passwords. In this paper, we have carried out a complete survey of present graphical password techniques. The present day graphical password techniques can be categorized into two categories: recognition-based and recall-based techniques.

Although the fundamental argument for graphical passwords is that people are better at memorizing graphical passwords than text-based passwords, the current user studies are very limited and there is no longer yet convincing evidence to guide this argument. Our preliminary evaluation suggests that it is extra challenging to break graphical passwords the use of the ordinary attack techniques such as brute force search, dictionary attack, or spyware. However, because there is not but vast deployment of graphical password systems, the vulnerabilities of graphical passwords are nevertheless not fully understood.

Overall, the contemporary graphical password techniques are still immature. Much more research and user research 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. S. Akula and V. Devisetty, "Ima ge Based Registration and Authentication System," in Proceedings of Midwest Instruction and Computing Symposium, 2004.
3. R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in Proceedings of 9th USENIX Security Symposium, 2000.
4. L. Sobrado and J.-C. Birget, "Graphical passwords," The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4, 2002.
5. 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.
6. 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.
7. RealUser, "www.realuser.com," last accessed in June 2005.
8. 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.
9. 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.
10. 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.
11. 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.
12. I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The Design and Analysis of Graphical
13. J. Thor pe 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.
14. 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.
15. 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.
16. 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.
17. 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.
18. 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.
19. G. E. Blonder, "Graphical passwords," in Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent, Ed. United States, 1996.
20. Passlogix, "www.passlogix.com," last accessed in June 2005.
21. 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.
22. 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.
23. S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Effect s of tolerance and image choice," in Symposium on Usable Privacy and Security (SOUPS). Carnegie-Mellon University, Pittsburgh, 2005.