International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 6, June - 2013

Implementation of Persuasive Cued Click-Points Techniques for Folder Security using Secure Hash Algorithm

Ms. Shilpa. L. Dhapade

[#]*GUIDE:Prof. Nilmani Verma, Department of Computer Science and Enginnering*
School of computer Engineering and IT, MATS University, Aarang, Raipur(C. G)

Abstract— **A typical computer user has passwords for many purposes: logging into accounts, retrieving e-mail, accessing applications, databases, networks, web sites, and even reading the morning newspaper online. Password provides security mechanism for authentication and services against unwanted access to resource. User often create memorable text password that are easy for attackers to guess, but strong–assigned password are difficult for user to remember. A graphical based password is one promising alternative of textual passwords. Cued click points is a click-based graphical password scheme, a cued-recall graphical password technique. This scheme use images instead of textual password as psychology studies have revealed that the human brain is better at recognizing and recalling images than text. In CCP users click on one point per image for a sequence of images. The next image is based on the previous click-point. User testing and analysis showed no evidence of patterns in ccp, so pattern-based attacks seem ineffective. Although result showed that Hotspots remain a problem. Hotspots[17]-[20] are areas of the images that have higher likelihood of being selected by user. By adding Persuasive feature to CCP, encourages users in selecting the password in random manner rather than using a particular sequence. This paper presents the design, implementation, and evaluation of a knowledgedge-based authentication mechanism that is of Persuasive cued click points (PCCP) password scheme with folder Cryptography. In this paper I have proposed a new hybrid graphical password based system, which is a combination of recognition and recall based techniques with the implementation of SHA(secure hash algorithm) Algorithm for encrypting the folder . It's tough to encrypt the folder. Now a day any hacker can decrypt the folder security, but the SHA algorithm provides more security to folder. It will work for any Operating System. An important goal of the PCCP is to provide support to user in selecting better password thus increasing security by expanding password space.**

Keywords— Graphical passwords, hotspots, persuasive technology, usable security, folder security.

1. INTRODUCTION

Computer systems and the information they store and process are valuable resources which need to be protected. Computer security system must also consider the human factor such as ease of a use and accessibility. Current secure systems suffer because they ignore the importance of human factors in security. An ideal security system considers security, reliability, usability, and human factor. The knowledge based authentication system includes the text password and graphical passwords. Typically text passwords are string of letters and digits, i.e. they are alphanumeric. Such passwords have the disadvantage of being hard to remember .Weak passwords are vulnerable to dictionary attacks and brute force attacks where as strong passwords are hard to remember.

A password authentication system should encourage strong passwords while maintaining memorability[9,11,12].In an attempt to create more memorable passwords, graphical password system have been devised. In these systems authentication is based on clicking on images rather than typing alphanumeric strings[5]. Graphical passwords techniques can be categories into Recognition Based Techniques and Recall Based Techniques, further this recall based techniques can be categories into pure recall based techniques and cued recall based techniques. In such systems user identify and target previously selected location within one or more images .The images act as memory cues to aid recall [13]. Example include PassPoints [10] and Cued Click Points[14]. HotSpots and Pattern Based attacks is effective in PassPoints[2,15,16,17] while Hotspots attack is effective in cued recall based techniques[3] .To overcome all these existing defects the PCCP technique came into existence. Result show that PCCP is effective at reducing hotspots and avoiding patterns formed by click-points within a password, while still maintaining usability and security issues[1].

The paper is prepared as follow. We discuss about the different passwords and graphical passwords, literature survey, persuasive click points, methodology , applications security and conclusion.

2. BACKGROUND

Passwords require the user to protect the user name and password from unauthorized use. The Taxonomy of Password Authentication Techniques is shown in the figure below.

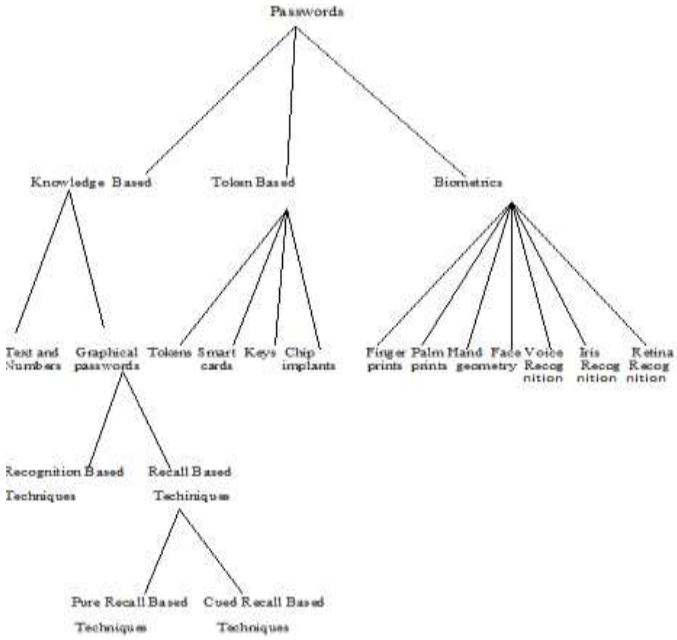


Fig. 1 A Taxonomy of Password Authentication Techniques

The text password and graphical passwords comes under the knowledge base authentication system. Text passwords are the most popular user authentication method that is mainly use by all users today, but it has some drawbacks related to security and usability. Alternative such as token based and biometric systems also have their own drawbacks[18, 19]. It leads to the need for another method, hence graphical password come into existence.

2.1Graphical password techniques

In general, the graphical password techniques [7] can be classified into two categories: recognition-based and recall-based graphical techniques

.

2.2.1Recognition Based System

Recognition-based systems use various types of images such as faces, random art, everyday objects, and icons. In recognition-based techniques, a user is presented with a set of images, images may and the user passes the authentication by recognizing and identifying the images he or she selected during the registration stage. There are many recognition based schemes. Some of them are is Pass Faces which was developed by Real User Corporation. Another recognition-based scheme is Pass-Objects which was developed by obrado and Birget [6]. Recognition-based graphical password technique is a stress-free technique as it is easy to remember, which increases the usability, but it is vulnerable to replay attack and mouse tracking because of the use of a fixed image as a password, so it is not completely secure.

2.2.2 Pure Recall-based Techniques

In this group, users need to reproduce their passwords without any help or reminder by the system. Draw-A-Secret technique [1], Grid selection [14], and Passdoodle[8] are common examples of pure recall-based techniques. Draw-A-Secret (DAS) [20] was the first recall-based graphical password system proposed. Users draw their password on a 2D grid using a stylus or mouse (see Figure 2).

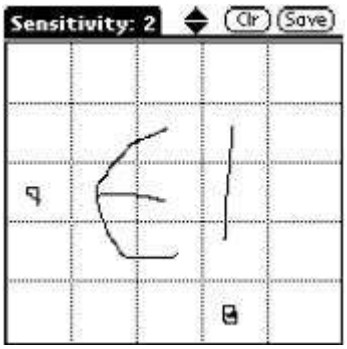


Fig. 2 Draw- A-Secret (20)

A drawing can consist of one continuous pen stroke or preferably several strokes separated by \pen-ups" that restart the next stroke in a different cell. To log in, users repeat the same path through the grid cells. The system encodes the user-drawn password as the sequence of coordinates of the grid cells passed through in the drawing, yielding an encoded DAS password. Its length is the number of coordinate pairs summing across all strokes.

In summary, DAS does offer a theoretical space comparable with text passwords, but the possibility that users will prefer predictable passwords such as symmetric passwords with few strokes [22] suggests that, as with text passwords, the effective space will be considerably smaller. Without an implementation and user studies, we can tell little more. Similarly, while a key motivation for DAS was the superior memorability associated with images, the lack of suitable user studies leaves as an open question how effectively this can be leveraged in graphical authentication [21].

2.2.3 Cued Recall-based Techniques

In this technique, the system provide some clue with the help of that users can which reproduce their passwords with high Correctness. There are many implementations, such as CCP and passpoint scheme. These clues will be presented as hot spots within an image. The user has to choose some of these regions on the image to register as their pass-word and they have to choose the same region on the image following the same sequence to login into the system. The user must remember the “chosen click spots” and keep them secret. This techniques are vulnerable to pattern attacks and hotspots.

Fig. 3 : On passpoint,a password consists of 5 ordered points on the image (the numbered labels do not appear in practice)

3. LITERATURE SURVEY

CCP was developed as an alternative click based graphical password scheme where users select one point per image for five images as shown inFig.4: The interface displays only one image at a time; the image is replaced by the next image as soon as a user selects a click point. The system determines the next image to display based on the user's click-point on the current image. The next image displayed to users is based on a deterministic function of the point which is currently selected. It now presents a one to-one cued recall scenario where each image triggers the user's memory of the one click-point on that image. Secondly, if a user enters an incorrect click-point during login, the next image displayed will also be incorrect. Legitimate users who see an unrecognized image know that they made an error with their previous click-point. Conversely, this implicit feedback is not helpful to an attacker who does not know the expected sequence of images.

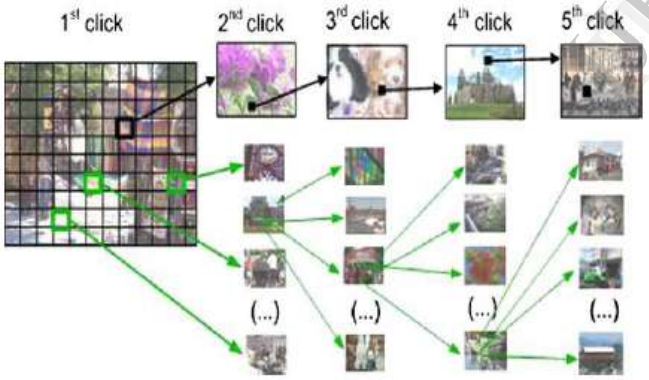


Fig. 4 With CCP, user select one click-point per image. The next image display is determined by the current click-point.

Various comprehensive investigations on the CCP graphical based authentication schemes have been accomplished and found that hotspots remain the problem. The hotspots are more vulnerable to dictionary attacks and reduce the effect of secure password system. Sonia Chiasson and Alain Forget in their paper showed the possibilities of prediction of password by using Cued Click points and Persuasive Cued Click points. The below graph shows such possibilities.

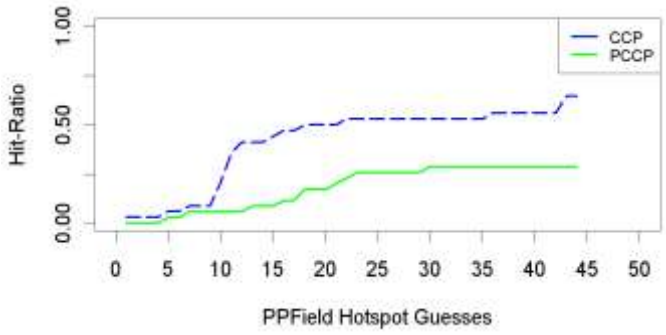


Fig. 5 PPField Hotspot Guesses

Sonia Chiasson , Alain Forget , Robert Biddle , P.C. van Oorschot have compares data from their three lab studies: PassPoints (PP), Cued Click-Points (CCP), and Persuasive Cued Click-Points (PCCP). Table 1 summarizes the number of participants, passwords, and individual click-points collected. More points per image were collected for PassPoints (PP). since each user's password gave 5 click-points on an image whereas for CCP and PCCP, there was only one click-point per image.

Study	Number of participants	Total number of click-points	Total number of passwords
Passpoint (PP)	43	2800	560
CCP	57	2520	504
PCCP	39	1500	300

Table 1: Number of participants, click-points, and passwords per lab study. Note that only passwords where users were successfully able to confirm and login are used in their analysis and included in this table.

4. PERSUASIVE CUED CLICK POINTS

As we have seen in literature survey that in PP, CCP there exist the guessing attack, capture attack, and hotspot problems which reduces the security of graphical password schemes and to overcome all above this paper proposed the design, implementation, and evaluation of knowledge-based authentication mechanism i.e., PCCP with folder Cryptography.

The persuasive technology was first proposed by Fogg as a technology to make the users to have a better authentication mechanism. Visual attention research [23] shows that different people are attracted to the same predictable areas on an image. This suggests that if users select their own click-based graphical passwords without guidance, hotspots will remain an issue. Davis et al. [24] suggest that user choice in all types of graphical passwords is inadvisable due to predictability. PCCP system could influence users to select more random

click-points while maintaining usability. Here the prediction of password is difficult for the attacker as password is generated in a random manner. The goal was to encourage users to behave more securely by using their own choice. In effect, behaving securely became the safe path-of-least-resistance.

Persuasive cued click points in which a password consists of five click-points, one on each of five images. During password creation, or during registration most of the image is dimmed except for a small view port area that is randomly positioned on the image as shown in figure. Users must select a click-point within the view port, and they cannot be able to click anywhere outside the viewport i.e.,outside the view port clicking action does not work. Viewport is nothing but a framed area. Within that random view port range there would be several tolerance squares per image or we can say tolerance area, tolerance area is nothing but the collection of all points closed to the clicked password point. If they are unable or unwilling to select a point in the current viewport, they may press the Shuffle button to randomly reposition the view port. The view port guides users to select more random passwords that are less likely to include hotspots. A user who is determined to reach a certain click-point may still shuffle until the viewport moves to the specific location.

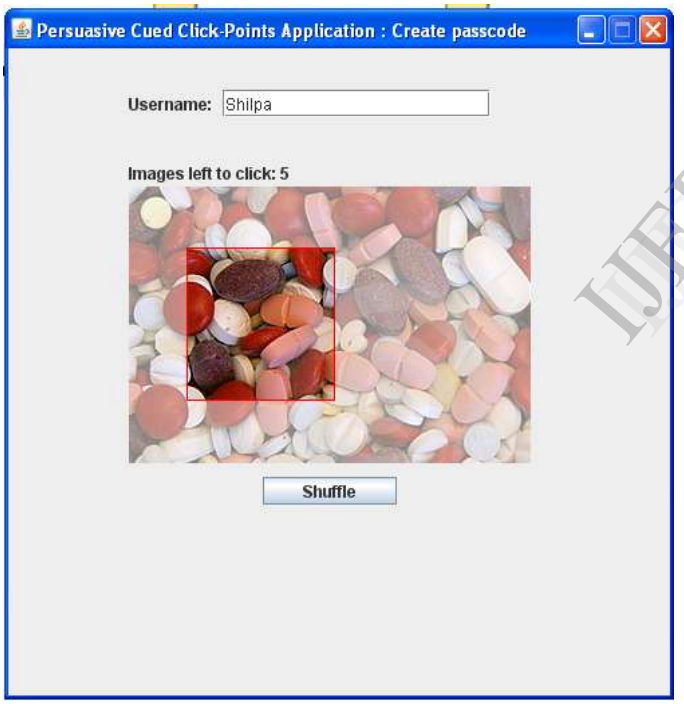


Fig.6 User interface for password creation

5. METHODOLOGY

This system uses the concept of PCCP which provides high security. It makes user to select password in a more secured way. For that the algorithm for password creation is in this manner:

1) To select or to create password user is presented with a single image and our application will choose and highlight a random view port (an area in the image) say of 2 x 2 inch for the user. Mind you random view port by our application.

2) Within that random view port range there would be several tolerance squares per image (say, 1 x 1 cm).Tolerance squares per image will be constant for the image.

3) When user selects a tolerance square, within the view port, out application will present the user with a new image based on the tolerance square selected.

4) In the new image user again performs step 1 to 3 above, until the user is presented with 5 such images.

5) When the user is done with selecting his choices, that information is mapped with the username and saved in a database.

To login for username they should use the correct sequence of click points. This system will be difficult for attackers where the sequence of image cannot be predicted easily. This method does not provide any alert messages, if the chosen image is wrong. It will be known to them only during the final click point. So the chance of guessing the sequence is very low.

Login for username process consist of following steps:

1. When the user attempts to login with his username, he will be presented with the same initial image but this time with NO view port and obviously with no shuffle button but only all the tolerance squares will be effective. So, total number click able areas per image = (w→h)/t^2, where t =1cm, in our case, which implies t^2=1x1cms, w = width and h = height of the whole image.

2. Now the user selects his choice in the first image and when he selects, our application will bring the next image related to that choice (tolerance square) and present to the user for next selection.

3. When the user finishes selecting that way in 5 sequential images, and the selections matches the user's stored information, the things would unlock.

The overall flow diagram for register process and Login is shown in figure below.

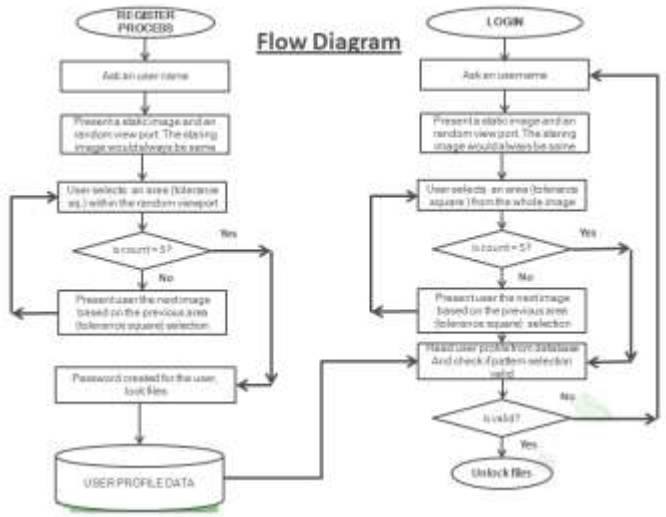


Fig. 7 Overall Flow Diagram for Register and Login Process

The modules used are described below. This is an example or the application for the persuasive click points concept.

6. PROCESS FOR FOLDER ENCRYPTION

Fig. 8 Overall process for folder encryption

The modules used are listed as follows:
1. Authentication
2. Graphical passwords
3. Image Based Registration and Authentication System (IBRAS):
4. Admin Process
5. Folder Encryption
6. Folder Decryption

7. APPLICATION

We can apply this method of authentication in the bank sector, for windows security etc. The increasing number of online services has raised another serious issue of number of web accounts a user has to maintain. As every website requires the user to register before accessing its resources, the user has to register with each website separately and maintain multiple login accounts. Remembering several password pairs are difficult for the users due to human memory limitations with alphanumeric passwords. Therefore, for easy recall of passwords, the users either set simple passwords (sometimes same) for all their accounts or set alphanumeric passwords and write it on piece of papers. But such practices suffer from various online attacks such as guessing, dictionary, phishing etc. and often lead to compromise of user's. This method of authentication is also applicable in network related application. This technique is highly suitable for places where high level security is required. This paper present the application of PCCP technique in our prototype model which is in folder form.

8. SECURITY

PCCP's fight against the standard security threats such as guessing attacks and capture attacks.

8.1 Guessing Attacks

The most basic guessing attack against PCCP is a brute force attack and dictionary attacks. Brute Force Attack: In this attack attacker tries to get every possible code, combination, or password by guessing until he get the correct one. This type of attack is a time consuming attack. A complex password can make the time for identifying the password by brute force long. Dictionary Attack: This also an another type of password guessing attack for identifying the user's password it make use of dictionary of common words

8.2 Capture Attacks

Password capture attacks occur when attackers directly obtain passwords by intercepting user entered data, or by tricking users into revealing their passwords. Shoulder surfing and malware falls under the category capture attack Shoulder surfing can be avoided to some extend by making some manipulation on user interface side such as reducing the size of the mouse cursor or dimming the image. Malware is an another capture attack more attention must be given to this attack as it is hazardous to both text and graphical passwords since key logger, mouse logger, and Screen scraper malware could send captured data remotely or otherwise make it available to an attacker. The attacker's has to work hard because PCCP is not vurnuable to hotspot attack; attacker must also determine Sequence of images for attack.

8.3 Hotspots

Hotspots are definite areas in the image that have a higher chance of being chosen by users as part of their passwords. If attacker is smart enough in guessing the hotspots in an image, then a dictionary of passwords containing combinations of these hotspots can be built. In PCCP Random view port is presented while password creation to force users not select any Hotspots (common predictable selections by user in an image).Random view port is a security enhancement that would guide the users in making things difficult for attackers who can exploits common predictable selection within an image. Hotspots are known to be problematic for PassPoints.

9. FOLDER SECURITY

Providing security to the folder is one of the most challenging job in the world of security system, so that unauthorized user unable to open the file without permission. Taking in action all these things, we can design a software model which provide image based authentication as well as encrypting folder using Secured Hash Algorithm.

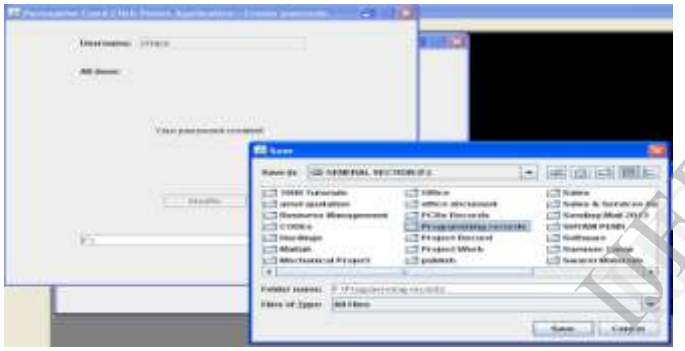
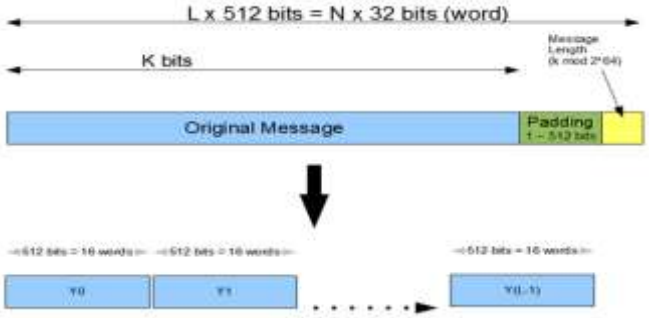


Fig: 9 Folder Encryption

9.1 Secure Hash Algorithm

SHA stands for "Secure Hashing Algorithm". It is a hashing algorithm designed by the United States National Security Agency and published by NIST. It is the improvement upon the original SHA0 and was first published in 1995. SHA1 is currently the most widely used SHA hash function, although it will soon be replaced by the newer and potentially more secure SHA2 family of hashing functions. It is currently used in a wide variety of applications, including TLS, SSL, SSH and PGP. SHA1 outputs a 160-bit digest of any sized file or input. In construction it is similar to the previous MD4 and MD5 hash functions, in fact sharing some of the initial hash values. It uses a
512 bit block size and has a maximum message size of 2 - 1 bits.



10. CONCLUSION

User authentication is a fundamental component in most computer security contexts. In this extended abstract, we proposed a simple graphical password authentication system which provides the more secure authentication than the text password scheme. We described the system operation with implementation of PCCP and trying to implement SHA Algorithm for folder security. A security goal in password-based authentication systems is to maximize the effective password space. We have shown that it is possible to allow user choice while still increasing the effective password space. Furthermore, tools such as PCCP's viewport (used during password creation) cannot be exploited during an attack. The approaches discussed in this paper present a middle ground between insecure but memorable user-chosen passwords and secure system generated random passwords that are difficult to remember.

ACKNOWLEDGMENT

I would like to express my gratitude and appreciation to all those who gave me the possibility to complete this paper. A special thanks to our final year project coordinator, whose help, stimulating suggestions and encouragement, helped me to coordinate my project especially in writing this paper.

REFERENCES

[1] Sonia Chiasson, Elizabeth Stobert, Alain Forget, Robert Biddle and P. C. Van Oorschot. Persuasive Cued Click-Points: Design ,implementation, and evauation of a knowledge-based authentication mechanism. In *IEEE Transactions on Dependable and Secure Computing (TDSC)*, Oct 2011.

[2] S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot. User interface design affects security: Patterns in click-based graphical passwords. International Journal of Information Security, Springer, 8(6):387-398, 2009.

[3] Sonia Chiasson , Alain Forget, Robert Biddle and P. C. Van Oorschot. Influencing user towards better password: Persuasive Cued Click-Points. I n Human Computer Interaction (HCI), The British Computer Society, September 2008.

[4] Zhi Li, Qibin Sun, Yong Lian, and D. D. Giusto, 'An association-based graphical password design resistant to shouldersurfing attack', International Conference on Multimedia and Expo (ICME), IEEE.2005.

[5] Susan Wiedenbeck Jim Waters, Jean-Carnille Birget, Alex Brodskiy Nasir Memon. SOUPS' 05, July 6-8, 2005, Pittsburg, PA, USA.

[6] P. C. van Oorschot, A. Salehi-Abari, and J. Thorpe. Purely automated attacks on passpoints-style graphical password. IEEEE Trans. Info. Forensics and security, vol. 5, no. 3, pp. 393-405, 2011

[7] Stobert, S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot. Exploring usability effects of increasing security in click-based graphical password. In Annual Computer Security Applications Conference (ACSAC), 2010.

[8] P. C. van Oorschot and j. thorepe. Exploting predictability in clicked-based graphical password, Journal of Computer Security, 2011..

[9] "Waziir Zada Khan, Mohammed Y Aalsalem and Yang Xiang. A Graphical Password Based System for Small Mobile Devices. International Journal of Computer Science Issue, Vol. 8, Issue 5, No 2, September 2011

[10] S. Wiedenbeck, J. Water, J. Birget, A. Brodskiy, and N. Memon, Passpoints: Desing and Longitudinal evaluation of a graphical password system. International Jounral of Human- Computer Studies, vol. 63, no. 1-2, pp. 102-127, 2005.

[11] Rachna Dhamija and Adrian Perrig, "Deja Vu: A User Study. Using Images for Authentication" In Proceedings of the 9th USENIX Security Symposium, August 2000.

[12] L.Sobrado and J.C. Birget, "Graphical Passwords", The Rutgers Schloar, An Electronic Bulletin for Undergraduate Research, vol 4, 2002.

[13] E. Tulving and Z. Pearlstone. Availablity Versus Accessibility of information in memory for words. Journal of Verbal Learning, Vol. 5, pp. 381-391, 1966.

[14] S.Chiasson, A. Forget, and R. Biddle. Graphical password authentication using cued click points. In European Symposium On Research in Computer Security (ESORICS), LNCS 4734, September 2007, pp. 359-374.

[15] A. Salehi-Abari, J. Thorpe, and P. van Oorschot. On purely automated attacks and click bassed graphical password . In Annual Computer Security Application conf.(ACSAC), 2008.

[16] A. Dirik, N. Menon, and J. Bireget. Modeling user choice in the passpoints graphical password scheme,. In 3rd ACM Symposium on Usable Privacy and Security (SOUPS), July 2007.

[17] J. Thorpe and P. C. van Oorschot. Human –seeded attacks and exploiting hot-spots in graphical passwords. In 16th USENIX Security Symposium, August 2007.

[18] L. Jones, A. Anton, and J. Earp. Towards understanding user perceptions of authentication technology. In ACM Workshop on Privacy in electronic Society,2007.

[19] A. Jain, A. Ross, and S. Pankanti. Biometrics: a tool for information security. Transaction on Information Forensics and Security (TIFS), vol. 1, no. 2, pp. 125-143, 2006.

[20] I. Jenmyn, A. Mayer, F. Monrose, M. reiter, and A. Rubin. The design and analysis of graphical passwords. In 8th USENIX security Symposium August 1999.

[21] Robbert Biddle, S. Chaisson, P. C. van Oorschot. Graphical Password: Learing from the first Twelve Years, School of Computer Science, Carleton University, Tech.Rep. TR-11-01,January4, 2011.

[22] P. C. van Oorschot and J. Thorpe. On predictive modles and user-drawn graphical password. In ACM Transaction on information and System Security, 10(4):1-33, 2008

[23] J. Wolf. Visual Attention . In K. De Valois, Ed. Academic Press, 2000, pp. 335-386.

[24] D. Davis, F. Monrose, and M. Reiter, "On user choice in graphical password schemes," in 13th USENIX Security Symposium, 2004