Usability and Security of Recognition based Graphical Password Scheme

Pranita Binnar
Dept. of Computer Engineering
Ramrao Adik Institute of Technology
Navi Mumbai, Maharashtra

Vanita Mane
Dept. of Computer Engineering
Ramrao Adik Institute of Technology
Navi Mumbai, Maharashtra

ABSTRACT
Authentication is the first line of defense against compromising confidentiality and integrity. People can remember pictures better and for longer periods than alphanumeric passwords. All graphical passwords have two different aspects which are usability and security. Woefully none of these schemes were being able to fulfill both of these aspects at the same time. We analyze the known attack method and categorize them into two kinds Attack by Password Space and Attack by Password Capture. In this paper we summarized the usability and security reported in some user's studies of recognition based graphical password schemes. Finally some suggestion were given

Keywords
Recognition Base Graphical Password scheme,Graphical Password Authentication,Usability,Security attack

1. INTRODUCTION
Traditionally the security of digital device has focused on low level, technical design and implementation details .Security experts often refer to humans as the "weakest link" in the security chain [1]. Security and usability are two opposite end of spectrum. When security of system is increases then their usability is decreases and usability features increases then there security decreases. An important goal of knowledge based authentication is to support users in selecting password of higher security with lager password space.

The base question is that weather the graphical password as secure as text base password? If we design the graphical password system properly then answer is yes. As knowledge base password system is less costly compare to others systems. The measure constitutes taken into consideration while designing system should be less vulnerable to attack [2].

The remaining of this paper organized as follows section II briefly reviews the authentication methods ,section III introduces literature survey and configuration survey of six current Recognition based graphical password(RBGP) schemes. Section IV usability features in RBGP, section V details with security attack type based on password space and password capture. Section VI is summarization of usability and security in RBGP schemes and in section VII finally conclusion and some suggestion are given.

2. RELATED WORK
A Password is a form of secret authentication data i.e. used to control access to a resource. User authentication is the process during which a (human) user proves they are who they claim to be. This is achieved by a distinctive characteristic. This characteristic can differentiate one individual from another. These characteristics can be called authentication factors and are said to fall into three categories: things you know (knowledge-based authentication, e.g. a password), things you have (token based authentication, e.g. a card or key), and things you are (physical biometrics e.g. finger prints, face or retina scans) [3].

Biometric authentication gives unique identity to user. Biometric authentication provides high security than the text based password but devices used for such authentication are very costly. Hence authentication process is complex and time consuming than other. Security and usability of token based authentication system is high. But main problem with this system is once the token is lost then the entire system security getting lost. Knowledge based authentication techniques helps to enhance real high security. This technique is having the greater password space so it is difficult to break password from specific security attack.

3. LITERATURE SURVEY
Graphical password authentication has two types Recognition based scheme and Recall based scheme. Recognition based schemes, also called Cognometric schemes, in this scheme user has to recognize pictures during login time from the given portfolio. In recall based graphical password authentication has two types of picture password techniques are there reproducing a drawing and repeating the selection [4].

The user has to verify knowledge of a secret he or she shares with the system. Contrary to the abstract nature of textual passwords, graphical authentication relies on visual memory and user has to access that secret in stored memory. Definition of Recognition base Graphical Password (RBGP) [5] is as follow:

- *Pass Image* – Select images from the set of images for authentication
- *Distracter* - An image shown on a challenge screen which is not a Pass Image for the user.
- *Challenge screen* - When a user authenticates, they are presented with multiple grids of images which includes a Pass Image and a number of distracter images. Each grid is called a challenge screen.
- *Challenge session* –This is the authentication session. This consists of a number of challenge screens i.e test screen from which the user must choose their Pass Image.
- *Pass Image set* - The set of images which comprise the user's selection of Pass Image.

Recognition Based Graphical password Schemes

Déjà vu [6] scheme has been introduced. It has to select and memorize a subset of "random art" images from a portfolio and the collection is generated using mathematical formula. While login into the system users has to recognize images from a set of decoys images. During authentication, select 5 images which belong to user's portfolio from a panel of 25 images. Images are abstract it is more difficult for users to write down their password or share it with others by describing their images. All the portfolio images are saving on trusted server

Pass Face Scheme [7] is the most extensively to date is than others. In this scheme user has to pre-select a set of human faces. During login, users must select the face belonging to their set from among decoys. Several such rounds are repeated with different panels. For successful login, each round must be executed correctly. The set of images in a panel remains constant between logins, but images are permuted within a panel, incurring some usability cost.

In 2004, the story scheme [8] proposed by categorizing the available picture to 9 categories. User has to select at least 5 pass images as passwords from the mixed pictures of 9 categories in order to make a story easily to remember.

Use Your Illusion [9] requires that users select portfolio images from panels of decoys. The idea is that the authenticate user can still recognize the images even the images are distorted, while the distortion creates difficulties for others to guess the password. This scheme is resistant to social engineering and shoulder-surfing attacks.

Weinshall [10] proposed the Cognitive Authentication scheme intended to be safe against spyware and shoulder-surfing. Keyboard input is used rather than a mouse and users must recognize images from their previously memorized portfolio.

In Convex hull Clicks scheme [11], users select and memorize a portfolio of images, and must recognize these images from among decoys displayed, over several rounds. The images are small icons and several dozen are randomly positioned on the screen. Each panel contains at least three of the user's icons. When the system uses five pass icons it is good resistant to shoulder surfing than three pass icons. This design is intended to protect against shoulder-surfing, but comes at a cost of longer login times.

Table I shows configuration survey of Recognition base graphical password scheme

Table 1. Configuration Survey

Schemes	**Pass images**	**Total no. of images**	**Image as assignment**	**Image Type**	**Order**
Déjà vu	5	25	Selected by user	Random art	No
Pass face	3	24	Assigned to user	Faces	No
Story	5	9	Selected by user	Photographs of objects	Yes
Use your illusion	3	24	Provided by user	Personal photographs obscured	No
Cognitive authentication	30	80	Provided by user	Random art	No
Convex hull clicks	5	100	Provided by user	Photographs of object	Yes

4. USABILITY FEATURES IN RBGP SCHEME

There is no universal protocol for designing usable system for graphical password system. If the product can be achieving objectives of user then the product is more qualitative [12].Objectives of user is effectiveness, efficiency and satisfaction. Human have greater ability to remember items if it seen before. This is an easier memory task than to recognize item than the recall. To achieve that, there are six main usability features have been identified. The features are memorability, efficiency, input reliability and accuracy, easy and fun to use, grid based and freedom of choice.

5. SECURITY ATTACKS IN RBGP SCHEME

Security attack in graphical password authentication techniques are categories into attack type by Guessability, Recordability and Observability are as follows.

5.1 Password Space

Password space is the number of choices from the portfolio available to users for selecting a password [13]. The important factor of secure password system is password space. There are two kinds of password space practical password space and theoretical password space (TPS).For each recognition based graphical scheme it is very difficult to analyses ideal formula, because practical password space differs from scheme to scheme. RBGP schemes usually include total no. of images with size *N* and *d* is the user's picture password. Password pictures can be in order or in disorder. The equation (1) and (2) are orderly and disorderly TPS.

The orderly TPS is:

$$\sum_{r=1}^{d} {}^{r}P_{n} = \sum_{r=1}^{d} N!/(N-R)! \qquad (1)$$

The disorderly TPS is:

$$\sum_{r=1}^{d} {}^{r}C_{n} = \sum_{r=1}^{d} N!/R(N-R)! \qquad (2)$$

5.1.1 Brute Force Attack

Brute force attack is orderly comprehensive key search technique. This attack searches all possible elements in the TPS until the correct one is found. When the theoretical password space is large then it is very hard to crack the password.

5.1.2 Dictionary Attack

Dictionary attack involves guessing passwords from an exhaustive list called a dictionary.

5.2 Password Capture

Common means of attack are Observability and Recordability [14][15]: social engineering and spyware attack, Shoulder surfing, intersection analysis.

5.2.1 Shoulder Surfing

Shoulder surfing refers to someone watching over a users shoulder when user enters password information into system. CHC is battle to shoulder surfing attack. Other schemes like Deja vu, Pass Faces and Story are falls under shoulder surfing attack because password images are directly display on challenge screen and it is observed by criminals.

5.2.2 Intersection Analysis

Criminals can use the intersection of two test sets to leak the password images. While login into the system ,the password images may be key to system or it may be decoy images that are part of test sets then intersection attack is more vulnerable to such scheme In Deja vu, all the password images are part of the challenge sets, and decoy icons are changed in each round.. Convex Hull Clicks and Pass Faces using multiple images choice as pass objects are also falls under such intersection attack.

5.2.3 Social Engineering

Orgill et al. social engineering attack techniques are Tricking, Phishing and Pharming. Graphical passwords are less susceptible to Tricking. For Deja vu and Use Your Illusion, the pictures are random art. It is very difficult to describe them verbally and record them. Convex Hull Click, there are many icons, icons are easy to describe with others .In story scheme pictures can be easily describe to others Remaining schemes which uses pictures such type of attack is more susceptible to social engineering.

5.2.4 Spyware attack

Spyware is a type of malware that secretly collects password information without knowing to use. The presence spyware, which includes some loggers and some scrapers whose click points or drawing style are fixed for every login, such recall based scheme are easy to crack by mouse –loggers contrary in RBGP schemes when click points and drawing style are not fixed, these schemes are hard to crack by mouse-loggers or key-loggers.

To protect user's information joint efforts should be taken from both perspective users and developers. From perspective they should use strong antivirus software from developers perspective password scheme must be more secure and reliable

6. COMPARATIVE ANALYSIS OF RBGP SCHEME

Summarizes Table II, the security of the 6 graphical password schemes we analyzed. X it is resistant to attack.√ the scheme is open to attack. In the Tricking, Phishing, 'Middle' denotes that difficulty has increased. 'Difficult' means the Tricking or Phishing is difficult. In the Spyware Attack column, 'Screen' means screen-scrapers can be used in the scheme. We have analyzed that some systems which require high security levels, it is appropriate to sacrifice some usability to ensure the absolute security. The security of the recognition based graphical password can be quantifiably measured in terms of resistance to observation and guessing attack.

Table 2. Security Of Rbgp

Scheme		Déjà vu	Pass face	Story	Use your illusion	Cogniti ve authent ication	Convex hull clicks
Password Space(bits)		16	13	12	11	73	32
Guessability	Bruit Force Attack	X	X	X	X	√	√
	Dictionary Attack	√	X	√	√	√	√
Observability	Shoulder Surfing	X	X	X	X	√	√
	Spyware Attack	Screen	Screen	Screen	Screen	√	√
Recordability	Intersection Attack	X	√	X	X	X	√
	Tricking	Difficult	Difficult	Difficult	Middle	Difficult	Difficult
	Phishing	Middle	Middle	Middle	Middle	Difficult	Difficult

Summarizes Table III the usability features of 6 recognition base graphical Password schemes we analyzed 'Y' means yes or available and 'N' means not or not applicable to specific schemes. So we have analyzed that user requirements with the special target environment For example portable devices, such as mobile phones, which generally do not contain confidential information, we may pay more attention to usability aspect.

Table 3. Usability Of Rbgp

Scheme			**Déjà vu**	**Pass face**	**Story**	**Use your illusion**	**Cognitive authentication**	**Convex hull clicks**
Usability	satisfaction	Mouse usage	Y	Y	N	Y	Y	Y
		Meaningful	N	N	N	Y	Y	N
		Keyboard usage	N	Y	Y	Y	N	Y
		Create simply	Y	Y	Y	Y	Y	Y
		memorability	N	Y	Y	Y	Y	Y
		Simple steps	Y	Y	Y	Y	Y	Y
		Training supply	Y	Y	Y	N	Y	N
		Assignable image	Y	Y	Y	Y	N	N
		Nice interface	N	Y	N	Y	Y	N
		Pleasant Picture	N	Y	N	Y	N	N
	Efficiency	Applicable	N	N	Y	Y	Y	N
	Effectiveness	R and D	N	Y	N	N	Y	Y

7. CONCLUSION

Human tends to remember graphics and image better than text and it is more difficult to break the graphical passwords from traditional attack methods: Brute Force Search, Dictionary Attack, or Spyware. Usability and security represents opposite ends of a spectrum. Therefore the tradeoffs require based on the User's requirement. The security of the RBGP can be quantifiably measure in terms of resistant to Guessing Attack and Observation attack.Feature scope is need to be implement Hybrid method using Recall Based Graphical Password and Recognition Based Graphical Password

8. REFERENCES

[1] A. Paivio. "Mind and Its Evolution",A Dual Coding Theoretical Approach. Lawrence Erlbaum: Mahwah, N.J.,2006.

[2] Renaud, K. Mayer, P. Volkamer, M. Maguire, J., "Are graphical authentication mechanisms as strong as passwords?," Computer Science and Information Systems (FedCSIS), 2013 Federated Conference on , vol., no., pp.837,844, 8-11 Sept. 2013

[3] Hafiz, M.D., Abdullah, A.H., Ithnin, N., Mammi, H.K., "Towards Identifying Usability and Security Features of Graphical Password in Knowledge Based Authentication Technique," Modeling and Simulation, 2008. AICMS 08. Second Asia International Conference on , vol., no., pp.396,403,13-15 May 2008

[4] Haichang Gao, Ning Liu, Kaisheng Li, Jinhua Qiu, "Usability and Security of the Recall-Based Graphical Password Schemes", High Performance Computing and Communications and 2013 IEEE International Conference on Embedded and Ubiquitous Computing (HPCC EUC), 2013 IEEE 10th International Conference on , vol., no., pp.2237,2244,13-15 Nov. 2013

[5] Yadav U. D, Mohod, P.S., "Adding persuasive features in graphical password to increase the capacity of KBAM," Emerging Trends in Computing, Communication and Nanotechnology (ICECCN), 2013 International Conference on , vol., no., pp.513,517, 25-26 March 2013

[6] R. Dhamija and A. Perrig. Deja Vu "A user study using images for authentication". In 9th USENIX Security Symposium, 2000

[7] Real user corporation,"the science behind passfaces," 2004[online].available: http://www.realuser.com

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

[9] E.Hayashi, N. Christin, R. Dhamija, and A. Perrig."Use Your Illusion:Secure authentication usable anywhere". In 4th ACM Symposium on Usable Privacy and Security (SOUPS), Pittsburgh, July 2008

[10] D. Weinshall. "Cognitive authentication schemes safe against spyware". In IEEE Symposium on Security and Privacy,May 2006.

[11] S. Wiedenbeck, J. Waters, L. Sobrado, and J. Birget.Design and evaluation of a shoulder surfing resistant graphical password scheme.In International Working Conference on Advanced Visual Interfaces (AVI), May 2006.

[12] Bevan, Nigel. "Quality in use: Meeting user needs for quality." Journal of Systems and Software 49.1 (1999): 89-96.

[13] Rasekgala, M., Ewert, S., Sanders, I., Fogwill, T., "Requirements for secure graphical password schemes," IST-Africa Conference Proceedings, 2014 , vol., no., pp.1,10, 7-9 May 2014

[14] G. Orgill, G. W. Romney and P. M. Orgill: "The Urgency for Effective User Privacy Education to Counter Social Engineering Attacks on Secure Computer Systems. In: Proceedings of the 5th Conference on Information Technology Education. pp. 177-181, 2004.

[15] R. Biddle, S. Chiasson, and P.C. van Oorschot. "Graphical passwords: Learning from the First Twelve Years. ACM Computing Surveys, 44(4), Article 19:1-41, 2011.