A Click Based Graphical Password Scheme Using Hard AI Problems

Pranita Haridas Mokal
Department of Information Technology,
Amrutvahini College of Engineering,
Sangamner, (M.S) India- 431005
pranitamokal62@gmail.com

Rohit N. Devikar
Department of Information Technology,
Amrutvahini College of Engineering,
Sangamner, (M.S) India- 431005
rohit.devikar89@gmail.com

***Abstract*- Many security primitives are based on difficult mathematical problems. Using hard AI problems for security is emerging as an new standard, but has been underexplored. As AI-complete problems cannot be solved by computer alone, but also require human computation, so that Captcha is used. In this paper, a new security primitive is proposed which is based on hard AI problems. In this paper, recognition based CaRP schemes are combined to develop a security primitive. The recognition based CaRP schemes are combined as input schemes. This primitive also combines Captcha. The input recognition schemes used are viz.ClickText scheme, ClickAnimal Scheme and AnimalGrid scheme. The proposed system is build on android platform. The proposed scheme is resistant to number of password attacks, such as online guessing attacks, relay attacks, and, if combined with dual-view technologies, shoulder-surfing attacks is resistant. In this paper, we are going to compare recognition based CaRP schemes. After implementing and combining these schemes we will conclude which scheme provides the mammoth degree of security.**

Keywords- component password,Graphical password, Reverse Turing Test,CaRP,Captcha, Security primitive.

I. INTRODUCTION

In the field of artificial intelligence, the most difficult problems are known as AI-complete or AI-hard[7], implying that the difficulty of these computational problems is similar to that of solving the central artificial intelligence problem— making computers as intelligent as people, or strong AI. To call a problem AI-complete reflects an attitude that it would not be solved by a simple specific algorithm. AI-complete problems cannot be solved with present computer technology alone, but would require human computation. This property can be useful, for instance to test the presence of humans with CAPTCHAs, and for computer security to circumvent brute-force attacks. An important task in security is to create cryptographic Primitives[14] based on hard mathematical problems that are computationally inflexible. The discrete logarithm problem is fundamental to the ElGamal encryption, the Diffie-Hellman key exchange[17], the Digital Signature Algorithm, the elliptic curve cryptography. Under this standard, the most prominent primal invented is Captcha, which distinguishes human users from computers by presenting a challenge, i.e. puzzle, beyond the capability of computers but easy for humans. Captcha is now a standard Internet security technique to protect online email and other services from being harmed by bots. But as compared to cryptographic primitives based on hard math problems, this primitive has a limited success.

In this paper, we proposed a new security primitive based on CaRP scheme *(Captcha as gRaphical Passwords)*. CaRP is click-based graphical password scheme in which a sequence of clicks on an image is used to obtain a password. In CaRP scheme, images used in are Captcha challenges, and a new CaRP image will be generated for every login attempt. The notions of CaRP is generic. In the proposed scheme, the recognition based CaRP schemes are used. The recognition based CaRP scheme are Clicktext scheme, ClickAnimal Schme, AnimalGrid Scheme. In the proposed system, these three schemes are used as input schemes for login.

The proposed scheme is resistant to online dictionary attacks on passwords, which provides a major security threat for various online services [13].

II. BACKGROUND AND RELATED WORK

a) Graphical Passwords

Graphical password was introduced by Greg E. Blunder in 1996. In this scenario, the users have to select some points on the image as their password. The order and the position of the chosen points would become the user's password. In order to get access to the system, the users have to select the same positions of the image in the correct order. Unfortunately, the requirement for the users to select the same and almost exact positions of the image in the correct order, raise difficulty for the users in entering their password. In addition, the display of the mouse cursor on the screen will make this scheme even easier to be cracked through shoulder surfing. Dhamija and Perrig proposing another kind of graphical password that they called Deja Vu. Instead of selecting several positions on the image, Dj vu displayed several random images that should be selected by the users as their password. Since the size of the images are much larger than the size of the correct position allowed in the Blunder scheme, Déjà vu clearly has eliminated the problem of mistakenly select the image position when entering the

password. The other good thing from Deja Vu is the usage of the abstract images provided to be selected as the user's password. Abstract images will make the password more secure than the ordinary image[4].

In ordinary image, unauthorized person can guess user's password based on the user's preference. In spite of its advantage, the usage of abstract images raises a new problem to the users. Instead of recognizing, abstract images will force users to recall their password. Therefore users can forget their password easier than the one proposed by Blunder. Since in Dj vu scheme, the users still have to direct the mouse pointer to the picture password, this scheme still easy to be cracked through shoulder surfing. Several Pictures Displayed in PassFace Scheme To overcome the problem of recalling the picture, Davis et al proposing a graphical password that he called PassFace[11]. Instead of selecting random images, Davis displays several images of human faces that should be selected by the users as their password. For this purpose, Davis provides several hundred images of human faces to be selected by the users. The advantage of this password scheme is the high ability of the users to recognize their password. This is due to the high ability of human to perform recognition instead of recalling. Unfortunately, this password scheme is still easy to be cracked through shoulder surfing. In addition the users tendency to choose faces that have the same ethnic or gender as they are, make the password even easier to be guessed based on the users identity or preference[5].

b) Captcha

A CAPTCHA is Completely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part. It is a challenge-response test. This test is used to determine whether the user is human or not. CAPTCHAs are used to prevent bots or automated programs from using various collecting sensitive information or using the services of any legitimate user. Applications of Captcha are registering for any email accounts and collecting email addresses.

Captcha presents a certain challenge to show the capabilities difference between humans and bots in solving various hard AI problems. visual Captchas are of two types viz. text Captcha and Image-Recognition Captcha (IRC). The earlier type of Captchas relies on character recognition and the latter relies on non-character objects recognition .Security primitives of text Captchas has been comprehensively studied. The principle following established for text Captcha is it should rely on the complexity of character segmentation and it is computationally expensive. It is combinatorial hard[6].

III. LITERATURE SURVEY

A. R. Biddle, S. Chiasson and P. C. Van Oorchot Scheme

a) Recall Based Systems:

In Recall based system, the user recalls the password and reproducing the secret drawing.So that it is also called as draw metric systems. In recall based systems, the user enter their password either on a blank canvas or on a grid. In this scystem, there are no memory prompts or cues .Hence the Recall is a difficult in order to retrive the password. But users are considering the interface as a cue.This interface cue is the same cue which is available for user and attacker also.Textual passwords are also consider as using recall. In case of textual passwords the name of the system is used as the memory cue by the user and user includes this in his/her password. In case of graphical password, there is not such use of system as memory cue. There is possibility of using such cue in graphical password is relating a recall based password to user account name. There are amount of security vulnerabilities are general to nearly all recall-based systems because the features of these systems are similar [1].

b) Recognition-Based Systems

In recognition-based systems, different types of faces, images, random art, different objects, and icons are used. The cues for images are somewhat similar in each login attempt. In this system, only some part of the user's secret is exposed in any one login attempt. Hence there is need of various server probes. The phishing site which relays information between the legitimate site and the user in real time alternatively uses a man-in-the-middle (MITM) attack. In this, the user enters the username and passes this to the genuine site then retrieves the panel of images. These panels of images are displayed to the user on phishing site alone. In this way the attacker the gain access to the user's account [1].

B. Pinkas and T. Sander scheme

In Pinkas and T. Sander scheme, the RTTs (Reverse Turing Tests) are combined with any password based authentication system of user. In this scheme, before entering the username and password ,the user first needed to pass the Reverse Turing test .As each login attempt need to pass the RTT, the number of guessing attempt for access to account are prevented. In general any authentication, the login attempts are N so that in case of this PS scheme the number of test pass are also N. This means the an adversary should perform all the N tests or pass RTTs in order to gain access to the user account. Hence the speed of an attacker automatically slows down or an attacker has to appoint the RTT solver. Hence this scheme reduces the dictionary attack[2].

IV. EXISTING SYSTEM

A. CaRP Scheme

In CaRP scheme, there is authentication server which stores the salt value as s and hash value of password and salt as *H(ρ, s)*. p is the password of an user account. At the first step, authentication generates the CaRP images.AS also stores the image object location. In other words, AS stores the co-ordinates of clickable points. Then AS sends these images to the user to click their password on an images. When user clicks on an image i.e. clicked points, these clicked points are recorded as co-ordinates .These clicked points are the password for user account. After this the AS retrieves the stored salt value sand again calculate the hash value of clicked point p' and salt value s. Then compare both hash values i.e. compares *H(ρ, s) and H(ρ', s)*.If both calculates are same then authentication is successful otherwise access id denied to user.

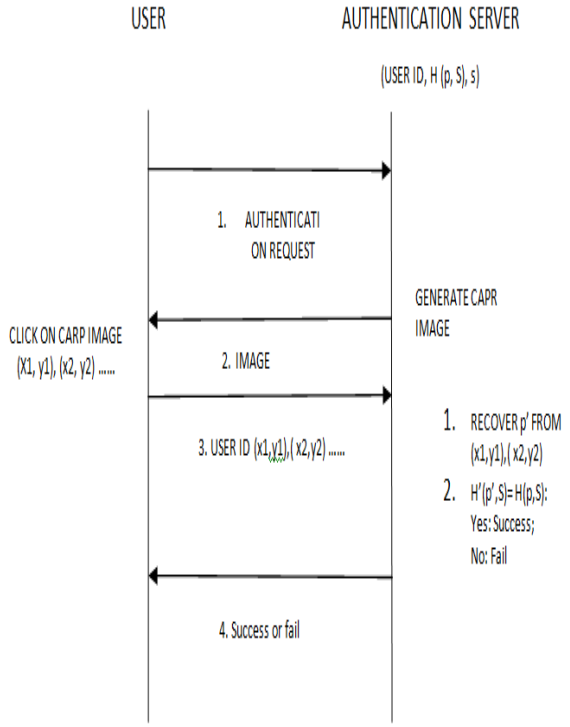

Figure 1. CaRP Scheme.

B. *ClickText Scheme*

It is a type of recognition-based CaRP scheme. *ClickText* Scheme is based on text Captcha. It consist of simple character which are not visually confusing to users such as difference between , Letter "O" and digit "0".These visually confusing characters are not included in character set. The password in *ClickText* is sequence of characters. For example:"PQ7#96". The password in *ClickText* scheme is similar to textual password. Captcha engine is used to generate the ClickText image. In ClickText image generation, lacation of every character are recorded which is used to find the ground truth value. During authentication phase, all the characters are arranged at random on 2D space. In every login attempt positions of characters are different and user has to select the appropriate sequence of characters as password.

C. *ClickAnimal Scheme*

ClickAnimal is build on Captcha Zoo. In this scheme, the sequence of animals is a password. The 3D models of sequence of animals are built. The Captcha engine is used to generate the ClickAnimal images. In order to generate the 2D models from 3D models of an animal's different views, positions, colors etc. are applied. The 2D animals are then arranged on the cluttered background like grass. Some animals can be occluded by another but condition is that the core portion should not be occluded. The user has to identify their password as sequence of animals from animals arranged on that cluttered background.

D. *AnimalGrid Scheme*

It builds on the ClickAnimal scheme .In this scheme ClickAnimal scheme is combined with Grid. . Animal Grid combines ClickAnimal and Click A Secret scheme (CAS). In CAS, user has to click on the grid as a password.CAS is not object dependent. During entering of password, first ClickAnimal image is displayed. After animal as a password is selected, the n*n grid for the corresponding animal is generated. When user clicks on the animal, then the clicked points are recorded as co-ordinates. Using these co-ordinates, bounding rectangle is obtained. Using ground truth value, the server again covers the animals from received sequence of animals. Then regenerate the grid image from bounding rectangle. Then recovers the password from those images. Then calculates the hash and compared with stored hash.

V. PROPOSED SYSTEM

The proposed scheme is android based scheme. The proposed scheme is used to reduce on-line guessing attacks, shoulder-surfing attacks and it will improve the security of existing Applications. In the proposed scheme user has to first select the password scheme and then select the password for selected scheme. This password is stored at server side. Server stores user's details in registration phase. The email-id of user is stored during registration phase. In authentication phase, user requests are received at server side. At server side the password schemes (i.e.ClickText, Click Animal and AnimalGrid) are fetched. Then captcha generation algorithm and IP algorithms are used to regenerate image. After this Hash is generated using Secure Hash algorithm(SHA).Then performing visual cryptography and generate shares on captcha image. The share1 is send via email and share2 is send via network. At user side ,when both shares are received then perform decryptography and regenerate captcha image. After this user has to enter password. if password is correct then authentication is successful otherwise failed.

VI. SYSTEM ARCHITECTURE

.

In the proposed system, there are two phases viz.

1) Registration Phase
2) Authentication Phase

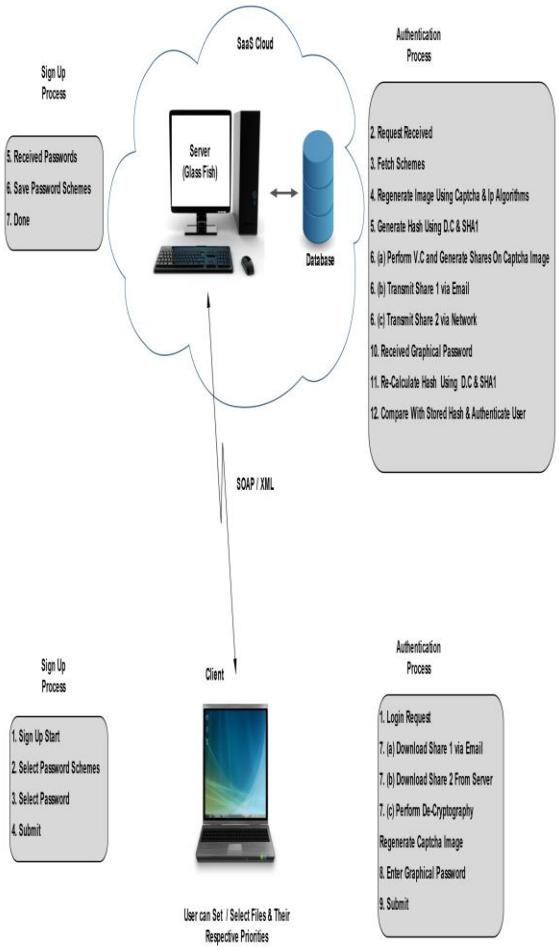

Figure 2. Architecture of Proposed System.

1) Registration Phase:

In this phase, user has to enter the details like username, date of birth, email-id etc. Then user has to select the password schemes like Click text, Click-Animal and Animal-Grid.

After selecting the password scheme, user has to Select the password for his/her account. This information is stored at server side during registration phase.

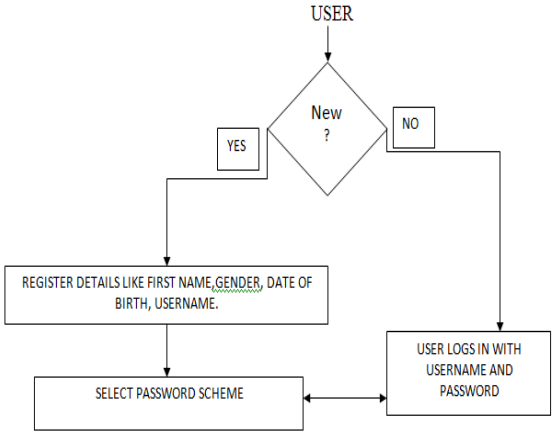

Figure 3. Registration Phase

2) Authentication Phase:

In this phase, the user has to sends the login request to server. At server side user request is received. After that the scheme for that user account is fetched in order to process the user request. Then at server side images are regenerated according to schemes for user account using captcha and image processing algorithms. After that hash value is generated using discrete centralization (DC) and secure hash algorithm (SHA-1).Then perform visual cryptography and generate shares on Captcha image. The transmit share-1 via email and transmit share-1 via email.
Then at client side, download share-1 via email and share-2 via network. Then perform De-cryptography and regenerate the captcha image. Enter graphical password.
At server side, the password is received. Then recalculate the hash value and compared it with the stored hash. If hash value matches provide access to user.

VII. RESULTS

Data Set Name	Actual Objects	Retrieved Objects	Correct Retrieved Objects
Class 1	**20**	**18**	**17**
Class 2	**25**	**24**	**23**

Confusion matrix			
		Class 1	Class 2
	Class 1	17	1
	Class 2	1	21

Precision Class 1	(Relevant Intersect Retrieved) / Retrieved	Correct Retrieved Object / Retrieved Objects	0.944444444
Precision Class 2	(Relevant Intersect Retrieved) / Retrieved	Correct Retrieved Object / Retrieved Objects	0.958333333

Recall Class 1	(Relevant Intersect Retrieved) / Relevant	Correct Retrieved Object / Actual Objects	0.85
Recall Class 2	(Relevant Intersect Retrieved) / Relevant	Correct Retrieved Object / Actual Objects	0.92

	Precision	Recall
Class 1	0.944444444	0.85
Class 2	0.958333333	0.92
Total	0.951388889	0.885

Accuracy Percentage	0.885

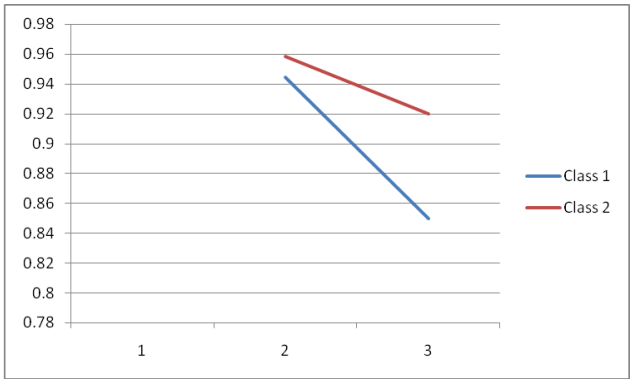

Figure 4. Graph Of Approximate Results

VIII. MATHEMATICAL MODEL

Let s (be a main set of) ≡ {SDB, LDB, C, A, S, MR, AO}

Where,

SDB is the copy of the server database. This database is responsible for storing user information related to cloud interactions. (Elaborate..)

LDB is a set of local database that a user owns. It consists of data tables having data items related to the products and their sales transactions.

C is a set of all clients using the server database and mining services from the server. And (c_1 , c_2 , c_3, ...c_n) Є C. (elaborate..)

A is a set of algorithms applied on the input data to get mining results.

S is the server component of the system. The server is responsible for registering, authenticating and providing associations to the end user. (Elaborate..)

MR is a set of mining rules that are applied on the input dataset provided by the client from his LDB. And (mr_1 , mr_2 , mr_3, ...mr_n) Є MR

AO is a set of associations that are extracted from the input and a form the output of the system.

Functionalities :

SDB' = RegisterUser(uid, password, fullname, address, country, contact, email);
password = SHA1(input_password);
U = AuthenticateUser(uid, password, SDB');
LDB1 = ManageProducts(pid, product name, cost);
LDB2 = ManageBilling(transactions, items);
LDB = LDB1 + LDB2
ED(Encoded data) = EncodeTransactions(LDB2, EncodingAlgorithm(EA));
UPLOAD(ED);
AO = Apply Mining(ED);
Results = Decode(Download(AO));

CONCLUSION

In this paper we have combined ClickText, ClickAnimal and AnimalGrid three recognition based CaRP schemes. All the recognition based CaRP schemes are combined as the input schemes for login and user has to select that schemes first. These schemes are developed on android platform. After implementing and combining these schemes we will conclude which scheme provides the mammoth degree of security. If we combined this scheme with dual view technology then it can be used to resist the shoulder surfing attack also.

ACKNOWLEDGMENT

The satisfaction that accompanies the successful completion of any task would be incomplete without mentioning the people who made it possible. I am grateful to a number of individuals whose professional guidance along with encouragement have made it very pleasant endeavor to undertake this seminar.

I have a great pleasure in presenting the seminar on " A Click Based Graphical Password Scheme Using Hard AI Problems "under the guidance of Prof.R.N. Devikar.

I am truly indebted and grateful to Head of Department Prof. S. E. Pawar and Prof.B. S. Borkar for their valuable guidance and encouragement.

I take an opportunity to thank all the staff members of our department. Finally I express my sincere thanks to all those who helped me directly or indirectly in many ways in completion of this project work.

REFERENCES

[1] R. Biddle, S. Chiasson, and P. C. van Oorschot, "Graphical passwords: Learning from the first twelve years," *ACM Comput. Surveys*, vol. 44,pp. 22-30.

[2] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords," in *Proc. 8th USENIX Security Symp.*, 1999, pp. 1–15.

[3] H. Tao and C. Adams, "Pass-Go: A proposal to improve the usability of graphical passwords," *Int. J. Netw. Security*, vol. 7, no. 2, 2008, pp. 273–292.

[4] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system," *Int. J. HCI*, vol. 63, Jul. 2005, pp. 102–127.

[5] P. C. van Oorschot and J. Thorpe, "On predictive models and userdrawn graphical passwords," *ACM Trans. Inf. Syst. Security*, vol. 10, no. 4, 2008 pp. 1–33,.

[6] L. von Ahn, M. Blum, N. J. Hopper, and J. Langford, "CAPTCHA: Using hard AI problems for security," in *Proc. Eurocrypt*, 2003, pp. 294–311.

[7] K. Golofit, "Click passwords under investigation," in *Proc. ESORICS*, 2007, pp. 343–358.

[8] A. E. Dirik, N. Memon, and J.-C. Birget, "Modeling user choice in the passpoints graphical password scheme," in *Proc. Symp. Usable Privacy Security*, 2007, pp. 20–28.

[9] J. Thorpe and P. C. van Oorschot, "Human-seeded attacks and exploiting hot spots in graphical passwords," in *Proc. USENIX Security*, 2007, pp. 103–118.

[10] P. C. van Oorschot, A. Salehi-Abari, and J. Thorpe, "Purely automated attacks on passpoints-style graphical passwords," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 3, Sep. 2010, pp. 393–405.

[11] P. C. van Oorschot and J. Thorpe, "Exploiting predictability in clickbased graphical passwords," *J. Comput. Security*, vol. 19, no. 4, 2011, pp. 669–702.

[12] P. C. van Oorschot and S. Stubblebine, "On countering online dictionary attacks with login histories and humans-in-the-loop," *ACM Trans. Inf. Syst. Security*, vol. 9, no. 3, 2006, pp. 235–258.

[13] M. Alsaleh, M. Mannan, and P. C. van Oorschot, "Revisiting defenses against large-scale online password guessing attacks," *IEEE Trans. Dependable Secure Comput.*, vol. 9, no. 1, Jan./Feb. 2012, pp. 128–141.

[14] L. von Ahn, M. Blum, N. J. Hopper, and J. Langford, "CAPTCHA: Using hard AI problems for security," in *Proc. Eurocrypt*, 2003, pp. 294–311.

[15] S. Chiasson, P. C. van Oorschot, and R. Biddle, "Graphical password authentication using cued click points," in *Proc. ESORICS*, 2007, pp. 359–374.

[16] S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot, "Influencing users towards better passwords: Persuasive cued click-points," in *Proc. Brit. HCI Group Annu. Conf. People Comput., Culture, Creativity, Interaction*, vol. 1. 2008, pp. 121–130.