International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

A Three Level Graphical Password Scheme for Providing High Degree of Security

Pranita H. Mokal[1], R. N. Denikar[2]

[1]Pune University, Amrutvahini College of Engineering, Sangamner-422605

[2]Professor, Pune University, Amrutvahini College of Engineering, Sangamner-422605

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 are resistant. In this paper, a new password scheme is developed to provide more security. This scheme combines recognition based schemes. In this scheme three levels of security is provided.***

Keywords: *Graphical password, Reverse Turing Test, CaRP, Captcha, Security primitive*.

1. 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.

In this paper, we broadly examine and discuss the graphical password using CAPTCHA and AI hard problems. CAPTCHA is short form of Completely Automated Public Turing test to tell Computers and Humans Apart) [1][2][3], It is also recognized as Human Interactive Proof (HIP). CAPTCHA is an automated Turing test in which not only generation of challenges but also grading of responses are performed by computer programs. CAPTCHAs are based on Artificial Intelligence (AI) problems. Artificial Intelligence (AI) problems are the problems that are easily solved by humans but cannot be solved by current computer programs or bots.

2. Literature Survey

1. In this paper, numerous graphical password schemes from 1996 are studied. The present graphical password schemes are categorize into four categories: Recognition based schemes, Recall based schemes, and Hybrid schemes. This paper provides a complete security overview of available research of existing graphical password schemes. Password attacks are classified based on password space and capture based. This paper focused on the brute force attacks and dictionary attacks. Preliminary analysis is done along with password attacks. In this paper various recognition based password scheme such as Déjà vu, Jensen et al., Passfaces , Story are studied , in recall based scheme Hong et al, Blonder, DAS are studied and in hybrid scheme Jiminy, GrIDsure,ac etc schemes are studied.

2. CaRP Scheme: In CaRP, for every login trial a new image is presented. Alphanumerical characters are used in this scheme in order to generate a CaRP image. This CaRP image is a Captcha challenge. In CaRP Scheme secure channel I used between clients and the authentication server through Transport Layer Security (TLS). The authentication server stores a salt value *s* and a hash value $H(\rho, s)$ for every user ID, ρ is the password of the user and h is the hash value. During authentication phase, *authentication* server produce a CaRP image then records the locations of the objects in the image and finally sends the image to the user to click his password. The coordinates of the clicked points are also recorded and drive to *AS*. *AS* maps the received coordinates against the CaRP image, as well as pull throughs a series of clickable points of visual objects, ρ', that the new clicked points by user on the image. Then authentication server take backs salt *s* of the user account, again calculates the hash value of ρ' with the salt. Then compares the it *with* the hash value stored for that user account. If the two hash values are equivalent then authentication succeeds.

3. Proposed Scheme

The proposed scheme is click based graphical password scheme using AI hard problem. In this scheme, we combine recognition based graphical password schemes such as clicktext, clickAnimal and AnimalGrid schemes. We provide three levels of security. An objective of our system is as follows: 1) This new scheme should be combination of different recognition based schemes, biometrics scheme, and token-based authentication schemes. 2) This scheme should provide passwords that are easy to remember and difficult for attacker to presume. 3) This scheme should provide the user easy password reset method.4) It should easy for use in case of novice user also. In this system for providing more security discrete centralization and SHA-1 algorithm is used.

For accessing the system the user must followed the following steps.

1) Registration
2) Login.

Registration Phase

While constructing the three dimensional password first the user registers himself by filling all fields, the registration form is consist of different field they are, full name field contain of name of user who wish to register, full address of user can put in address field. State of user in state field, city fields contain the city of user, telephone number fields store the personal telephone number of user, mobile number, Email id provided in to Email field, user name contain in user fields, and password is selected in password.

After filling all fields in registration form the different environment are available so that user can select any environments. Now user can select any environment which will be part of his three dimensional password. Here three different environment available users may select any one.

Figure 1: Registration Phase GUI

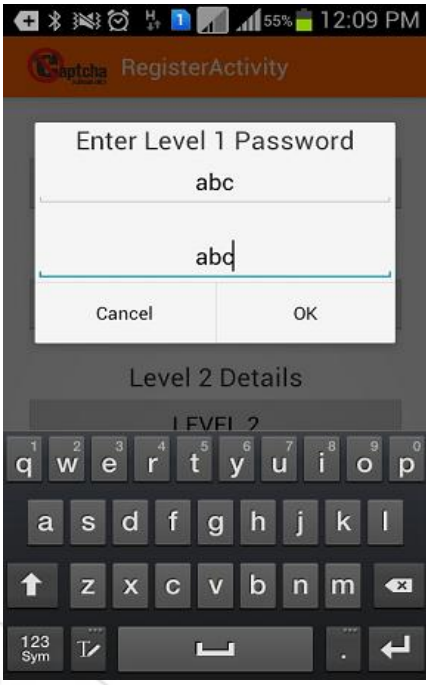


Figure 2: Enter Level1 password

Figure 3: Enter Level2 password

- In figure 4, user selects the first image as a level password and then enters the alphanumeric password

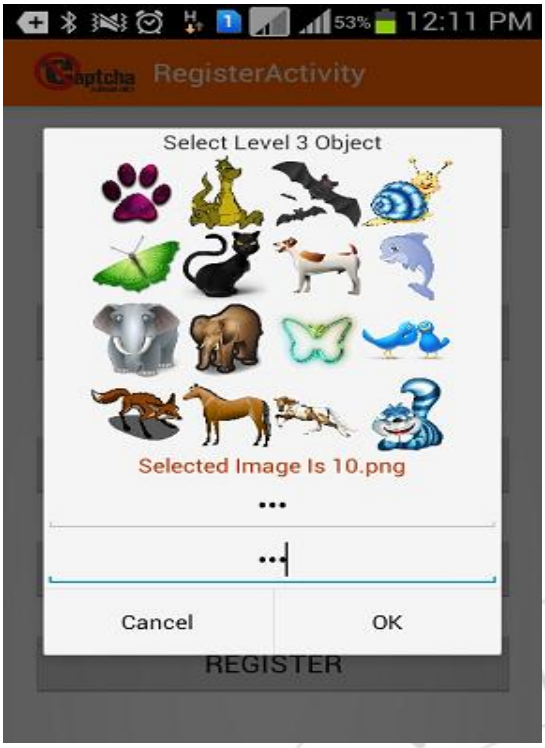


Figure 4: Enter Level3 password

Authentication Phase

In click based graphical password scheme, the server is developed in Netbeans and the client is developed in eclipse. First server should be deployed then only client process starts. When server is deployed then along with captcha server both Glassfish server and database process runs. server In client module we designed the graphical user interface for user. In this module, first the connection of wifi network is tracked first and connect to those network only which network the server module using. Each time client should enter the IP address of network which both client and server module is using. After connection is established server send Hello message to client. In authentication phase, user has to first enter the level 1 password as clicktext scheme password. When user enters the level 1 password then system displays level 2 password as Click Animal password scheme and after entering level 2 password , level 3 password should entered by user. When all password levels are cleared by user then system provides access for upload- download.

Figure 5: Authentication Phase GUI

Figure 6: Enter Level2 password

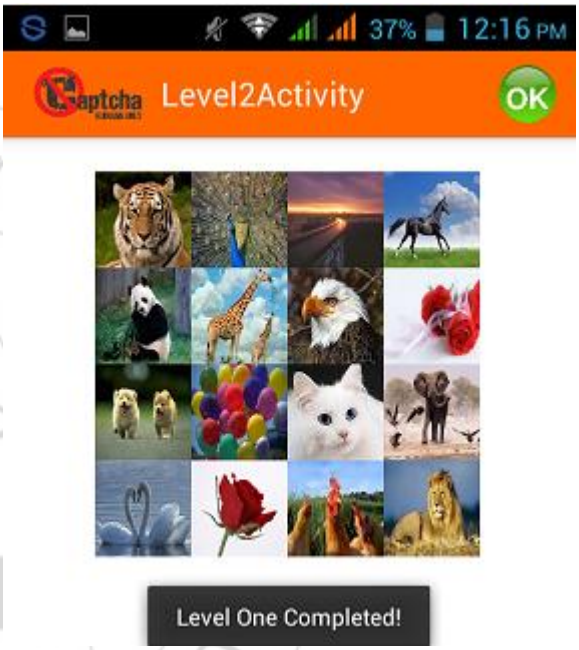


Figure 7: Enter Level2 password

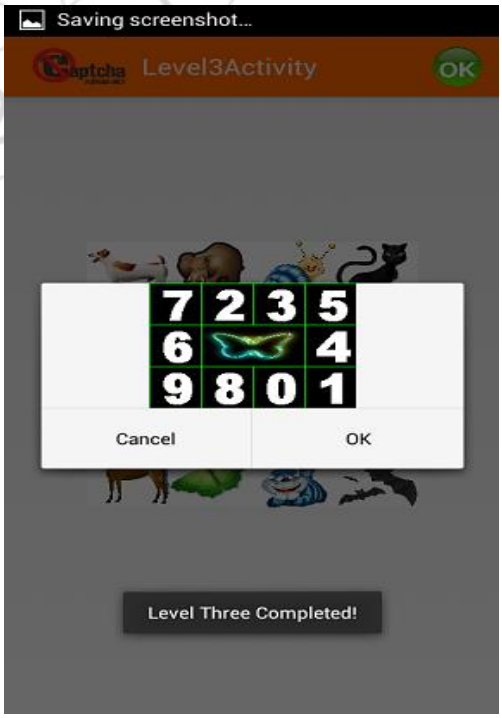


Figure 8: Enter Level3 password

Figure 9: File Upload Download Window Displayed

Figure 10: File Uploading

Figure 11: File Downloading

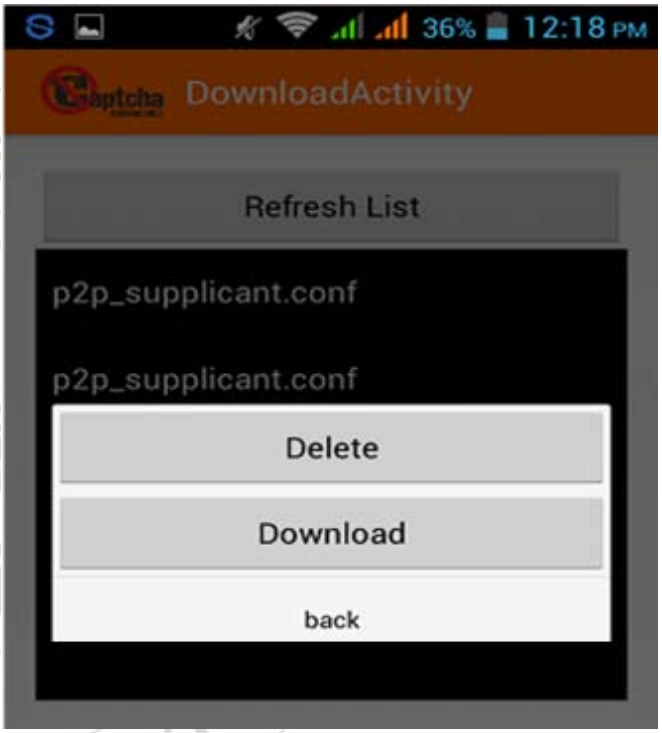


Figure 12: File Downloading Options Displayed

Figure 13: File Downloaded successfully

3.1 System Requirements

- **Hardware Requirements**

1. RAM: 512 MB.
2. PROCESSOR: PENTIUM-4 and Above.

- **Software Requirements**

1) OPERATING SYSTEM: WINDOWS XP
2) PROGRAMMING LANGUAGE: JDK 1.6,
3) Eclipse SDK
4) DATABASE: MySQL Server

3.2 Application

1. Critical Servers.
2. Nuclear & Military Facilities.
3. Airplanes & Jet Fighters etc.
4. ATMs.
5. Desktop computers & laptops.

4. Result Analysis

Results are analysed based on the concept precision and recall.

Table 1: Results based on precision and Recall 1

DataSet Name	Actual	Total	Correct
Legitimate User	20	18	7
Non-Legitimate User.	20	18	7

Table 2: Confusion Matrix

Confusion Matrix	*Legitimate User*	*Non-Legitimate User*
Legitimate User	17	7
Non-Legitimate User.	1	16

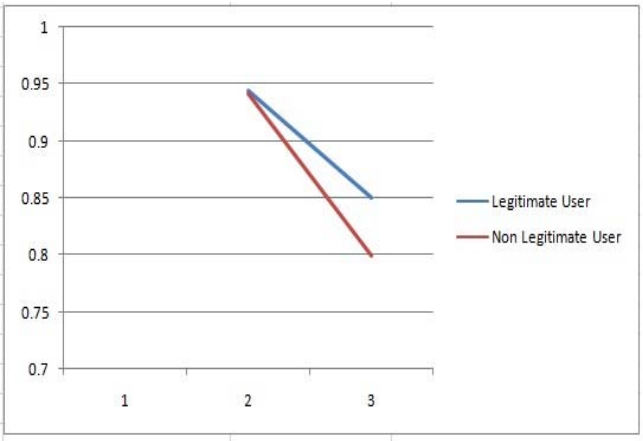
Table 3: Results based on precision and recall 2

Precision	Legitimate User	Relevant Intersect Reviewed/Retrieved	Correct Relevant Object/ Retrieved Object	0.83
Recall	Non Legitimate User	Relevant Intersect Reviewed/Retrieved	Correct Relevant Object/ Retrieved Object	0.8

Table 4: Results based on precision and recall 3

User	*Precision*	*Recall*
Legitimate User	17	7
Non- Legitimate User.	1	16
Total	0.94281045	0.825
Accuracy Percentage	0.825	NA

Result



5. Conclusion

In this paper, three different password levels are proposed. Each level provides the different degree of security. From the calculation and experimental result the level2 and level3 three generates the huge amount of passwords. After that the level 3 gives the higher degree of security. If the intruder want to break-in our proposed system then he have to use all above different possibilities, which is practically infeasible The computational complexity is greatly reduced as compare to existing system and the detection speed is much faster than existing system.

6. Future Enhancement

The work on this graphical password scheme can be extended by considering different ways of creating new captcha challenge. The proposed system is developed for file sharing system but it can be applicable to banking, ATMs, Military applications. The level of security can be improved by adding the more security primitive. Also focusing on provide shoulder surfing resistance.

References

[1] K. Renaud. “Evaluating authentication mechanisms”. In L. Cranor and S. Garnkel, editors, *Security and*

Usability: Designing Secure Systems That People Can Use, chapter 6, pp.103-128. O'Reilly Media, 2005.

[2] A. Adams and M. A. Sasse. "Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures". *Communications of the ACM*,42:41-46, 1999.

[3] D. Feldmeier and P. Karn. "UNIX Password Security-Ten Years Later". *In Crypto'89*, August 1989.

[4] R. Morris and K. Thompson. "Password Security: A Case History". *Communications of the ACM*, 22(11):594-597, 1979.

[5] D. Florencio and C. Herley. "A large-scale study of WWW password habits". *In 16th ACM International World Wide Web Conference (WWW)*, May 2007.

[6] A. Adams, M. A. Sasse, and P. Lunt. "Making passwords secure and usable". *In HCI 97: Proceedings of HCI on People and Computers*, pp.1-19, London, UK, 1997.

[7] G. Blonder. "Graphical passwords". *United States Patent*, 5,559,961, 1996.

[8] B. Kirkpatrick. "An experimental study of memory". *Psychological Review*, 1:602-609, 1894

[9] S. Madigan. "Picture memory". In J. Yuille, editor, *Imagery, Memory, and Cognition: Essays in Honor of Allan Paivio*, chapter 3, pp.65-89. Lawrence Erlbaum Associates, 1983.

[10] A. Paivio, T. Rogers, and P. C. Smythe. "Why are pictures easier to recall than words?", *Psychonomic Science*, 11(4):137-138, 1968.

[11] R. Shepard. "Recognition memory for words, sentences, and pictures". *Journal of Verbal Learning and Verbal Behavior*, 6:156-163, 1967.

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

[13] X. Suo, Y. Zhu, and G. Owen. "Graphical passwords: A survey". *In Annual Computer Security Applications Conference (ACSAC)*, December 2005.

[14] 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.

[15] X.Y. Liu., J.H. Qiu., L.C. Ma., H.C. Gao., etc., "A Novel Cued-recall Graphical Password Scheme", *In sixth International Conference on Image and Graphics (ICIG)*, pp.949-956, 2011.

[16] H.C. Gao., Z.J. Ren., X.L. Chang., X.Y. Liu., etc., "A New Graphical Password Scheme Resistant to Shoulder-Surfing", *International Conference on Cyberworlds (CW)*, pp.194-199, December 2010.

[17] D. Nali and J. Thorpe. "Analyzing user choice in graphical passwords". *Technical Report TR-04-01, School of Computer Science*, Carleton University, May 2004.

[18] H. Tao. "Pass-Go, a new graphical password scheme". *Master's thesis, School of Information Technology and Engineering*, University of Ottawa, June 2006.

[19] H. Tao and C. Adams. "Pass-Go: A proposal to improve the usability of graphical passwords". *International Journal of Network Security*,7(2):273-292, 2008.

[20] J. Thorpe. "On the Predictability and Security of User Choice in Passwords". *PhD thesis, School of Computer Science*, Carleton University, January 2008.