Available online at www.elixirpublishers.com (Elixir International Journal)

Network Engineering

Elixir Network Engg. 89 (2015) 37039-37042

ISSN: 2229-712X

# A Click Based Graphical Password Scheme Using AI Hard Problem

Pranita H Mokal and R. N. Devikar

Amrutvahini college of Engineering, Sangamner, Ahmednagar, City, India.

**ARTICLE INFO**

**Article history:**

Received: 6 November 2015;

Received in revised form:

10 December 2015;

Accepted: 18 December 2015;

**Keywords**

Textual Password,

Graphical Password,

CAPTCHA,

AI Hard Problem.

**ABSTRACT**

For providing security,password is important factor. Now a day in any field security is essential.The textual password is the most common password but the textual password has several issues.The new password scheme is introduced in which images are used as a password known as Graphical password.In this paper, a new password scheme is developed which combines recognition based schemes.In this scheme three levels of security is provided.



## Introduction

Now a day for every system authentication is important factor. Authentication is one process in which a system verifies the identity of a User who wants to access it. The authentication systems are categorize into three categories such as: Biometric based authentication, Token based authentication, Knowledge based authentication. In token based techniques, tokens are nothing but physical devices that are used to access secure systems. They can be in the form of a card. Token based authentication is used in key cards, bank cards and smart cards. In biometric based authentication there is use of known and recorded physical traits of a user to authenticate his identity. It is based on fact that no two individuals share the same exact physical traits. It may include Voice recognition Fingerprints Face scanning and recognition etc. Knowledge based techniques contain both text-based and picture-based passwords. This can be separated into two categories: recognition-based and recall-based graphical techniques. In recognition-based techniques, first a set of images are presented to user and for authentication the user should recognize and identifying the images that user has selected at some stage in the registration phase. In recall-based techniques, a user should replicate something that user generated or selected at some stage in the registration phase.

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 reactions are presented 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 resolved by present computer programs or bots.

## Literature Survey

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.

## 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 among clients and the authentication server using Transport Layer Security (TLS). The authentication server stores a salt value *s* and a hash value $H(\rho, s)$ for every user ID, $\rho$ is the password of the user and h is the hash value. During authentication phase, *authentication* server produce a CaRP image then records the object's locations in the image and finally sending an image to the user to click his/her 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, $\rho'$, 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 $\rho$ 'with the salt. Then compares the it *with* the has value stored for that user account. If the two hash values are equivalent then authentication succeeds.

## 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

Tele:

E-mail addresses: pranitamokal62@gmail.com

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.

**Overview of Click Based Password Scheme**

In this scheme, during registration phase first user has to enter his details like username, address, email id, security question and answer etc. The user has to give his own security question .In other words, user has the freedom to select any security question. This security question is required for resetting the password. The username is primary key in this scheme. During authentication phase, user has to go through three levels of security. First, user has to enter the correct password for level1 which is clicktext password scheme after that user has to enter the level2 password which is clickAnimal scheme and finally user has to enter the level3 password which is AnimalGrid scheme. As user enters level1, level2 and level3 password system grant access to user. Then user can upload or download his file.

**System Requirements**

- **Hardware Requirements:**

1. RAM: 512 MB.
2. Processor: Pentium-4 and Above.

- **Software Requirements:**

1. Operating System: Windows XP
2. Programmimg Language: JDK 1.6, Eclipse SDK
3. Database: MySQL Server

**System Architecture**

The following Figure 1 show the system architecture. In click based graphical pass- word scheme, three recognition graphical password schemes are combined. These schemes are nothing but level1, level2 and level3 passwords. Discrete centralization and SHA-1 algorithms are used to provide more security to the password system. This scheme is developed on android platform.

The modules of this system are as follows:

1 Client-server module
2 ClickText Module
3 ClickAnimal Module
4 AnimalGrid Module

**Client-server module**

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 wireless 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.

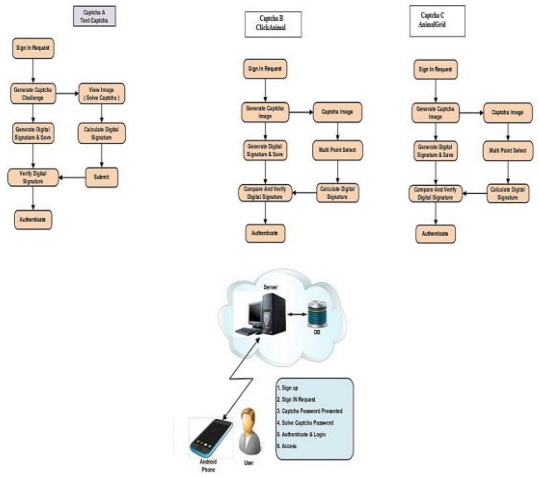


**Figure 1. System architecture**

**ClickText Module**

This is a recognition-based CaRP scheme. It consist of characters which are not visually-confusing such as , Letter O and digit 0 seen as same which may cause confusion in CaRP images.So that one character is excluded from the alphabet setoff this scheme. A password of this scheme is a sequence of characters. e.g., =HNS34KIU which is comparable to a textual password. A ClickText image is created by means of the core Captcha engine as if a Captcha. Each location of characters is recorded all through generation of clicktext image. These recorded locations are then further used to to produce ground truth value the character clicktext image. The authentication server is using the ground truth value to classify the characters resultant to user- clicked points. In ClickText images, characters can be prearranged at random on 2D space.

**ClickAnimal Module**

This is a recognition-based CaRP scheme. It is built on the concept of Captcha Zoo. In Captcha Zoo, an alphabet of similar animals are used as password. One or more 3D models are created for every animal. Then Click Animal images are generated by using the Captcha generation process: During this process, 3D models are applied to produce 2D animals. In this process, different views, textures, colors, lightning , and distortions are applied. The resultant 2D animals are then set on a cluttered background like grassland. Some animals possibly will be obstructed by other animals in the image, but the condition is that the core parts should not be obstructed in order for humans to identify each of them.

**AnimalGrid Module**

This scheme is related to ClickAnimal scheme. In this scheme, generated ClickAnimal image is presented first. Then user has to select the appropriate image as a password. When an animal is preferred, then grid of n*n become visible to user. The size of grid-cell is equal to the the bounding rectangle of the selected animal. A user can choose zero to multiple grid-cells in order to match his/her password. For that reason a password is a sequence of animals with grids. A password have to start on with an animal. When the user clicks on the the animal on the image as a password image. the clicked point's coordinates are recorded. The bounding rectangle is calculated based on that clicked points. The user after that clicks a sequence grids from zero to multiple grid-cells that match the grid cells of the following first animals in her password, and then gets back to the ClickAnimal image.

**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 |

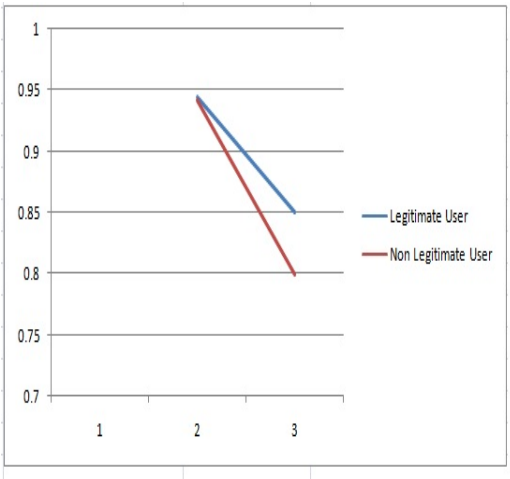
**Table 3. Results based on precision and recall 2**

| | | | | |
|---|---|---|---|---|
| **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**




**Application**

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

**Conclusion**

In the dissertation 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.

**Future Enhancement**

The work on the click based 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 improve by adding the more security primitive. Also focusing on provide shoulder surfng resistance.

**Acknowledgment**

I am extremely grateful to Mr. R. N. Devikar for his guidance and support. I will forever remain grateful for the constant support and guidance extended by guide, in making this report. Through our many discussions, he helped me to form and solidify ideas. The invaluable discussions I had with his, the penetrating questions he has put to me and the constant motivation, has allowed to the development of this project.

I wish to express my sincere thanks to the Head of department, Prof. B. S. Borkar also grateful thanks to the departmental sta_ members for their support. I am obliged to our Principal Dr. G. J. Vikhe Patil for their inspiration and co-operation.

**Reference**

[1] Bin B. Zhu, Je_ Yan, Guanbo Bao, Maowei Yang, and Ning Xu, IEEE, and Yun- Qing Shi,Fellow, "Captcha as Graphical PasswordsA New Security Primitive Based on Hard AI Problems", IEEE Transactions on information fornsics and security, Volume 2, Feb 2014.

[2] R. Biddle, S. Chiasson, and P. C. van Oorschot, "Graphical passwords: Learning from the first twelve years", International Journal of Scientific and Research Publi cations , pp.273-284, Volume 3, Issue 6, June 2003.

[3] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords", International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, PP.453-459, Volume 2, Issue-6, January 2013.

[4] K. Renaud , "Evaluating authentication mechanisms", Security and Usabil ity:Designing Secure Systems That People Can Use, PP.103-128, Volume 1, Issue 2, 2005.

[5] D. Davis, F. Monrose, and M. K. Reiter, " On user choice in graphical password schemes", in Proc. 13th USENIX Security Symp, pp.114, Aug. 2004.

[6] S. Wiedenbeck, J.Waters, J.-C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: E_ects of tolerance and image choice", Proc. Pittsburgh, pp. 112, Jul. 2005.

[7] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, " Authentication using graphical passwords: Basic results ", Proc. Human-Comput. Interaction Int., Las Vegas, NV, Jul. 2527, 2005.

[8] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, " Pass Points: Design and longitudinal evaluation of a graphical password system", Int. J. Human Comput. Stud., volume 63, no. 1/2, pp. 102127, Jul. 2005.

[9] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The design and analysis of graphical passwords ", Proc. 8th USENIX Security Symp., Washington DC, pp. 114, Aug. 1999.

[10] J. Thorpe and P. C. van Oorschot," Graphical dictionaries and the memorable space of graphical passwords" , Proc. USENIX Security, San Diego, CA, Aug. 913, pp. 10,2004.

[11] A. Adams and M. A. Sasse, "Users are not the enemy: Why users compromise computer security mechanisms and how to take remedial measures", Commun. ACM, volume 42, no. 12, pp. 4046, Dec. 1999.

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

[13] Jansen, W. Gavrila, S. Korolev, V. Ayers, R. Swanstrom, "Picture Password: A Visual Login Technique for Mobile Devices", In Proceedings of the 5th international conference of information and community security, pp. 313324, June 2003.

[14] D. Hong, S. M an, B. Hawes, and M. Mathews, " A password scheme strongly resistant to sp yware ", In Proceedings of International conference on security and management, Las Vergas, NV, 2004.

[15] R. Dhamija and A. Perrig., "Dj vu: A User Study Using Images for Authentication", In Proceedings of the USENIX Security Symposium, 2000.

[16] I. Jermyn, A. Mayer, F. Monrose. M. K. Reiter and A. D. Rubin, " The Design and Analysis of GraphicalPasswords, In Proceedings of the 8thUSENIX Security Symposium, 1999.