INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

GRAPHICAL PASSWORD: CLICK-BASED GRAPHICAL PASSWORD SCHEME TO PREVENT ACCESS AGAINST ATTACKS

POOJA PRAVIN NIWALKAR, PROF. NITIN J JANWE

Department of Computer Science & Engineering, Rajiv Gandhi College of Engineering, Research &Technology, Chandrapur-442401

Accepted Date: 15/03/2016; Published Date: 01/05/2016

Abstract: Security based primitives is emerging in exciting new paradigm for protection, but has been underexplored. In this paper a new security primitive is used called as click based graphical password scheme, which comes under the family of graphical password systems which is one of the top technology called Captcha which we call Captcha as graphical passwords (CaRP). Consumers usually choose passwords that are unforgettable and are easy for aggressors to guess, but the strong system allotted passwords are hard for users to recall. Mostly protection primitives are based on complex and difficult mathematical complications. Utilizing Artificial Intelligence problems for security is issuing as a new prototype. A new protection primitive is introduced based on strong and complex AI problems which is known as Captcha as Graphical Password (CaRP). Notably, a CaRP based password can alternatively be detected by automatic online estimating attacks. CaRP it extends sensible protection and usability and comes out to fit well with some practical examples for bettering online security

Keywords: Graphical password, hotspots, CaRP, Captcha, dictionary attack, protection primitive.

Corresponding Author: MS. POOJA PRAVIN NIWALKAR

Access Online On:

www.ijpret.com

How to Cite This Article:

Pooja Pravin Niwalkar, IJPRET, 2016; Volume 4 (9): 273-278

PAPER-QR CODE

INTRODUCTION

Cyber security is an important issue to tackle. Various user authentication methods are used for this purpose. It helps to avoid misuse or illegal use of highly sensitive data. Text and graphical passwords are mainly used for authentication purpose. But due to various flaws, they are not reliable for data security. Text passwords are insecure for reasons and graphical are more secured in comparison but are vulnerable to shoulder surfing attacks. Hence by using graphical password system and CAPTCHA technology a new security primitive is proposed. We call it as CAPTCHA as gRaphical Password (CaRP).CaRP is a combination of both a CAPTCHA and a graphical password scheme. Captcha's given as Completely Automated Public Turing test to tell computers and Humans Apart. It‟s mainly used for users to accessing their protected resources. It is a kind of challenge response test use to compute specifically whether the user is human or not. The essential and underlying task in this security based project is to create secured login authentication towards the end user.

There are different ways for providing security. Here we introduced is one of the new methods for the security purpose. A new protection primitive is showed based on AI troubles, namely, a new family of graphical password schemes built on top of Captcha technology, which is known as Captcha and Graphical Password (CaRP). Here a user while get login to their respective accounts or websites there an image will be generated. The user should click on that image or on any part of that image as a password and that image or clicked particular part will be stored as their graphical password and those images are differently generated for different users. Considering that generated graphical image as a password along with the user's regular password for further logins. Hence introduce a security for the users so they can browse safely and their personals will be safe.

In this paper click point based captcha plays a vital role to ensure the security for end user validation. The feasibility of the project is analyzed and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company.

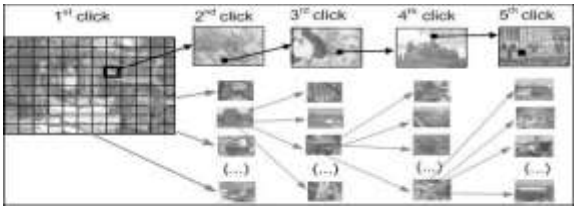
The remainder of this paper is organized as follows: the introduction about the various scheme and background related works in section II. Section III describe the introduction related to click based graphical password. Section IV & V describes the implementation models and system architecture of the project. Finally the conclusion and acknowledgement of the project .And at last paper is concluded.

II. Background and Related works

A large number of graphical password schemes have been proposed. They can be classified into three categories according to the task involved in memorizing and entering passwords: recognition, recall, and cued recall. Each type will be briefly described here. More can be found in a recent review of graphical passwords [1].A recognition-based scheme requires identifying among decoys the visual objects belonging to a password portfolio.A typical scheme is Pass faces [2] wherein a user selects a portfolio of faces from a database in creating a password .During authentication, a panel of candidate faces is presented for the user to select the face belonging to her portfolio. This process is repeated several rounds, each round with a different panel. A successful login requires correct selection in each round. The set of images in a panel remains the same between logins, but their locations are permuted. Story is similar to Pass faces but the images in the portfolio are ordered, and a user must identify her portfolio images in the correct order.

III. Click-based Graphical Password

Our work is based on Click-based graphical password scheme.It require a user to click on a set of points on one or more presented background image.In click based password user should easy to remember picture but hard to crack.



The image will be provided to user for authenticating there documents. The user need to select a particular point on the image for its password. That point’s co-ordinate are collected and saved. User need to click on another point for password. That particular point’s co-ordinate is also collected and saved. While entering password for same document co-ordinates of the points should match i.e the click on image should the that particular point. A wrong click leads down an incorrect path, with an explicit indication of authentication failure only after the final click.

Do’s and Don’ts for click based graphical password

- ✓ It should be easy to remember but hard to crack.

- ✓ Avoid hotspots on the picture while selecting click point.
- ✓ Always remember the click point and picture which will become helpful for knowledge based authentication.
- ✓ Do not use too much bright and black picture for password.

IV. Implementation

MODULES DESCRIPTION:-

User registration:

In this module, Users are having authentication and security to access the detail which is presented in the Image system. Before accessing or searching the details user should have the account in that otherwise they should register first.

Captcha in Authentication:

In this module we use both Captcha and password in a user authentication protocol, which we call *Captcha-based Password Authentication (CbPA) protocol*. The CbPA-protocol in requires solving a Captcha challenge after inputting a valid pair of user ID and password. For an invalid pair of user ID and password, the user has a certain probability to solve a Captcha challenge before being denied access.

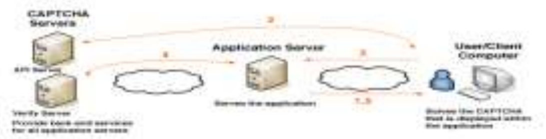
Overcoming Thwart Guessing Attacks:

In a guessing attack, a password guess tested in an unsuccessful trial is determined wrong and excluded from subsequent trials. The number of undetermined password guesses decreases with more trials, leading to a better chance of finding the password. To counter guessing attacks, traditional approaches in designing graphical passwords aim at increasing the effective password space to make passwords harder to guess and thus require more trials.

Security of Underlying Captcha:

Computational intractability in recognizing objects in CaRP images is fundamental to CaRP. Existing analyses on Captcha security were mostly case by case or used an approximate process. No theoretic security model has been established yet. Object segmentation is considered as a computationally expensive, combinatorially-hard problem, which modern text Captcha schemes rely on.

V. System Architecture


CAPTCHA Servers
API Server
Verify Server
Provide back-end services for all application servers
Application Server
Serves the application
User/Client Computer
Solves the CAPTCHA that is displayed within the application
2
4
3
1,5

The system architecture diagram states about the overall idea of the project, it makes us to understand how it flows from starting to end phase. The numbers directed by arrow gives us the direction of flow of steps taken place in the project.

CONCLUSIONS

Graphical password are an alternative to textual alphanumeric password. It satisfies both conflicting requirements i.e it is easy to remember and hard to guess. By the solution of shoulder surfing problem, it become more secure and easy password scheme. By implementing encryption algorithm and hash algorithm, for storing and retrieving pictures and point, one can achieve more security. CaRP has good potential for refinements. More importantly, CaRP inspire new inventions of such AI based security primitives. But Picture password i.e graphical password is still immature, so more research is required in this field.

ACKNOWLEDGEMENT

We would like to thank Department of Computer Science & Engineering, RCERT Chandrapur for providing infrastructure and guidance to understand graphical passwords that provide security.

REFERENCES

1. R. Biddle, S. Chiasson, and P. C. van Oorschot, “Graphical passwords: Learning from the first twelve years,” ACM Comput. Surveys, vol. 44, no. 4, 2012.
2. (2012, Feb.). The Science Behind Passfaces [Online]. Available:http://www.realuser.com/published/ScienceBehindPassfaces.pdf.
3. 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.
4. H. Tao and C. Adams, —Pass-Go: A proposal to improvethe usability of graphical passwords,‖ *Int. J. Netw. Security*,vol. 7, no. 2, pp. 273–292,2008.
5. 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, pp. 102 127, Jul. 2005.

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. D. Florencio and C. Herley. ―A large-scale study of WWW password habits‖. In 16th ACM International WorldWide Web Conference (WWW), May 2007.

8. 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.

9. J. Thorpe. ―On the Predictability and Security of User Choice in Passwords‖. PhD thesis, School of Computer Science, Carleton University, January 2008.

10. S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon. ―PassPoints: Design and longitudinal evaluation of a graphical password system‖. International Journal of Human-Computer Studies, 63 (1-2): 102-127, 2005.

11. P. C. van Oorschot, A. Salehi-Abari and J. Thorpe. ―Purely Automated Attacks on PassPoints-Style Graphical Passwords‖. IEEE Transactions on Information Forensics and Security, 5(3): pp.393-405, 2010.

12. Real User Corporation. *The science behind Passfaces*. White paper, http://www.realuser.com/published/ ScienceBehindPassfaces.pdf, accessed Feb. 2012.

13. Baljit Singh Saini and Anju Bala "A Review of Bot Protection using CAPTCHA for Web Security," IOSR Journal of Computer Engineering, 2013, pp. 36-42, 2013.

14. Xiao Ling-Zi and ZHANG Yi-Chun "A Case Study of Text-Based CAPTCHA Attacks," in International Conference on Cyber-Enabled Distributed Computing and Knowledge Discover, 2012.

15. Chen-Chiung Hsieh and Zong-Yu Wu "Anti-SIFT Images Based CAPTCHA Using Versatile," IEEE, 2013.

16. L. Wang, X. Chang, Z. Ren, H. Gao, X. Liu, and U. Aickelin, ―Against spyware using CAPTCHA in graphical password scheme,‖ in *Proc. IEE Int. Conf. Adv. Inf. Netw. Appl.*, Jun. 2010, pp. 1–9.

17. J. Bonneau, ―The science of guessing: Analyzing an anonymized corpus of 70 million passwords, ‖ in *Proc. IEEE Symp. Security Privacy*, Jun. 2012, pp. 20–25.

18. J. Elson, J. R. Douceur, J. Howell, and J. Saul, ―Asirra: A CAPTCHA that exploits interest-aligned manual image categorization,‖ in *Proc. ACM CCS*, 2007, pp. 366–374.

19. R. Lin, S.-Y. Huang, G. B. Bell, and Y.-K. Lee, ―A new CAPTCHA interface design for mobile devices, ‖ in *Proc. 12th Austral. User Inter. Conf.*, 2011, pp. 3–8.

20. S. Kim, X. Cao, H. Zhang, and D. Tan, ―Enabling concurrent dual views on common LCD screens, ‖ in *Proc. ACM Annu. Conf. Human Factors Comput. Syst.*, 2012, pp. 2175–2184.