Scientific Journal of Impact Factor (SJIF): 3.134
e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 3, Issue 1, January -2016

SECURE AUTHENTICATION BY USING GRAPHICAL PASSWORD TECHNOLOGY

Narendra Chaudhari[1], Sagar Handure[2], Mandar Pawar[3], Prof.Sinju N.S.[4]

[1,2,3,4]*Department of computer engineering, Genba Sopanrao Moze College of Engineering, Balewadi*

Abstract *— Various security primitives rely on upon hard experimental issues. Using hard AI issues for security is creating as an invigorating new perspective, yet has been under-researched. In this paper, we show another security primitive in perspective of hard AI issues, to be particular, a novel gathering of graphical mystery key systems taking into account top of Captcha advancement, which we call Captcha as graphical passwords (CaRP). CaRP is both a Captcha and a graphical mystery key arrangement. CaRP addresses different security issues totally, for instance, web estimating attacks, exchange ambushes, and, if merged with twofold view developments, shoulder-surfing strikes. Unmistakably, a CaRP mystery key can be found just probabilistically by means of modified web theorizing strikes paying little mind to the likelihood that the watchword is in the request set. CaRP furthermore offers a novel approach to manage area the most likely comprehended picture hotspot issue in standard graphical mystery key systems, for instance, PassPoints, that frequently prompts weak watchword choices. CaRP is not a panacea, but instead it offers sensible security and comfort and appears to fit well with some practical applications for improving online security.*

Keywords- Graphical password, password, hotspots, CaRP, Captcha, dictionary attack, password guessing attack, security primitive.

I. INTRODUCTION

Security is most essential in our everyday life. CAPTCHA remaining for "Totally Automated Public Turing test to differentiate Computers and Humans One from the other", is a programmed challenge-reaction test to recognize people and machines. Captcha is utilized for assurance against diverse assault i.e. bot[12]. In image based captcha is click based graphical passwords, where arrangement of click on a picture is utilized to determine a secret key. It gives insurance against online word reference assaults on secret key. In this for login each time click on pictures. Captcha can be applied on touch screen gadgets where on writing passwords is not more secure, particularly for secure web applications.
In ahead of schedule framework just content secret word is utilized which is extremely hard to recollect if enter a long password[17][13]. On the off chance that we utilize littler secret key then it can be effortlessly recognize and we additionally utilize basic password for some records so for that Image based captcha give more security amid confirmation.

II. LITERATURE REVIEW

1. Graphical passwords: Learning from the first twelve years
AUTHORS: R. Biddle, S. Chiasson, and P. C. van Oorschot,
Description:
Beginning around 1999, a considerable number of graphical secret key plans have been proposed as different options for text based password confirmation. We give an extensive outline of distributed examination in the region, covering both ease of use and security angles and also framework assessment. The article first inventories existing methodologies, highlighting novel elements of chose plans and recognizing key ease of use or security points of interest. We then audit convenience necessities for information based verification as they apply to graphical passwords, distinguish security dangers that such frameworks must address and survey known attacks, talk about methodological issues identified with observational assessment, and recognize zones for further research and enhanced strategy.

2. Pass-Go: A proposal to improve the usability of graphical passwords
AUTHORS: H. Tao and C. Adams,
Description:
Inspired by an old Chinese game, Go, we have designed a new graphical password scheme, Pass-Go, in which a user selects intersections on a grid as a way to input a password. While offering an extremely large full password space (256 bits for the most basic scheme),our scheme provides acceptable usability, as empirically demonstrated by, to the best of our knowledge, the largest user study (167 subjects involved) on graphical passwords, conducted in the fall semester of 2005 in two university classes. Our scheme supports most application environments and input devices, rather than being

limited to small mobile devices (PDAs), and can be used to derive cryptographic keys. We study the memorable password space and show the potential power of this scheme by exploring further improvements and variation mechanisms.

3. On predictive models and user drawn graphical passwords
AUTHORS: P. C. van Oorschot and J. Thorpe,
Description:
In commonplace text-based password schemes, users typically choose passwords that are easy to recall, exhibit patterns, and are thus vulnerable to brute-force dictionary attacks. This leads us to ask whether other types of passwords (e.g., graphical) are also vulnerable to dictionary attack because of users tending to choose memorable passwords. We suggest a method to predict and model a number of such classes for systems where passwords are created solely from a user's memory. We hypothesize that these classes define weak password subspaces suitable for an attack dictionary. For user-drawn graphical passwords, we apply this method with cognitive studies on visual recall. These cognitive studies motivate us to define a set of *password complexity factors* (e.g., reflective symmetry and stroke count), which define a set of classes. To better understand the size of these classes and, thus, how weak the password subspaces they define might be, we use the "Draw-A-Secret" (DAS) graphical password scheme of Jermyn et al. [1999] as an example. We analyze the size of these classes for DAS under convenient parameter choices and show that they can be combined to define apparently popular subspaces that have bit sizes ranging from 31 to 41—a surprisingly small proportion of the full password space (58 bits). Our results quantitatively support suggestions that user-drawn graphical password systems employ measures, such as graphical password rules or guidelines and proactive password checking.

4. Modeling user choice in the pass points graphical password scheme
AUTHORS: A. E. Dirik, N. Memon, and J.-C. Birget,
Description:
Develop a model to identify the most likely regions for users to click in order to create graphical passwords in the *Pass Points* system. A Pass Points password is a sequence of points, chosen by a user in an image that is displayed on the screen. Our model predicts probabilities of likely click points; this enables us to predict the entropy of a click point in a graphical password for a given image. The model allows us to evaluate automatically whether a given image is well suited for the Pass Points system, and to analyze possible dictionary attacks against the system. We compare the predictions provided by our model to results of experiments involving human users. At this stage, our model and the experiments are small and limited; but they show that user choice can be modeled and that expansions of the model and the experiments are a promising direction of research.

5. Human-seeded attacks and exploiting hot spots in graphical passwords
AUTHORS: J. Thorpe and P. C. van Oorschot,
Description:
Although motivated by both usability and security concerns, the existing literature on click-based graphical password schemes using a single background image (e.g., Pass Points) has focused largely on usability. We examine the security of such schemes, including the impact of different background images, and strategies for guessing user passwords. We report on both short- and long-term user studies: one lab-controlled, involving 43 users and 17 diverse images, and the other a field test of 223 user accounts. We provide empirical evidence that popular points (hot-spots) do exist for many images, and explore two different types of attack to exploit this hot-spotting: (1) a "human-seeded" attack based on harvesting click-points from a small set of users, and (2) an entirely automated attack based on image processing techniques. Our most effective attacks are generated by harvesting password data from a small set of users to attack other targets. These attacks can guess 36% of user passwords within 2^{31} guesses (or 12% within 2^{16} guesses) in one instance, and 20% within 2^{33} guesses (or 10% within 2^{18} guesses) in a second instance. We perform an image-processing attack by implementing and adapting a bottom-up model of visual attention, resulting in a purely automated tool that can guess up to 30% of user passwords in 2^{35} guesses for some instances, but under 3% on others. Our results suggest that these graphical password schemes appear to be at least as susceptible to offline attack as the traditional text passwords they were proposed to replace.

III.SYSTEM ANALYSIS

EXISTING SYSTEM:
Security factors are based on hard mathematical issue. Using hard AI issue for security is upcoming as an exciting new technique, but has been underexplored.Basic task in security is to create cryptographic primitives depend on hard mathematical issues that are computationally intractable.
The main idea of the paper is to replace the textual password with a graphical password.In ancient times,the passwords were materialized in the form of graphical passwords with X,Y as co-ordinates on the images. Randomization clicks on the images enable the user to access the system is one of the major disadvantage.To remove this disadvantage,Persuasive cued

click points comes into the picture An image will be framed with multiple click points in turn, which will have successive cued clicks on the images.The main point is, the user should select a clickpoints on the image

DISADVANTAGES:

- This technique has gained limited success than cryptographic primitives based on hard math issues and their wide applications.
- In this technique,the important concept is Captcha, which differentiate human users from computers by presenting a captcha challenge.

PROPOSED SYSTEM:

We invented a new security technique rely on hard AI issue which consist of graphical password systems built upon Captcha technology,which is known as Captcha as a graphical passwords (CaRP). CaRP is both a Captcha and a graphical mystery key arrangement. CaRP addresses different security issues totally, for instance, web estimating attacks, exchange ambushes, and, if merged with twofold view developments, shoulder-surfing strikes.

In this paper we have step forward in security level by adding One Time Password (OTP) to our proposed system.While login after entering username and text password user has to select image from group of images and in selected image user has to select clickpoints to generate password.Then it will generate an OTP and automatically sent on users registered mobile,by entering correct OTP user will be login successfully.

ADVANTAGES:

- The proposed system offers reasonable security and usability and it looks fit well with some practical applications for improving online security. This threat is widespread and supposed as top cyber security risk.
- The system defense against online dictionary attacks is a more subtle problem than it might appear.

IV.MODULES

1. User Registration Module:

First user need to provide basic information like first name,last name,city,username,password,mobile number,also answers for security questions in case of password forgeted.During registration we have to follow some validation constraints such as mobile number must be 10 digits long,Username and password should contain combination of alphabets,symbols and numbers.Password should not be less than 8 characters.After that user is provided with group of images,in selected image user has to select certain points on the image to generate a captcha password.To validate mobile number OTP is generated and automatically sent on users registered mobile,which he has to enter and get verified his mobile number.After entering all the details user has to click on submit button to get register successfully.

2. User Login Module:

In user login module user has to enter username,text password,and select the same image from the group of images which he has selected during registration and also has to select already selected clickpoints on that image.After selecting correct image and clickpoints,OTP is generated and sent on users registerd mobile.Then user has to enter correct OTP which he has received on his mobile to login successfully.

3. Administrator:

The administrator will first login on to the site and he will include the details about Hotels, Cabs and Airline tickets. In view of the necessity the clients will use the administrations and they will book the administrations. After that in view of the use the nature of the administration is makes improves. A chart is created for every administration. The graph is visible to administrator only. After viewing the ratings the admin will update the details.

4.One Time Password Scheme:

A one-time password (OTP) is a password that is valid for only one login session or transaction, on a computer system or other digital device.OTPs avoid a number of shortcomings that are associated with traditional (static) password-based authentication.

Advantage of OTPs is that, in contrast to static passwords, they are not vulnerable to replay attacks. This means that a potential intruder who manages to record an OTP that was already used to log into a service or to conduct a transaction will not be able to abuse it, since it will no longer be valid. A second major advantage is that a user who uses the same (or similar) password for multiple systems, is not made vulnerable on all of them, if the password for one of these is gained by an attacker. A number of OTP systems also aim to ensure that a session cannot easily be intercepted or impersonated without knowledge of unpredictable data created during the previous session, thus reducing the attack surface further.

V. SYSTEM ARCHITECTURE

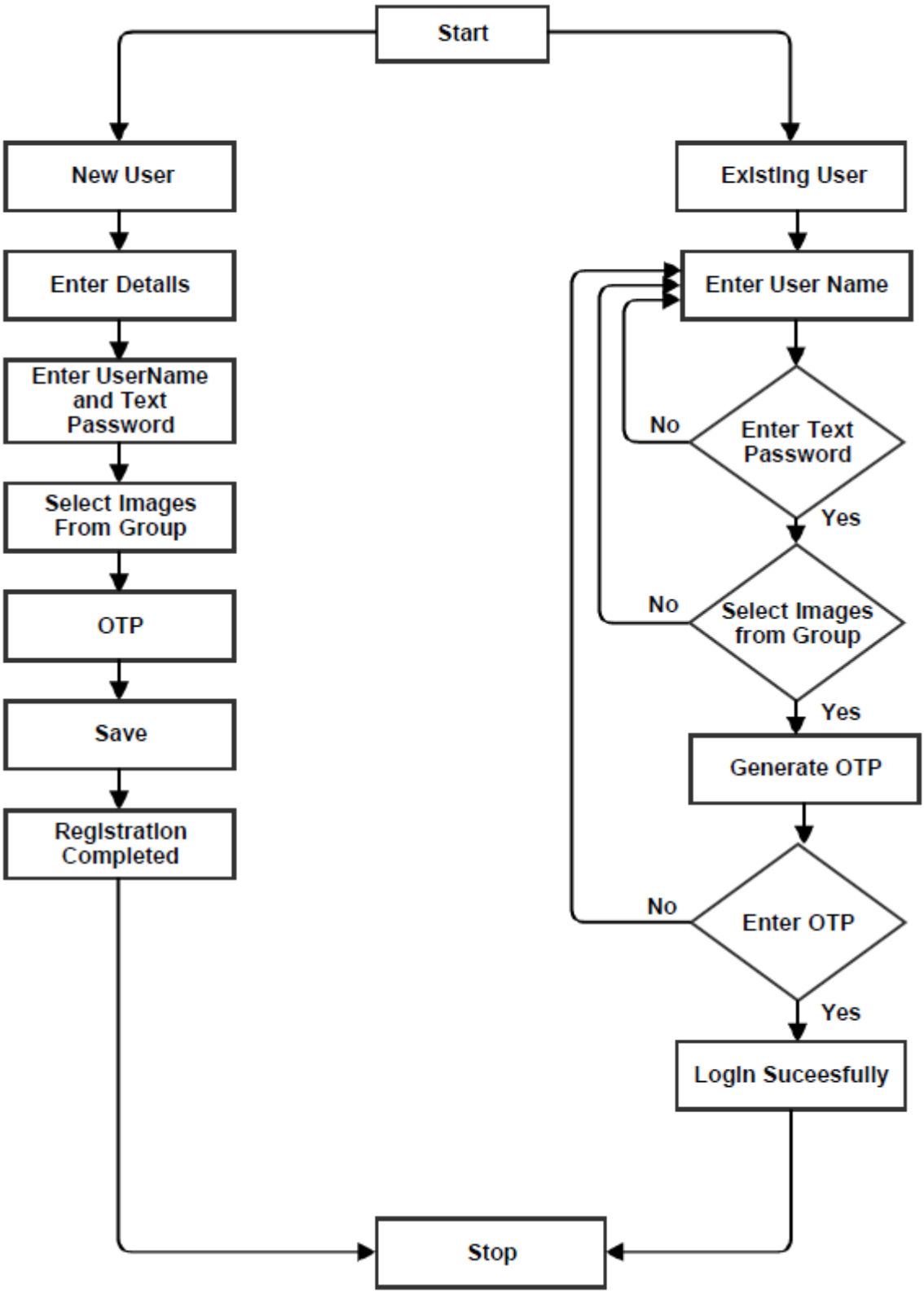

Figure 1. System Architecture

In above Figure 1. while login if the user is new then user has to register first. While registering user first enter the detail like name, mobile no, user name, text password, etc. After successful registration user can login by using username and password. if username and password is incorrect then it gives four attempts to enter correct credentials

otherwise it logins and next it goes to selection of image Captcha.here user needs to select image intensity as password which stored while registering user account.If the Captcha password is correct then access is enable otherwise access is denial.Once successfully done with capctha password OTP will generate and send on user mobile which entered during user registration.If the entered OTP is correct then access is enable otherwise access is denial.

VI. CONCLUSION AND FUTURE WORK

Our graphical password system provides more security to data and assurance against different attack. Our graphical password system is based on text password and graphical password. For successful login user has to select correct image which is chosen by user during a registration and this system provide text password which provide more security to data. Future work depends on Pattern.

Future works might incorporate enhancing the following strength against lighting conditions; perhaps by using more sophisticated and expensive capturing devices such as infrared cameras that can operate in absence of light and give more accurate tracking results. Including the double left click and the drag mode (enabling/disabling with the right double eye squint) functionalities. Adding voice charges to dispatch the project, begin the identification process, and to empower/cripple controlling the mouse with the face. Future work might incorporate enhancing the vigor against the lighting conditions. By utilizing the exceptionally qualified camera work the operation to get more precise result. Adding the scrolling movement (Using nose) Functionality. Also add the speech module which will operated by users mouse and launch on the start of the PC. Likewise we can include using so as to look over usefulness face developments.

ACKNOWLEDGEMENT

We might want to thank the analysts and also distributers for making their assets accessible. We additionally appreciative to commentator for their significant recommendations furthermore thank the school powers for giving the obliged base and backing.

REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the Clouds: A Berkeley View of Cloud Computing,"Technical Report EECS-2009-28, Univ. California, Berkeley, 2009.

[2] K.J. Arvelin and J. Kekalainen, "Cumulated Gain-Based Evaluation of IR Techniques," ACM Trans. Information Systems, vol. 20, no. 4, pp. 422-446, 2002.

[3] P.A. Bonatti and P. Festa, "On Optimal Service Selection," Proc. 14th Int'l Conf. World Wide Web (WWW '05), pp. 530-538, 2005.

[4] J.S. Breese, D. Heckerman, and C. Kadie, "Empirical Analysis of Predictive Algorithms for Collaborative Filtering," Proc. 14th Ann. Conf. Uncertainty in Artificial Intelligence (UAI '98), pp. 43-52, 1998.

[5] R. Burke, "Hybrid Recommender Systems: Survey and Experiments," User Modeling and User-Adapted Interaction, vol. 12, no. 4, pp. 331-370, 2002.

[6] W.W. Cohen, R.E. Schapire, and Y. Singer, "Learning to order things," J. Artificial Intelligent Research, vol. 10, no. 1, pp. 243-270, 1999.

[7] M. Deshpande and G. Karypis, "Item-Based Top-n Recommendation," ACM Trans. Information System, vol. 22, no. 1, pp. 143-177, 2004.

[8] A. Iosup, S. Ostermann, N. Yigitbasi, R. Prodan, T. Fahringer, and D. Epema, "Performance Analysis of Cloud Computing Services for Many-Tasks Scientific Computing," IEEE Trans. ParallelDistributed System, vol. 22, no. 6, pp. 931-945, June 2011.

[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, pp. 393–405, Sep. 2010.

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

[12] T. Wolverton. (2002, Mar. 26). *Hackers Attack eBay Accounts* [Online]. Available: http://www.zdnet.co.uk/news/networking/2002/03/26/hackers-attack-ebay-accounts-2107350/

[13] HP TippingPoint DVLabs, Vienna, Austria. (2010). *Top Cyber Security Risks Report, SANS Institute and Qualys Research Labs* [Online]. Available: http://dvlabs.tippingpoint.com/toprisks2010

[14] B. Pinkas and T. Sander, "Securing passwords against dictionary attacks," in *Proc. ACM CCS*, 2002, pp. 161–170.

[15] 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, pp. 235–258, 2006.

[16] M. Alsaleh, M. Mannan, and P. C. van Oorschot, "Revisiting defenses against large-scale online password guessing attacks," *IEEE Trans. Dependable Secure Computer.*, vol. 9, no. 1, pp. 128–141,Jan./Feb. 2012.
[17] 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.
[18] S. Chiasson, P. C. van Oorschot, and R. Biddle, "Graphical password authentication using cued click points," in *Proc. ESORICS*, 2007, pp. 359–374.

AUTHORS

Narendra Chaudhari, pursuing computer engineering at Genba Sopanrao Moze College of Engineering, Balewadi.

Sagar Handure, pursuing computer engineering at Genba Sopanrao Moze College of Engineering, Balewadi.

Mandar Pawar ,pursuing computer engineering at Genba Sopanrao Moze College of Engineering, Balewadi.

Prof.Sinju N.S.,Assistant Professor Department of computer engineering at Genba Sopanrao Moze College of Engineering, Balewadi.

.

