Captcha as A Graphical Password

Rohini R. Chaudhari[1], Gunjan Y. Chaudhari[2], Puja S. Bari[3]
[1, 2, 3] Dept of Computer Engineering
[1, 2, 3] SSBT College of Engineering and Technology Bambhori, Jalgaon

Abstract- *Most of the security primitives are based on hard mathematical problems. Use of hard AI problems for security is an exciting new paradigm. It has been under-explored. In this paper, we present a new security approach, Captcha as graphical passwords (CaRP), a novel family of graphical password systems built on top of Captcha technology. CaRP utilises both a Captcha and a graphical password scheme. CaRP addresses a number of security problems altogether, such as online guessing attacks, relay attacks and, when combined with dual-view technologies, it also addresses the shoulder-surfing attacks. Important thing is, a CaRP password can be found only probabilistically by automatic online guessing attacks even when the password is in the search set. PassPoints often leads to weak password choices. CaRP offers a novel approach to address the image hotspot problem in PassPoints. CaRP is not a universal remedy, but it offers reasonable security and usability and appears to fit well with some practical applications for improving online security.*

Keywords- Authentication, CaRP, color-based authentication scheme, dictionary attack, draw-a- secret, hybrid authentication scheme, shoulder surfing attack, 3D-password authentication scheme.

I. INTRODUCTION

Cyber security is information security, applied to computers and networks. This field covers all the processes and mechanisms by which computer-based equipment, information and services are protected from unintended or unauthorized access, change or destruction. Computer security also provide protection against unplanned events and natural disasters. In the computer industry, the term computer security refers to techniques that ensures that data stored in a computer cannot be access by any unauthorized individuals. Commonly, computer security techniques involve data encryption and passwords. Data encryption is the process of translating the plain-text data into a form of cipher-text data which is not readable without a deciphering algorithm. A password is a secret key that permits a user to access a particular program or system.

Online dictionary attacks on passwords is a major security threat for various online services. This threat is considered as a top cyber security risk. Providing security to online dictionary attacks is a more subtle problem than it might appear. Intuitive countermeasures such as throttling logon attempts do not work well for two reasons:

1. It causes denial-of-service attacks (which were exploited to lock highest bidders out in final minutes of eBay auctions) and incurs expensive helpdesk costs for account
   reactivation.
1. It is vulnerable to global password attacks whereby adversaries intend to break into any account rather than a specific one, and thus try each password candidate on multiple accounts and ensure that the number of trials on each account is below the threshold to avoid triggering account lockout.

II. LITERATURE SURVEY

P. C. van Oorschot and J. Thorpe[2]: In , ``On predictive models and user drawn graphical passwords", ACM Trans. Inf. Syst. Security, vol. 10, no. 4, pp. 133, 2008, 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 41a 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.

A. E. Dirik, N. Memon, and J.-C. Birget[5]: In ``Modeling user choice in the passpoints graphical password scheme", in Proc. Symp. Usable Privacy Security, 2007, pp. 2028, develop a model to identify the most likely regions for users to click in order to create graphical passwords in the PassPoints system. A PassPoints 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 PassPoints 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.

III. PROPOSED SYSTEM

Proposed system is a *Captcha as graphical passwords (CaRP), a novel family of graphical password systems built on top of Captcha technology*. CaRP is both a Captcha and a graphical password scheme. CaRP addresses a number of security problems altogether, such as online guessing attacks, relay attacks and, when combined with dual-view technologies, it also addresses the shoulder-surfing attacks.

With reference to literature work, Identification is a process to determine an unknown individual out of many. All authentication systems necessitate some form of ID for user identification, these are text-based login ID, fingerprint, or facial image. Then in the verification process, the system asks a evidence of the ID since the system does not know whether the user is the permissible ID holder. The proposed solution introduces a new security mechanism by using user authentication, device authentication to authenticate the user.

In proposed system following assumptions are made.

1. The authentication methods involve a multidimensional grid.
2. The color selection is in even color based method.
3. The secret password is even and more than 4 digits in hybrid method.

In proposed system following schemes are presented:

a. 3D Password Authentication Scheme:

A method called Cued Clicked Points(CCP) is implemented under the 3D Password Au-thentication Scheme. Here the user will be provided with images, amongst which he has to select one and make clicks anywhere on the image. These clicks are saved as password.

b. Color Based Authentication Scheme:

In Color Based Authenticatiton Scheme, at the time of registration, the user gives numbers(1to8) to colors in the color grid. In primary level authentication, when the user selects the color based authentication scheme, an interface is displayed. The interface composed of 8X8 number grid in which numbers from 1 to 8 are placed randomly. With 8X8 numer grid, a color grid is also displayed containing 4 pairs of colors. For every session, both these grids are different. The logic involved in this scheme is that the rating given to the first color of every pair represents a row and the rating given the second color in that pair represents a column of the 8X8 number grid. The number in the intersection of the row and column of the grid is the part of session password. This procedure is repeated for the remaining color pairs in the color grid.

c. Hybrid Authentication Scheme:

In the Hybrid Authentication Scheme, at the time of registration the user submits the secret password. The minimum length of the secret password is 8 and it should contain even number of characters. During the primary level authentication, when the user chooses the hybrid authentication scheme, an interface consisting of 6X6 grid is displayed. The grid contains both alphabets and numbers which are placed at random and the interface changes every time.

The mechanism involved in the hybrid authentication scheme is as follows: Firstly, the user has to consider the secret password in terms of pairs. The first letter in the pair of secret password selects the row and the second letter selects the column in the 6X6 grid. The intersection letter of the selected row and column generates the character which is a part of the session password. In this way, the logic is repeat for all other pairs in the secret password. Thereafter, the password inputted by the user i.e. the session password is now verified by the server to authenticate the user.

d. Pattern Matching Authentication Scheme:

In Pattern Matching Authentication Scheme, the user has to draw a sequence, known asthe pattern joining the dots. If the sequence drawn during authentication matches with the sequence drawn during the registration phase, then the user is given the permission to access the confidential files.

IV. RESULT AND DISCUSSION

Experimental result present the effectiveness of proposed system, in which involvement ofauthentication methods is proved better by carrying out experiments. Results are carried out using java. In proposed system Time consumed by each algorithm at different steps and also total time and average time for complete algorithm execution is considered. The results are taken by executing the algorithms with all combinations and average of ten iterations are taken into consideration. Below Results show verification and validation time required by each algorithm at each step.

Table shows time comparision of authentication methods. All values provided are in seconds. The proposed approach was evaluated by an experimental results in which included 5 users. The users are various technical and non-technical backgrounds, of different ages ranging from twenty to fourty years. The primary experimental objective was to evaluate the recognition success rate of the proposed method dependent on the size of target group population and also in comparison to traditional algorithm. Every participant accomplish ten repetitions of all three selected algorithms, so that 15 steps per user were recorded in total.

Table 1: Time Comparision of Authentication Methods

User No.	Text Pass-word	3D Pass-word	Color Pass-word	Hybrid Pass-word	Patt-ern	OTP	Encryp-tion
User1	0.02	0.01	0.033		0.12	15	0.05
User 2	0.01	0.02		0.042	0.17	10	0.059
User 3	0.01	0.01	0.25		0.16	20	0.59
User4	0.02	0.01		0.05	0.15	30	0.39
User 5	0.02	0.02	0.19		0.11	25	0.55
Average Time	0.016	0.157	0.46	0.142	20	0.3278	

The test was not evaluated sequentially but rather over a longer period of time (15mins) and with pauses in order to provide additional variability and to obtain more realistic study results. The users were seated while performing the test, but were not influenced in any other way. User time consumed is expressed as a time required performing all algorithm steps.

Advantages of proposed system:

a. CaRP protects system against online dictionary attacks on passwords, which have been for long time a major security threat for various online services.
b. CaRP also provides protection against relay attacks, which is an increasing threat to bypass Captchas protection.

V. CONCLUSION AND FUTURE SCOPE

Generally, there are many drawbacks related to the textual passwords which includes brute-force attacks and dictionary attacks. Similarly the graphical passwords includes shoulder-surfing attacks. The graphical passwords are very expensive to implement.

We have proposed CaRP, a *Captcha as graphical passwords, a novel family of graphical password systems. CaRP utilises both a Captcha and a graphical password scheme. We can* improved the usability of CaRP by using images of different levels based on the user login history and the machine used to log in. Of reasonable security and usability and practical applications, CaRP has good potential for refinements, which call for useful future work.

In future, it would be a point of research that how to increase security by using better user interface. By combining this algorithms with more famous algorithms, we get better security and less time consumption.

VI. ACKNOWLEDGMENT

The satisfaction that accompanies the successful completion of any task would be incomplete without the mention of people whose ceaseless cooperation made it possible, whose constant guidance and encouragement crown all efforts with success. Our sincere thanks to the Principal Prof. Dr. Kishor S. Wani, Shram Sadhana Bombay Trusts College of Engineering Technology, for providing us facilities and resources to complete project work. Our deepest thanks to the project guide, Prof. Dr. Girish K. Patnaik, Head of Computer Department for guiding and correcting our various project documents with utmost attention and care. Thanks and

appreciation to the parents for their invaluable support. We are highly obliged to the entire staff of Computer Department for their kind help and co-operation. We also take this opportunity to thank all our friends for offering all possible help.

REFERENCES

[1] L. von Ahn, M. Blum, N. J. Hopper, and J. Langford, ``CAPTCHA : Using hard AI problems for security", in Proc. Eurocrypt, 2003, pp. 294311.

[2] P. C. van Oorschot and J. Thorpe, ``On predictive models and user drawn graphical passwords", ACM Trans. Inf. Syst. Security, vol. 10, no. 4, pp. 133, 2008.

[3] M Sreelatha, M Shashi, M Anirudh, MD Sultan Ahamer,V Manoj Kumar, ``Authentication Schemes for Session Passwords using Color and Images", International Journal of Network Security and Its Applications (IJNSA),Vol.3, No.3,May2011.

[4] Mr.Sagar Kambale,Mr.PramodKamble, Mr.Yogesh Dhavan,Ms.Dipali Mahajan, Ms.Renuka Jadhav, ``CAPTCHA as graphical passwords", International Research Journal of Engineering and Technology (IRJET), Vol. 03, May-2016.

[5] 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. 2028.