Design and Implementation of Captcha with Click Point Authentication based on Hard AI Problems

A Blessy,
Freelancing in Information Security related Projects,
Tirunelveli, Tamil Nadu, India
blessy2789@gmail.com

Varun Chand,
Asst: Professor in Department of Information Technology,
College of Engineering and Management,
Alappuzha, Kerala, India
varunchand123@gmail.com

Binitha V Nair,
Assistant Professor in Department of Computer Science,
K R Gouri Amma College of Engineering for Women,
Alappuzha, Kerala, India
meetbinitha@gmail.com

Abstract : A fundamental task in security is to create cryptographic primitives based on hard mathematical problems that are computationally intractable Using hard AI problems for security is emerging as an exciting new paradigm, but has been underexplored. Here, we present a new security primitive based on hard AI problems, which we call Captcha in Click Point Authentication (C-CPA) from Captcha as Recognition based graphical passwords (CaRGP). CaRGP is both a Captcha and a Recognition based Graphical password scheme. C-CPA from CaRGP addresses a number of security problems altogether, such as online guessing attacks, relay attacks, and, if combined with dual-view technologies, shoulder-surfing attacks. Notably, a CaRGP password can be found only probabilistically by automatic online guessing attacks even if the password is in the search set. It also address the well-known image hotspot problem, such as PassPoints, that often leads to weak password choices. C-CPA from CaRGP offers reasonable security, usability and appears to fit well with some practical applications for improving online security.

Keywords: CAPTCHA(Completely Automated Public Turing tests to tell Computers and Humans Apart),C-CPA(Captcha in Click Point Authentication), CaRGP(Captcha and a Recognition based Graphical password), AI(Artificial Intelligence).

I. INTRODUCTION

Today for many organizations they need to store their enormous amount of data. Among these, cloud computing is the most cost effective and flexible network storage providers but it has some security issues. Cloud computing provide accuracy, so more data can be centralized into the clouds. The most important a security concern in cloud is the security due to internet based data storage and management. A fundamental task in security is to create cryptographic primitives based on hard mathematical problems that are computationally intractable. Using hard AI (Artificial Intelligence) problems for security, initially proposed, is an exciting new paradigm. Under this paradigm, the most notable primitive invented is Captcha, which distinguishes human users from computers by presenting a challenge, i.e., a puzzle, beyond the capability of computers but easy for humans. Captcha is now a standard Internet security technique to protect online email and other services from being abused by bots. This paper focuses on the survey of different authentication and CAPTCHA schemes. Section II presents the literature survey of different authentication and CAPTCHA schemes and section III concludes with discussions.

II. LITERATURE SURVEY

In cloud computing, there are different existing schemes that provide security. Users need to share sensitive objects with others based on the recipients' ability to satisfy a policy in distributed systems. The security schemes are authentication and CAPTCHA. One of the authentication scheme is Graphical based password schemes and captcha scheme is Text Captcha. The existing Authentication schemes are of three types. They are Token based

authentication, Biometric based authentication and Knowledge based authentication. The existing captcha techniques are Text captcha, EZ-Gimpy and asirra.

Token Based Authentication - Token based techniques, such as key cards, bank cards and smart cards are widely used. Many token-based authentication systems also use knowledge based techniques to enhance security. For example, ATM cards are generally used together with a PIN number.

Biometric Based Authentication - Biometric based authentication techniques, such as fingerprints, iris scan, or facial recognition, are not yet widely adopted. The major drawback of this approach is that such systems can be expensive, and the identification process can be slow and often unreliable. However, this type of technique provides the highest level of security.

Knowledge Based Authentication - Knowledge based techniques are the most widely used authentication techniques and include both text-based and picture-based passwords. The picture-based techniques can be further divided into two categories: recognition-based and recall-based graphical techniques. Using recognition-based techniques, a user is presented with a set of images and the user passes the authentication by recognizing and identifying the images he or she selected during the registration stage. Using recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage.

CAPTCHA: Using Hard AI Problems For Security - A captcha is a program that can generate and grade tests that: (A) most humans can pass, but (B) current computer programs can't pass. Such a program can be used to differentiate humans from computers and has many applications for practical security, including

- Online poll
- Free email services
- Search engine bots

Avoid worms, spams and online dictionary attacks. A captcha is a cryptographic protocol whose underlying hardness assumption is based on an AI problem.

Distortion Estimation Techniques in Solving Visual CAPTCHA - Here a correlation algorithm is developed, that correctly identifies the word in an EZ-Gimpy challenge image 99% of the time and a direct distortion estimation algorithm that correctly identifies the four letters in a Gimpy-r challenge image 78% of the time.

Asirra: A CAPTCHA that Exploits Interest Aligned Manual Image Categorization - Asirra, a CAPTCHA that asks users to identify cats out of a set of 12 photographs of both cats and dogs. Asirra is easy for users; user studies indicate it can be solved by humans 99.6% of the time in under 30 seconds. Barring a major advance in machine vision, we expect computers will have no better than a 1/54,000 chance of solving it.

Against spyware using CAPTCHA in graphical password scheme - A new approach had been to protect user's password against spyware attack by introducing CAPTCHA into the realm of graphical passwords. But, as long as the state-of-art-algorithms cannot solve the hard AI problems, it is probable to construct a graphical password. Here users are allowed to select their own graphical password images (pass-images). To be authenticated, the user only needs to distinguish his/her pass-images from decoy images and then enter certain parts of the CAPTCHAs string below the pass-images. The CAPTCHA is an image of distorted string randomly generated by system.

A new CAPTCHA interface design for mobile devices - A CAPTCHA is a computer-based security test used to distinguish human users from artificial users, preventing automated abuse of networked resources. As mobile network services improve, we can anticipate that future mobile network services will come under attack from automated programs. A new CAPTCHA approach is then introduced here which is intended specifically for mobile devices.

III. DESIGNING CAPTCHA IN CLICK POINT AUTHENTICATION FROM Ca-RGP

Knowledge based Authentication - Knowledge based techniques are the most widely used authentication techniques and include both text-based and picture-based passwords. The picture-based techniques can be further divided into two categories: recognition-based and recall-based graphical techniques. Using recognition-based techniques, a user is presented with a set of images and the user passes the authentication by recognizing and identifying the images he or she selected during the registration stage. Using recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage. Overall, it is believed that it is more difficult to break graphical passwords using the attacks comparing to text based password as its password space is smaller than graphical password.

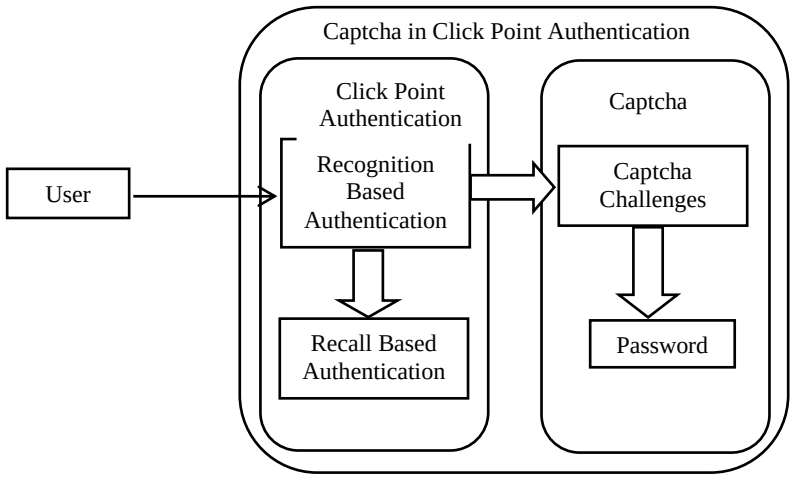

Fig 1 Captcha in Click Point Authentication

Operation of Knowledge Based Authentication

-Recognition based Authentication

-Image Recognition

-Pixel part Recognition

-Recall based Authentication

-Pixel Point Generation

-Authentication of anonymous user

Click Point Authentication - Click Point Authentication is a knowledge based authentication. It is a combined structure of recall based and recognition based authentication, used for increasing the password space and resistance against attacks. Here owners and users are registering their account and creating password using recognition based in which they are selecting an image as a password and then using recall based they are clicking on a pixel part of the image using mouse to generate a coordinates which is also added as the password. As soon as the recall based password is generated it will be send to the user's email id. It is believed that it is more difficult to break graphical passwords using attacks such as brute force, dictionary, guessing, spyware, shoulder surfing, social engineering attacks. This has N!/K!(N-K)! (N is the total number of picture objects/pictures; K is the number of pre-registered objects/selected images).

Pseudo Random code Generation - A PRKG is an algorithm for generating a sequence of numbers that approximates the properties of random numbers. The sequence is not truly random in that it is completely determined by a relatively small set of initial values, called the PRKG's state, which includes a truly random seed. The numbers are important in practice for their speed in number generation.

Pseudo code of PRKG - Linear Congruential Generator

LCG represents one of the oldest, easiest, fastest and best-known pseudorandom number generator algorithms. The generator is defined by the recurrence relation:

$X_{n+1} \cong (aX_n + c) \pmod m$

where X_n is the sequence of pseudorandom values, and

m, $0 < m$ – the "modulus"

a, $0 < a < m$ – the "multiplier"

c, $0 \leq c < m$ – the "increment"

X_0, $0 \leq X_0 < m$ – the "seed" or "start value" , are integer constants that specify the generator.

If $c = 0$, the generator is often called a multiplicative congruential method, or Lehmer RNG. If $c \neq 0$, the generator is called a mixed congruential method.

Captcha - A CAPTCHA (Completely Automated Public Turing tests to tell Computers and Humans Apart) is a program that generates and grades tests that are human solvable, but are beyond the capabilities of current computer programs. Here it is a sequence of clicks on an image, which is used to derive a password. Here a new CaRP image code is generated for every login attempt.

IV. PERFORMANCE ANALYSIS

Performance Analysis of captcha

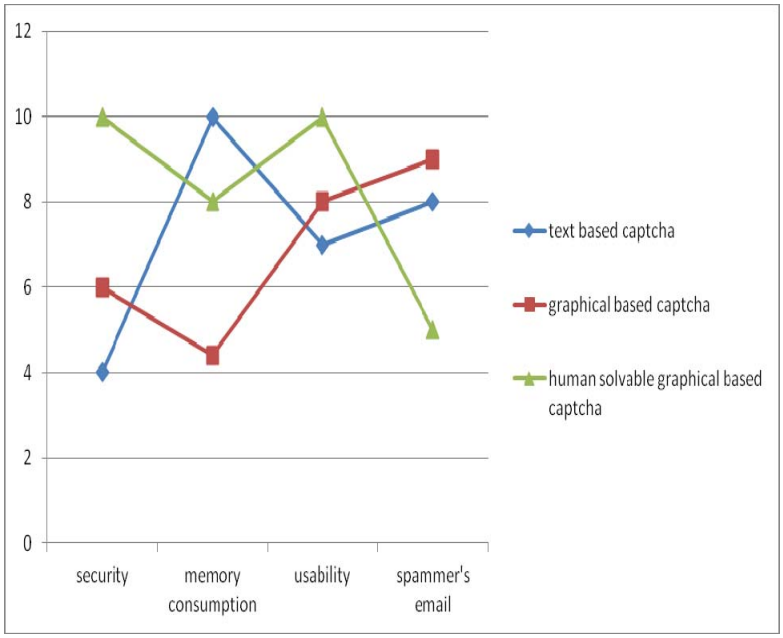

Fig 2 Performance Analysis of Captcha

Performance Analysis of CPA

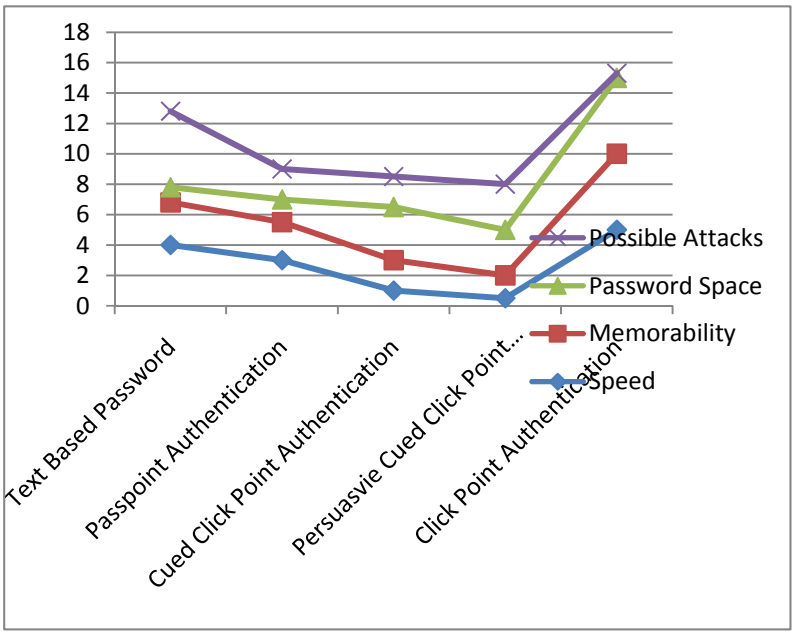

Fig 3 Performance Analysis of CPA

V. CONCLUSION

A Captcha in Click Point Authentication(C-CPA) from Captcha as Recognition based graphical passwords **(**CaRGP) is proposed and implemented to overcome all those security and privacy issues with high password space, less memory consumption, Secure login by avoiding all possible attacks like shoulder surfing, spyware, guessing, dictionary attacks, etc.,). It also avoids spammer's from mailing us by increasing the operating cost. It can also be used in touch screen devices.

VI. 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] 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.

[3] H. Tao and C. Adams, "Pass-Go: A proposal to improve the usability of graphical passwords," Int. J. Netw. Security, vol. 7, no. 2, pp. 273–292, 2008.

[4] 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.

[5] P. C. van Oorschot and J. Thorpe, "On predictive models and userdrawn graphical passwords," ACM Trans. Inf. Syst. Security, vol. 10, no. 4, pp. 1–33, 2008.

[6] K. Golofit, "Click passwords under investigation," in Proc. ESORICS, 2007, pp. 343–358.

[7] 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. 20–28.

[8] 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.

[9] 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.

[10] P. C. van Oorschot and J. Thorpe, "Exploiting predictability in click based graphical passwords," J. Comput. Security, vol. 19, no. 4, pp. 669–702, 2011.

[11] 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/

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

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

[14] 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.

[15] M. Alsaleh, M. Mannan, and P. C. van Oorschot, "Revisiting defenses against large-scale online password guessing attacks," IEEE Trans. Dependable Secure Comput., vol. 9, no. 1, pp. 128–141, Jan./Feb. 2012.

[16] 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.

[17] S. Chiasson, P. C. van Oorschot, and R. Biddle, "Graphical password authentication using cued click points," in Proc. ESORICS, 2007, pp. 359–374.

[18] S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot, "Influencing users towards better passwords: Persuasive cued click-points," in Proc. Brit. HCI Group Annu. Conf. People Comput., Culture, Creativity, Interaction, vol. 1. 2008, pp. 121–130.

[19] D. Davis, F. Monrose, and M. Reiter, "On user choice in graphical password schemes," in Proc. USENIX Security, 2004, pp. 1–11.

AUTHOR PROFILE

Blessy recieved B.E in Computer Science and Engineering from Scad College of Engineering and Technology, Anna University, M.Tech in Computer Science and Engineering from Hindustan University. She worked as an Assistant Professor in Department of Computer Science and Engineering, Scad Engineering College. She is currently Freelancing in Information Security related projects in Tirunelveli, Tamil Nadu, India.

Varun Chand is Assistant Professor in Department of Information Technology at College of Engineering and Management, Punnapra, Alappuzha, Kerala (India). He took B.Tech in Information Technology from Mahatma Gandhi University, M.Tech in Computer Science and Engineering from Karunya University, and MBA in Human Resourse and Management from Mahatma Gandhi University.

Binitha is Assistant Professor in Dept. of Computer Science and Engineering at K R Gouri Amma College of Engineering for Women, Cherthala, Kerala (India). She took M.Tech in Computer and Information Science from M S University.