GRAPHICAL PASSWORDS EFFECTS FOR TOLERANCE PASSWORD,IMAGECHOICE, AND OTP LOGIN SECURITY.

Mary Harin Fernandez F[1],Sangeetha M[2],Shanmugapriya T K[3]

[1]*Department of Computer Science and Engineering,JEPPIAAR SRR Engineering College,Padur,Chennai:603103*

[2]*Department of Computer Science and Engineering,JEPPIAAR SRR Engineering College,Padur,Chennai:603103*

[3]*Department of Computer Science and Engineering,JEPPIAAR SRR Engineering College,Padur,Chennai:603103*

Email Id:mary.fherin@gmail.com,*priyakumar794@gmail.com,sangeethamahendran747@gmail.com*

ABSTRACT:

Many security primitives are based on hard mathematical problems. Using hard AI problems for security is emerging as an exciting new paradigm, but has been underexplored. In this paper, we present a new security primitive based on hard AI problems, namely a novel family of graphical password systems built on top of Puzzle technology, which we call Puzzle as graphical passwords (CaPRP). CaPRP is both a Puzzle and a graphical password scheme. CaPRP 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 CaPRP password can be found only probabilistically by automatic online guessing attacks even if the password is in the search set. CaPRP also offers a novel approach to address the well-known image hotspot problem in popular graphical password systems such as PassPoints, that often leads to weak password choices. CaPRP is not a panacea, but it offers reasonable security and usability and appears to fit well with some practical applications for improving online security.

Keywords: CaPRP, Shoulder-surfing attack, Guessing attacks, Relay attacks.

1.INTRODUCTION:

Secure access to information underpins modern digital systems and services. We keep our communications, financial data,work documents, and personal media safe by providing identity information and then authenticating to that identity. Text passwords and personal identification numbers (PINs) are the dominant authentication method as they are simple and can be deployed on systems. However, passwords suffer from limitations in terms of memorability and security passwords that are difficult to guess are also hard to remember .This is a major problem as an average user possesses 25 online accounts secured with up to six different passwords and representing a substantial memory burden. . In order to mitigate these

problems, researchers have proposed *graphical password* schemes that rely on input such as selecting portions of an image. These systems have been shown to improve memorability without sacrificing input time or error rates while also maintaining a high resistance to brute force and guessing attaks password systems built Graphical on top of Puzzle technology, which we call Puzzle as graphical passwords (CaPGP) .CaPGP is both a Puzzle and a graphical password scheme. CaPGP addresses a number of security problems altogether, such as online guessing attacks, relay attacks. It offers reasonable security and usability and appears to fit well with some practical applications for improving online security. Security primitives are based on hard mathematical problems. Using hard AI problems for security is emerging as an exciting new paradigm, but has been unexplored.**A** Fundamental task in security is to create cryptographic primitives based on hard mathematical problems that are computationally intractable.

2.RELATED WORK:

We present a new security primitive based on hard AI problems, namely, a novel family of graphical password systems built on top of Puzzle technology which we call Puzzle as graphical passwords (CaPRP). CaPRP is both a Puzzle and a graphical password scheme. CaPRP addresses a number of security problems altogether, such as online guessing attacks, relay attacks, and, if combined. We present exemplary CaPRPs built on both text Puzzle and image-recognition Puzzle. One of them is a text CaPRP wherein a password is a sequence of characters like a text password, but entered by clicking the right character sequence on CaPRP images. CaPRP offers protection against online dictionary attacks on passwords, which have been for long time a major security threat for various online services. This threat is widespread and considered as a top cyber security risk. Defense against online dictionary attacks is a more subtle problem than it might appear.

2.1.RANDOM CAPTCHA SELECTION

A CAPTCHA is a test that is utilized to separate people and machines. CAPTCHA remains for "Totally Automated Turing test to differentiate Computers and Humans One from the other." It is regularly a picture test or a basic arithmetic issue which a human can read or unravel

2.2.ONE TIME PASSWORD

An OTP is more secure than a static password, especially a user-created password, which is typically weak. OTPs may replace authentication login information or may be used in addition to it, to add another layer of security.

2.3ONLINE BANKING

E-keeping money, or virtual managing an account, is an electronic installment framework that empowers clients of a bank or other to direct a scope of budgetary exchanges through the monetary organization 's site.

3.PROBLEM DEFINITION :

This paradigm has achieved just a limited success as compared with the cryptographic primitives based on hard math problems and their wide applications. Using hard AI (Artificial Intelligence) problems for security, initially proposed is an exciting new paradigm. Under this paradigm the most notable primitive invented is Puzzle, which distinguishes human users from computers by presenting a challenge.

4.IMPLEMENTATION

ALGORITHMS/TECHNIQUES USED:

I. *BUBBLESORT ALGORITHM:*

The security and usability problems in text- based Login And password schemes have resulted in the development of Puzzle password schemes as a possible alternative.
Step1:We can visualize the sum 1+2+3+...+n as a triangle of character .
Step 2: Numbers which have such a pattern of character are called Triangle (or triangular) numbers, written T(n), the sum of the integers from 1 to n time Using Factorial base Login Puzzle Solving.
Step 3: The formula used is n(n-1) where n is the number of characters used in the password.
Step 4: The probability will be used for shuffling the password
Step5: At each login the password will be shuffle

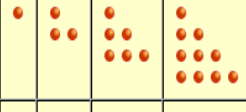
n	1	2	3	4	5	6
T(n) as a sum	1	1+2	1+2+3	1+2+3+4	1..5	1..6
T(n) as a triangle						
T(n)=	1	3	6	10	15	21

Table1: table for bubble sort

II. IMAGE SHUFFLING:

A CAPTCHA is a test that is used to separate humans and machines. CAPTCHA stands for "Completely Automated Turing test to tell Computers and Humans Apart." It is normally an image test or a simple mathematics problem which a human can read or solve, but a computer cannot. It is made to stop computer hackers from using a program to automatically set up hundreds of accounts, such as email accounts. Each individual is chosen randomly and entirely by chance, such that each individual has the same probability of being chosen at any stage during the sampling process, and each subset of n individuals has the same probability of being chosen for the sample as any other subset of n individuals This process and technique is known as simple random sampling, and should not be confused with systematic random sampling. A simple random sample is an unbiased surveying technique
1:Read the c1.x class
2:Reapeat
3:Randomly choose a small y
4:Decrypt c1x.class with y into class c0x.class
5:Load class c0x.class
6:Invoke c0x.class to obtain m and further x=c0(y,m)
7:until x=x
8:output(x,y)

III. AES ENCRYPTION:

When a software puzzle is built upon a data puzzle, the number of software puzzles is required to be very large such that an attacker is unable to re-construct the GPU-version software puzzles in advance and re-use them. Indeed, this requirement can be easily satisfied. For instance, even though a service provider merely adds one AES round transformation between two AES transformations in the standard 10 rounds, the number of AES variants is up to 49×4+3 = 278. Moreover, a software can have many polymorphic codes such that the number of software puzzles is even larger. Unfortunately, a smart adversary may

collect all the code blocks in the warehouse W,and rebulid the GPU version code block software puzzle is delivered to the adversary, he will reconstruct the GPU-version puzzle by matching the puzzle code blocks against the software puzzle.

ARCHITECTURE:

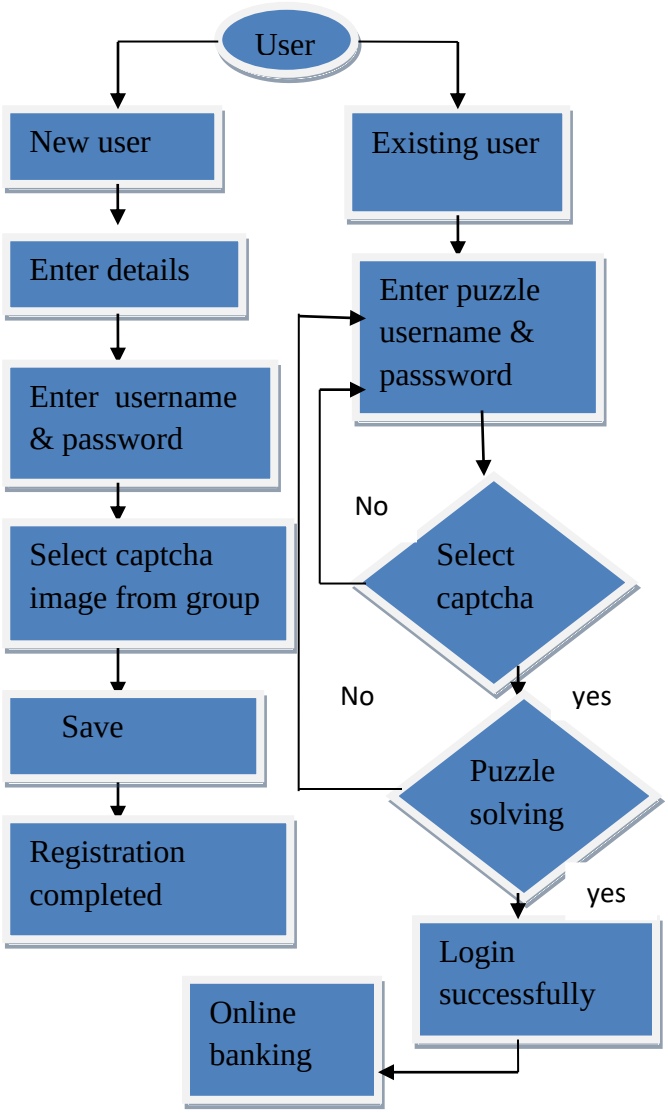


Fig 2:Login image puzzle solving using AES algorithm

5. Security Issues

5.1 Brute Force Attack

Brute force the main defense against search is to have a sufficiently large password space. Text-based passwords have a password space of 94^N, where N is the length of the password, 94 is the number of printable characters excluding SPACE. Some graphical password techniques have been shown to provide a password space similar to or larger than that of text-based passwords. Recognition based graphical passwords tend to have smaller password spaces than the recall based methods. It is more difficult to carry out a brute force attack against graphical passwords than text-based passwords.

5.2 Dictionary Attack

Since recognition based graphical passwords involve mouse input instead of keyboard input, it will be impractical to carry out dictionary attacks against this type of graphical passwords. Overall, graphical passwords are less vulnerable to dictionary attacks than text-based passwords.

5.3 Guessing Attack

Unfortunately it seems that graphical passwords are often predictable, a serious problem typically associated with text-based passwords. For example, studies on the Passface technique have shown that people often choose weak and predictable graphical passwords. Nali and Thorpes study revealed similar predictability among the graphical passwords created with the DAS technique. More research efforts are needed to understand the nature of graphical passwords created by real world users.

5.4 Social Engineering Attack

Comparing to text based password, it is less convenient for a user to give away graphical passwords to another person. For example, it is very difficult to give away graphical passwords over the phone. Setting

up a phishing web site to obtain graphical passwords would be more time consuming.

6.EXPERIMENTAL RESULT

The workload data are shown in Fig. 3. These show a general trend for reduced workload in the private image condition, an observation borne out by a significant difference in the summed measure of Overall Workload. To protect against alpha inflation, we do not report results for the component workload measures.

Functional characteristics	System image	User image
Median creation time	8	7
Median login time	6	7.5
Physical	3	2
Performance	8	6
Successful login within 3 trials	100%	100%
Successful login at first trial	100%	85%
Successful login at second trial	-	100%

Table 3:results in usability mode

.

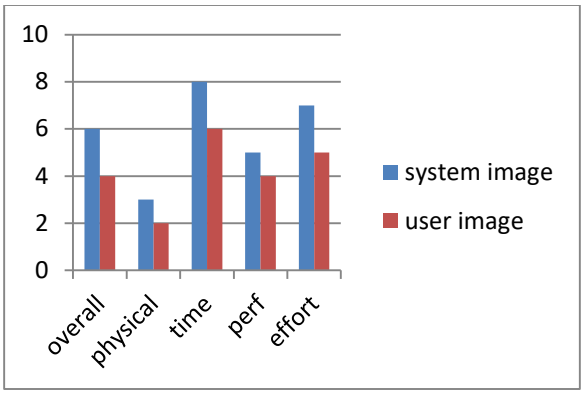


Fig4:data showing workload in usability study

Participants also rated ease of creating passwords with the private and public images and memorability of the private and public images respectively. These related measures were analyzed using repeated-measure Manova. These subjective data favor the private image condition over the public image condition.

Assume the time to perform one RSA decryption be $t0$, and the time to generate and verify one software puzzle be ts (Note that $t0 > ts$, otherwise, software puzzle is useless). Suppose the number of attacker's requests be na, and the number of genuine client requests be nc, the server's computational time required for replying all the requests is $\tau 1 = (na + nc) \times t0$ if there is no software puzzle; otherwise, $\tau 2 = (na + nc) \times ts + nc \times t0$ given that the adversary does not return valid solutions to the puzzles. Thus, software puzzle defense is effective if $\tau 1 \geq \tau 2$, *i.e.*, $na \geq ts\ t0 - ts\ nc$. That is, when the number of malicious requests na is greater than $ts\ t0 - ts\ nc$, the genuine clients spend less time in waiting for the services. Hence, a good strategy is to initiate the software puzzle defense if the number of requests is beyond a threshold, otherwise, no defense is required because quality of service is satisfactory for all clients.

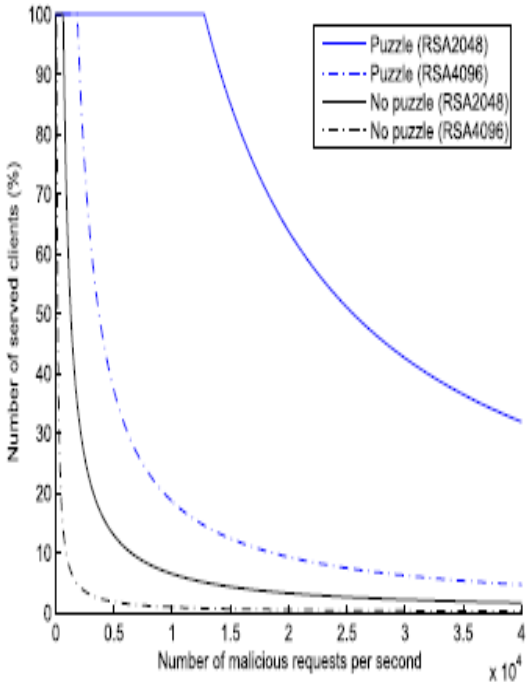


Fig 5:Service capability comparison of server with/without software puzzle for RSA2048 ,assume that the request rate of attacker is 20 times of that of honest clients.

6. Conclusion :

This system aims to provide addition layer of security to the normal authentication system by using graphical password scheme. Additionally, it provides accessibility to visually impaired users. This system tries to avoid shoulder surfing attack, dictionary attack, brute force attack, guessing attack by generating one time password. This one time password is sent to users email id from a database. The user must click on the sent items on the image provided in order to be authenticated. It requires large number of images in order to be secure and this will actually slow down the user authentication process.

7. Future Work :

This system can be extended by sending the one time password to users *whatsapp* account for authentication. Future work could include a user study with larger and more varied participants to validate the collected results and a more detailed analysis of this scheme.

REFERENCES

[1] A. Adams and M. Sasse, "Users are not the enemy," *Commun. ACM*, vol. 42, pp. 40–46, 2013.

[2] M. Adham, A. Azodi, Y. Desmedt, and I. Karaolis, "How to attack twofactor authentication internet banking," in *Proc. 17th Int. Conf. Financial Cryptography*, 2013, pp. 322–328.

[3] ARTigo, http://www.artigo.org/.

[4] F. Aloul, S. Zahidi, and W. El-Hajj, "Two factor authentication using mobile phones," *Proc. Comput. Syst. Appl.*, 2009, pp. 641–644.

[5] R. Biddle, S. Chiasson, and P. van Oorschot, "Graphical passwords: Learning from the first twelve years," *ACM Comput. Surveys* vol. 44, no. 4, p. 19, 2012.

[6] G. E. Blonder, "Graphical passwords," U.S. Patent 5 559 961, 1996.

[7] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," in *Proc. IEEE Symp. Security Privacy*, 2012, pp. 553–567.

[8] S.Chiasson, R. Biddle, and P. van Oorschot, "Asecond look at the usability of click-based graphical passwords," in *Proc. 3rd Symp. Usable Privacy Security*, 2007, pp. 1–12.

[9] S. Chiasson, P. C. van Oorschot, and R. Biddle, "Graphical password authentication using cued click points," in *Proc. 12th Eur. Symp. Res. Comput. Security*, 2007, pp. 359–374.

[10] S. Chiasson, A. Forget, R. Biddle, and P. C. Oorschot, "User interface design affects security: Patterns in click-based

graphical passwords, *Int. J. Inf. Security*, vol. 8, no. 6, pp. 387–398, 2009.
[11] S. Chiasson, E. Stobert, A. Forget, R. Biddle, and P. C. Van Oorschot, "Persuasive cued click-points: Design, implementation, and evaluation of a knowledge-based authentication mechanism," *IEEE Trans. Dependable Secure Comput.*, vol. 9, no. 2, pp. 222–235, Mar./Apr. 2012.
[12] A. De Luca, E. von Zezschwitz, N. D. H. Nguyen, M. Maurer, E. Rubegni,M. P. Scipioni, and M. Langheinrich, "Back-of-device authentication on smartphones," in *Proc. SIGCHI Conf. Human Factors Comput. Syst.*, 2013, pp. 2389–2398.
[13] B. Dodson, D. Sengupta, D. Boneh, and M. S. Lam, "Secure, consumerfriendly web authentication and payments with a phone," in *Proc. 2nd Int. ICST Conf. Mobile Comput., Appl., Serv.*, 2010, pp. 17–38.
[14] K. M. Everitt, T. Bragin, J. Fogarty, and T.Kohno, "A comprehensive study of frequency, interference, and training of multiple graphical passwords," in *Proc. SIGCHI Conf. Human Factors Comput. Syst.*, 2009, pp. 889–898.
[15] A. Gelman, J. Hill, andM. Yajima, "Why we (usually) don't have to worry about multiple comparisons," *J. Res. Educ. Effectiveness*, vol. 5, no. 2, pp. 189–211, 2012.
[16] A. Forget, S. Chiasson, and R. Biddle, "Shoulder-surfing resistance with eye-gaze entry in cued-recall graphical passwords," in *Proc. SIGCHIConf. Human Factors Comput. Syst.*, 2010 pp. 1107–1110.
[17] D. Florencio and C. Herley, "A large-scale study of web password habits," in *Proc. 16th Int. Conf. World Wide Web*, 2007, pp. 657–666.
[18] S. Hart and L. Staveland, "Development of a multi-dimensional workload