CAPCHA AS OTP– A NEW SECURITY PRIMITIVE BASED ON CRITICAL AI PROBLEM

Nimbalkar Chaitrali M, Khomane Madhuri D, Kokare Monika D, Mr.Shinde V. D.
Department of Computer Engineering, Savitribai Fule Pune University, Pune, India
coesomeshwar@gmail.com
SSPM's Someshwar Engineering College (www.sspms.org)
Somwshwarnagar, Tal- Baramati, Dist- Pune, 412306
chaitralinimbalkar111@gmail.com, mkhomane1@gmail.com, monikakokare1@gmail.com

Abstract

Critical mathematical problem are based on security primitives emerging as an exciting new paradigm but has been under explored for security using critical AI problem. In our proposed work we present a CAPTCHA has OTP(One Time Password). New security primitive an critical AI problem a novel family of graphical password system make on TOP of CAPTCHA technology that is called as CAPTCHA as graphical password (CaRP).In CaRP CAPTCHA and graphical password are mainly required. In CaRP various security problem such as online guessing attack, relay attack and dual view technology shoulder surfing attacks etc. And automatic online guessing attack even if the password is in the search set, found password with the help of probability CaRP are provide a reasonable security and usability and appears to fit well with some practical application for improve the online security.

Keywords: Graphical Password, CaRP, CAPTCHA, Password guessing attack, Dictionary attack and Primitive Security.

I. Introduction:

In our proposed work CAPTCHA generate automated test for security if any application human can pass data but computer program as CAPTCHA can't pass without authentication as to solve the critical AI problem. Email Services uses CAPTCHA of our design to prevent the bots from registering for account as distorted word(text captcha) as only intelligent human understand and bots are used for stop viewing information about user. CAPTCHA is a cryptographic protocol to prevent the dictionary attack ,relay attack in password system. An approach familiar to cryptographers used for investigating the state_of_the_art algorithm for primitives security. Text_based password schema have resulted in the development of graphical password schema as possible alternative for use security and usability problem.Gather document or information about a computer user and release that information back to the other person or unauthorized user.Avoid this problem use the CAPTCHA as CaRp schemas are vulnerable to spyware.CAPTCHA uses on algorithm based on critical AI problems and resist dictionary attack from discussed in text based password schemas. To provide high protection against spyware for used context of graphical password in CAPTCHA.A user study indicates improve in terms of login time security.

In security using critical AI problem initially related in CaRP the notion of CaRP is easy but guessing the password as correct or not. Text CAPTCHA and Image reorganization CAPTCHA are built a CARP, in Text CaRP password is a sequence of character like text password. In CaRP technology are used for clickAnimal, clickText, AnimalGrid. In information security program security awareness is important fact organized by

Cyber criminals are development of advanced hacking technique that can be used to steal money and protect information from the other general public. In implementing access control password authentication is one of the common building blocks are breaking password authenticated system attack is dictionary attack .To provide the best security using CAPTCHA as Text and Image recognization CAPTCHA to set the password as easy to memorable as alphanumeric password as text password is slightly critical to remind text password. CAPTCHA is the including of Gimpy family of tests, Bongo and pix. The identifying Gimpy involver three of approximately and distance of image is seven word of an image. EZ_Gimpy is a version of simpler that used only one word, CAPTCHA is a audio version of Gimpy.

A sequence of letter and number of words is render and distort then audio played spammer for the automated techniques and free e_mail account site .The purchase automatic ticket from ticket master. A program any parser the test generated by CAPTCHA can be used to unsolved AI problem.

II. Type of CAPTCHAs:

CAPTCHAs are classified based on what is distorted and presented as a challenge to the user. They are:

1. Text CAPTCHAs:

These are simple to implement. The simple novel approach is to present the user with some questions which only a human user can solve. Text questions are involving in text captcha and answer are only user can understand not robot.

Questions are very easy for a human user to solve, but it’s very difficult to program a computer to solve them. These are also friendly to people with visual disability – such as those with colour blindness. Other text CAPTCHAs involves text distortions and the user is asked to identify the text hidden. These text CAPTCHA has following methods such as:

1.1 Gimpy:

Gimpy is a very reliable text CAPTCHA built by CMU in collaboration supported yahoo for their Messenger service. Gimpy is based on the human ability to read extremely distorted text and the in ability of computer programs to do the same. Gimpy works by choosing ten words randomly from a dictionary, and displaying them in a distorted and overlapped manner. Gimpy then asks the users to enter a subset of the words in the image. The human user is capable of identifying the words correctly, but a computer program cannot.

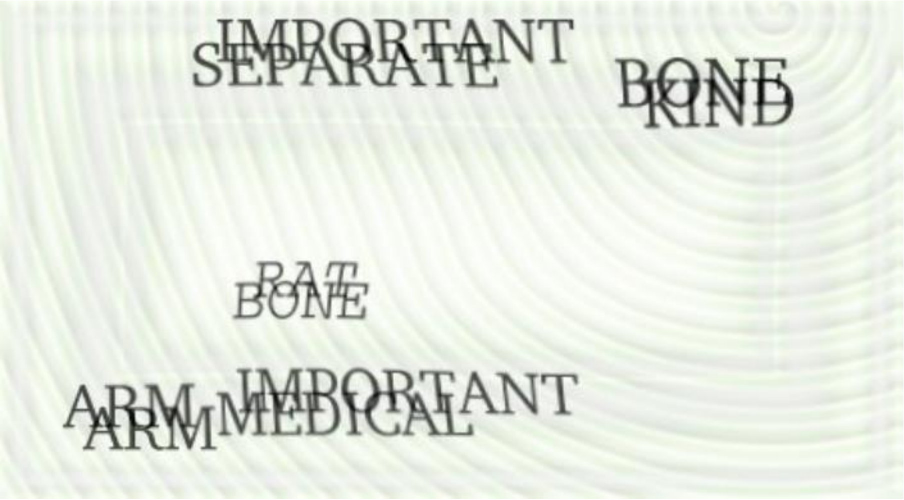

Fig.1:Gimpy

1.2 Ez – Gimpy:

Ez_gimpy identifies version of the Gimpy CAPTCHA, gain by Yahoo in their signup page. Ez – Gimpy randomly picks a single word from a dictionary and applies distortion to the text. The user is then asked to identify the text correctly.

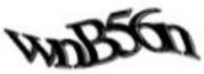

Fig 2: Yahoo’s Ez – Gimpy CAPTCHA

1.3 Baffle Text:

This was developed by Henry Baird at University of California at Berkeley. This is a variation of the Gimpy. This doesn’t contain dictionary words, but it take random alphabets to create a nonsense but pronounceable text. Distortions are then added to this text and the user is challenged to guess the right word. This technique overcomes the drawback of Gimpy CAPTCHA because, Gimpy uses dictionary words and hence, clever bots could be designed to check the dictionary for the matching word by brute-force**.**

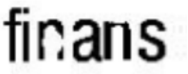

Fig 3: Baffle Text examples

1.4 MSN Captcha:

Microsoft uses a different CAPTCHA for services provided under MSN umbrella. These are mostely called MSN Passport CAPTCHAs. They use eight characters (upper case) and digits are 0-9. MSN captcha uses Foreground is dark blue, and background is grey. Warping is used to distort the characters, to produce a wave effect, for computer recognition very difficult.

XTNM5YRE

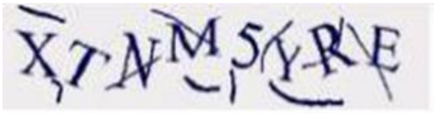

Fig 4: MSN Passport CAPTCHA

2. Graphic CAPTCHAs:

Graphic CAPTCHAs are challenges that include pictures or objects that have some sort of similarity that the users have to guess the matching image and also select some object on image to set the password. They are visual puzzles, similar to Mensa tests. Computer are used for generates the puzzles and grades the answers, but is can’t solve itself .

2.1 Bongo:

BONGO are used to asks the user to solve a visual pattern recognition problem. It displays two series of blocks, the left and the right. The blocks in the left series different from those in the right, and the user must find the functions that sets them apart. A possible left and right series is shown in Figure 2.1

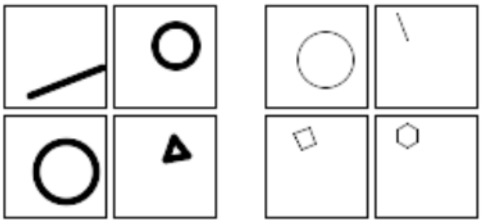

Fig 5: Bongo CAPTCHA

The left and right sets are different because everything on the left is drawn with thick lines and those on the right are in thin lines. After seeing the two blocks, the user is presented with a set of four single blocks and is asked to determine to which group the each block belongs to it. The user passes the test if user determines correctly to which set the blocks belong to it. It is careful to see that the user is not confused by a large number of choices.

2.2 PIX:

PIX is a program that has a large database of labelled images. All of these images are pictures of concrete objects (a horse, a table, a house, a flower). The program picks an object at random, finds six images of that object from its database, presents them to the user and then asks the question “what are these pictures of?”Current computer programs should not be able to answer this question, so PIX should be a CAPTCHA. However, PIX, as stated, is not a CAPTCHA: it is very easy to write a program that can answer the question “what are these pictures of?” Remember that all the code and data of a CAPTCHA should be publicly available; in particular, the image database that PIX uses should be public. Hence, writing a program that can answer the question “what are these pictures of?” is easy: search the database for the Images presented and find their label. Fortunately, this can be fixed. One way for PIX to become a CAPTCHA is to randomly distort the images before presenting them to the user, so that computer programs cannot easily search the database for the undistorted image.

2.3 Audio CAPTCHAs:

The audio captcha offer is based on sound. The program picks a word or a sequence of numbers at random, renders the word or the numbers into a sound clip and distorts the sound clip; it then presents the distorted sound clip to the user and asks users to enter its contents. This CAPTCHA is based on the difference in ability between humans and computers in recognizing spoken language. Nancy Chan of the City University in Hong Kong was the first to implement a sound-based system of this type. The idea is that a human is able to efficiently disregard the distortion and interpret the characters being read out while software would struggle with the distortion being applied, and need to be effective at speech to text translation in order to be successful. This is a crude way to filter humans and it is not so popular because the user has to understand the language and the accent in which the sound clip is recorded.

III. Background and Related Work:

How CAPTCHA as graphical password is more secure than alphanumeric password?
CAPTCHA is secure communication channel between user and web. CAPTCHA uses graphical password to improve the security as providing the spot clicking password on appear in image object generate or derive the

password. The alphanumeric password are is combination of 26 character, special symbols and numbers like 0-9 so hacker can combine them on personal information and any one combination are correct then hack the system so it occurred the password guessing attack, dictionary attack, machine learning attack relay attack that's why it is less secure. The conventional password system is not secured that's why CAPTCHA is used in marketing and e_banking. CAPTCHA is based on graphical password it is the set of collection of images appeared in one image and set the clickpoint on image as derive the password. CaRP is the built on graphical password schemes for user authentication. When user type or select the userId and faced to CAPTCHA and graphical password then call Captcha-based Password Authentication (CbPA) protocol its offer by authentication server. Authentication server are verify them and stored into database. CaRP is used for to break the password guessing attack, dictionary attack ,relay attack, machine learning attack .

Why CAPTCHA is needed in the online services and How ii is differs than Text password?

CHAPTCHA Starting around 1999, many graphical password schemes have been proposed as alternatives to text-based password authentication .To provide the covering usability and security as well as system evaluation. User require the password are user friendly or some personal information hints are knowledge-based authentication as they apply to graphical passwords as very secure , but identify security threats that such systems must address and review known attacks. These attacks are break the CaRP authentication server. CaRP can check the requested people entry verify on database and passed to authentication server for identification of login user and spot clicking password. CAPTCHAs real time example are gmail and hotmail for assign the text CAPTCHA and reenter them for verification are human or robot are logon these system. These type of CAPTCHA human can only understand and robot can't understand the text CAPTCHA.

IV. Literature Survey:

There is some techniques were implemented by researchers or author to improve the high security of system and efficiency of CAPTCHA as have been proposed in the literature for the set CAPTCHA as graphical password And some methods were proposed to improve online security and e_banking.

This paper is "CAPTCHA:Using Hard AI Problem For Security" Researchers by Von Ahn,Manual Blum,Nicholas J.Hopper and John Langford .author proposed work built the methods are1.Lazy Cryptographers Doing AI. 2.AI Problem as Security Primitives. 3.Two and Four AI Problem Families these methods are more usable for user and its user friendly.Author proposed these system take advantages are 1.Interaction with the AI community. 2.Reduction as they used in cryptography useful for progress of algorithmic development.3.It is used for securely and stegnographic communication. These system only use for Smartphone or PC or tablet. Application such as Robust Image Based Stegnography, Militery Application and Online Polls.

This paper is 'Towards New Security primitives Based on Hard AI Problem' researchers by Bin B.Zhu and Jeff Yan has author proposed work the methods are 1.Thawart Password Guessing 2.Passpoint 3.CaRP 4.Security Analysis. these methods are providing and detect the password guessing attacks, machine learning attacks ,dictionary attacks for using CAPTCHA as spot clicking password. Author proposed these system take advantages are 1. Clicktext is much more secure than normal text because it typically contains 30 or more characters. 2.CaRP can offer the same password entry across a different type of devices like Smartphone and PC and identifying throught device addresses. 3. Protect the relay attacks, cross_site scripting attacks. Application Such as 1. Cross device authentication. 2.E_banking.

This paper is develoed 'Novel Method for Graphical Password using CAPTCHA'. Researchers by Jayshree Ghorpade, Shamika Mulane and Devika Patil,Dhanashree Poal,Ritesh Prasad. Author proposed work built the different methods are CaRP, CAPTCHA, Graphical Password Techniques. It has provide the only human understandable password not robotics and computer thats why it break the attacks. Author proposed these system take advantages are 1.It provide cyber security for user authentication and avoid misuse or illegal use of highly sensitive data. 2. It protect the dictionary attack and password guessing attacks.3. To break the Online guessing attacks and Shoulder surfing attacks. 4. Usability (e.g., login success rates, login times, password creation times) as close as possible to, as or better than, text passwords. 5. Implicit feedback to legitimate users, when passwords are multi-part.It has only protect or providing security on data but not securely break the crime or identifine the criminals. Application such as 1.It is used for e_banking and Axis bank.

This paper is "Distortion Estimation Techniques in Solving Visual CAPTCHAs". Researchers by Gabriel Moy, Nathan Jones, Curt Harkless and Randall Potter has developed. Author proposed work built the different

methods are 1.Matching whole object by correlation 2.Matching Sub_Objects by Distoration Estimation. These methods are used for verification and match one to another .Author proposed these system take advantages are 1.Distortion estimation uses of cores and minipatch used for find which correlated distorted template image is stored on.2.Applaying Similar background removal algorithm for verification. It is use very large dictionary and large local distortion so the computation time become unmanageable. Application such as 1.It is applied for fingerprint matching problem.
This paper is 'A New Graphical Password Scheme Against Spyware by Using CAPTCHA' Researcher by Haichang Gao, Xiyang Liu, Sidong Wang and Ruyi .Author proposed work built the different methods are Capability to withstand spyware, CaRP. Now text password alternate schemes are not detect to spyware attacks and CAPTCHA as graphical password break the spyware attack in proposed system so it is more secure than text password. Author proposed these system take advantages are 1.Text-based password schemes have inherent security and usability problems, leading to the development of graphical password schemes are alternate schemes are vulnerable or break to spyware attacks. 2. Usability. 3. Understood to autherise users, when passwords are multi-part. It has one disadvantage are 1.Size of password spaces more than textual password.
This paper is "Breaking e_Banking CAPTCHAs " Researchers by Shujun Li University of Surrey, Roland Hochschule der Medien Stuttgart has developed. Author proposed work built the different methods are 1.Online banking 2.Automated attack. These system are much used for online banking and CAPTCHA provide the much better security, usability and reliability. e_banking system uses CAPTCHA are break the Automated attacks. . Author proposed these system take advantages are1.It prevent malicious manipulation of e_banking translation by automated Man _in_middle attackers. 2.e_banking CAPTCHAs are used for serving hundreads of millions of e_banking customers as secure and usable. Application such as 1.e_banking CAPTCHAs are recently work in Axis Bank and Online banking. 2. financial Institutions.

V. Methods for secure CAPTCHA

1. CAPTCHA and CaRP:

CAPTCHA is the communication channel between user and Web server from keyloggers and Spyware. CAPTCHA relies on recognizing an object on image to set the password by exploiting its surrounding context or image, a task that humans can perform very well but computer and robot can' t perform the task. An infinite number of images or collection of images can be used to generate CAPTCHA challenges, which can effectively not enable and break the learning process in machine learning attacks. The machine learning attack is computer expert or hacker can hack the system or find the password but our system to break the machine learning attacks. Image collection and CAPTCHA generation can be fully automated. CAPTCHA is more usable and reliable for user and not memorable password as compared to alphanumerical password. Image-Recognition CAPTCHA (IRC) is more secure than text CAPTCHA IRCs rely on the difficulty of object identification or classification, possibly combined with the difficulty of object segmentation and its improve the security. CaRP (CAPTCHA as gRaphical password) is a built on graphical password schemes for user authentication. When user type or select the userId and faced to CAPTCHA and graphical password then call Captcha-based Password Authentication (CbPA) protocol its offer by authentication server. CaRP schemes are click-based graphical passwords or spot clicking password according to the memory tasks in memorizing and select a spot or clickpoint not grid cell. CaRP is based on two categories: recognition and recognition-recall, recognition is requires recognizing an image and recognition-recall which requires recognizing an image and using the recollation objects as cues to enter a password. Recognition-recall combines the tasks or items of recognition and cued-recall, it's easy for human memory and the cued-recall has provides of a large password space

2. ClickText:

In CAPTCHA is set the collection of images is appear in one image and select the PIX or spot clicking password is based on image. Clickpoint is appear in ClickText, to selected the clickpoint or spot clicking password in images to derive the password as sequentially clicks on image. ClickText is a recognition-based CaRP scheme built on top of text Captcha., and thus one character should be eliminate from the alphabet. ClickText password is a sequence of characters in the alphabet and numeric during generation of image. The authentication server relies on the ground truth to identify the characters corresponding to user-clicked points and ClickText images, characters can be arranged as automatically by computer.

3. ClickAnimal:

ClickAnimal is a recognition-based CaRP scheme built on top of CAPTCHA Zoo. The CAPTCHA generation process is applied to generate ClickAnimal images: 3D models are used to make 2D animals by applying different views, textures, colors, lightning effects, and optionally distortions. The resulting **2D animals are** then arranged on a disarranged background s. Some animals may be closer by other animals in the image, but their basic parts are not closer in order for humans to identify each of them.

4. AnimalGrid:

AnimalGrid's password space can be increased by combining it with a grid-based graphical password and grid depending on the size of the selected animal. AnimalGrid is a combination of ClickAnimal and CAS.(Click-A-Secret) where in a user clicks the grid cells in her/his password. The number of grid-cells in a grid should be much larger than the characters size. It has the advantage correct animal should be clicked in grid-cell then grid to be correct. If a wrong animal is clicked, then grid is wrong at the authentication server side. To enter a password, a ClickAnimal image is displayed first then an animal is selected, an image of n × n grid present, with the grid-cell size equaling the bounding rectangle of the selected animal and verifying the spot on clicking animals in image then If the selected spot is correct not grid cell then log on successful.

5. Textpoint:

A point is said to be an internal point of an object if its distance to the closest boundary of the object exceeds a threshold. A set of internal invariant points of characters is selected to form a set of spot clicking password points for TextPoints . Spot clicking password on the image generated by underlyingCAPTCHA engine and verify the authentication server. TextPoints has a much larger password space than ClickText and it require more database space.

VI. CaRP Authentication:

CaRP (Captcha as gRaphical Passwords). CaRP is click-based graphical passwords or spot clicking password is a sequence of clicks on an image is used to derive a password. CaRP are used for more advanced protection such as secure channels between clients and the authentication server through Transport Layer Security (TLS) and CAS(CAPTCHA as Secret key).

A CaRP password is a sequence of clickable-points of image object that the user selects. CaRP receiving a login request, Authentication Server generates a CaRP image, records the locations of the objects in the image, and sends the image to the user to click the password. The coordinates of the clicked points are recorded and sent to Authentications Server along with user id.

1. Algorithm of CaRP:

Step 1: Start
Step 2: User send the authentication request to Authentication Server.
Step 3: Authentication Server generate the CaRP image and Send to the user.
Step 4: User send the userID and password click on clickpoint as appear in images and set the Password.
Step 5: This image is send to Authentication Server and set the AS to generate a CaRP image record. As store {UserID,H(p,s),s}.Here H is HashValue,p is Password and s is Salt.
Step 6: If password is H(p,s)=H(p,s) then login success else not success.
Step 7 :Stop

VII. Conclusion

In our proposed work based on cryptography and artificial intelligence have much to contribute to one another The objective of our work is to provide login time security, e_banking security and study different methods for providing a graphical password on system. Various methods are introduced in that work which is emerged in recent years. This analysis shows that different technologies used in all the paper with taking different way for detecting password guessing attack, dictionary attack, machine learning attack and relay attack. In our proposed work to provide the more security than alphanumeric or text password.

References:

[1] R. Biddle, S. Chiasson, and P. C. van Oorschot, "Graphical passwords: Learning from the first twelve years," ACM Comput. Surveys, 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.
[3] H. Tao and C. Adams, "Pass-Go: A proposal to improve the usability of graphical passwords," Int. J. Netw. Security, 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, Jul. 2005.
[5]H. Gao, X. Liu, S.Wang, and R. Dai, "A new graphical password scheme against spyware by using CAPTCHA," in Proc. Symp. Usable Privacy Security, 2009.
[6] L. Wang, X. Chang, Z. Ren, H. Gao, X. Liu, and U. Aickelin, "Against spyware using CAPTCHA in graphical password scheme," in Proc. IEEE Int. Conf. Adv. Inf. Netw. Appl., Jun. 2010.
[7] S. Li, S. A. H. Shah, M. A. U. Khan, S. A. Khayam, A.-R. Sadeghi, and R. Schmitz, "Breaking e-banking CAPTCHAs," in Proc. ACSAC,2010.
[8]L. von Ahn, M. Blum, N. J. Hopper, and J. Langford, "CAPTCHA: Using hard AI problems for security," in Proc. Eurocrypt, 2003.
[9] S. Chiasson, P. C. van Oorschot, and R. Biddle, "Graphical password authentication using cued click points," in Proc. ESORICS, 2007.
[10]H. Gao, X. Liu, S.Wang, and R. Dai, "A new graphical password scheme against spyware by using CAPTCHA," in Proc. Symp. Usable Privacy Security, 2009.
[11] L. Wang, X. Chang, Z. Ren, H. Gao, X. Liu, and U. Aickelin, "Against spyware using CAPTCHA in graphical password scheme," in Proc. IEEE Int. Conf. Adv. Inf. Netw. Appl., Jun. 2010.
[12] B. Pinkas and T. Sander, "SeCuring passwords against dictionary attacks," in Proc. ACM CCS, 2002.