ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

An Advanced Security Integrated Authentication System for Net Banking

B.Hema, K.R.Anu Prashika, V.A.Makdooma, S.Rajeswari

Department of Information Technology, Velammal Institute of Technology, Chennai, Tamil Nadu, India

ABSTRACT: It present a new security primitive based on hard AI problems, namely, a novel family of graphical password systems built on top of Puzzle technology,in which we call Puzzle as graphical passwords (Digital Signatures). CaPtcha is both a Puzzle and a graphical password scheme. CaPtcha addresses a number of security problems altogether, such as online guessing attacks, relay attacks, and, if combined with dual-view technologies, shoulder-surfing attacks can be prevented. Notably, a CaPtcha password can be found only probabilistically by automatic online guessing attacks even if the password is in the search set. CaPtcha 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. CaPtcha is not a panacea, but it offers reasonable security and usability and appears to fit well with some practical applications for improving online security.We present exemplary CaPtcha built on both text Puzzle and image-recognition Puzzle login. One of them is a text CaPtcha wherein a password is a sequence of characters like a text password, but entered by clicking the right character sequence on CaPtcha images. CaPtcha 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.

KEYWORDS*:* Text Based Puzzle Solving, Random Captcha Image Recognition, Image Based Puzzle Solving.

I.INTRODUCTION

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 under explored. A fundamental task in security is to create cryptographic primitives based on hard mathematical problems that are computationally interact able. Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) - Program that figures out if a human or a both is trying to use the following services. It creates a test that's easy for a human to pass, but difficult for a computer. Captcha was created by Luis von Ahn, Manuel Blum, Nicolas Hopper and John Langford in the year 2000 at Carnegie Mellon University and it was named after Alan Turing. CAPTCHA is the reverse Turing test, computer asks question to identify if human or not. Imitation Game started as an Interrogator, identifies whether one is machine or person if machine can pass 70% of questions, in presence of intelligence. Main uses are prevention of Spam, Bot Website Registration, Ticket Purchases and Lop-sided Online Poll Results .Information had a paramount role during history at all times. Its control is synonymous of ability and power. It can represent battle plans, secret negotiations or current events and television news. Exploitation of information can bring richness. Information used to be transmitted by manuscript or by voice; now it can travel thousands of kilometers in some tenths of second thanks to waves and cables. These fast technological developments make information extremely important in our life. However, this powerful information is now more volatile and can be easily intercepted or reproduced with all the consequences which we can imagine such as false medical diagnostic, false military targets or false proof of events. Image authentication is important in many domains: military target images, images for evidence in court, digital notaries' documents, and pharmaceutical research and quality control images. All these images have to be protected in order to avoid false judgments. The wide availability of powerful digital image processing tools allows extensive access, manipulations and

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

reuse of visual materials. In fact, lot of people could now easily make unauthorized copies and manipulate images in such a way that may lead to big financial or human lives losses. These problems can be better understood with a simple example. A patient with a serious illness, discovered from medical diagnostic images, may eventually get better due to medical treatments. The medical follow-up of that patient involves the interpretation of historic images to evaluate the progression of the illness in time. A possible false diagnosis can jeopardize the patient life, if the stored image underwent malevolent manipulations, storage errors or compression, such that the resulted distortions cannot be detected by the doctor. This is an example where modifications are not tolerated. However, in many other applications we need to tolerate some image processing operations for transmission, enhancement or restoration while we still need to detect at the same time any significant changes in the image content. Therefore, there is an ambiguity since some changes must be tolerated while others not. Nevertheless, the user is required to remember a static password which is vulnerable to shoulder surfing attacks. Moreover, it is possible to reconstruct the secret pattern from images of the smart phone screen. Changing the pattern frequently and multi-factor authentication are countermeasures for this attack strategy but they impose more burdens on the users. Although biometric security mechanisms are increasingly applied for authentication on mobile devices, they are naturally limited and difficult to substitute in case of being lost or compromised.

THE ETHICS OF CAPTCHA

CAPTCHA was designed from the beginning to help defend against irregular and illicit activity on the web. On one hand, it can be an incredible simple but potent tool in preventing malicious activity in any number of applications. In this way, CAPTCHA helps enforce an ethical standard of accepted internet practices, usually impeding the use of automation or bots to rapidly interact with website elements, and ensuring that the user is in fact human. Recently however, Google came under fire for using CAPTCHA as a means to decode street numbers for its Google Maps site. The ethics of such a practice were called into question with regards to privacy and the unknowing participation of users in this interpretation of information.

A BANK

The official site of one of the central banks in Argentina. Among other services, the site offers a system for issuing a status report of taxes, debts, loans, and credit payments.

CAPTCHA CHARACTERISTICS: This is probably the weakest CAPTCHA of the bunch. It seems like the CAPTCHA-generator randomly chooses two backgrounds (template color and orientation), the characters, and the font color. In our sample, the combinations seemed random, so that if the font color is by chance very similar to the background, the CAPTCHA would be difficult, and otherwise it would be extremely easy for any OCR tool to solve.

COMMON ATTACKS IN A BANK

Internet banking does not mean only the bank side, we have to see it in a complex way

- Client side (=PC/browser)
- Network infrastructure (=Internet)
- Server side (=bank)

II.PROPOSED SYSTEM

Our proposed system offers reasonable security and usability and appears to fit well with some practical applications for improving online security. 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. Puzzle Login (top of Puzzle technology Using mathematical problems).Image Puzzle Solving Using AES Algorithm. The workflow of our project involves a four way authentication process followed by transactions by customer of bank.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

III.LITERATURE SURVEY

1. Graphical Passwords: Learning from the First Twelve Years- Robert Biddle, Sonia Chiasson
We present a new CAPTCHA which is based on identifying an image's upright orientation. This task requires analysis of the often complex contents of an image, a task which humans usually perform well and machines generally do not. Given a large repository of images, such as those from a web search result, we use a suite of automated orientation detectors to prune those images that can be automatically set upright easily. We then apply a social feedback mechanism to verify that the remaining images have a human-recognizable upright orientation.

2. Distortion Estimation Techniques in Solving Visual CAPTCHAs- Gabriel Moy, Nathan Jones
CAPTCHAs, which are automated tests intended to distinguish humans from programs, are used on many web sites to prevent bot-based account creation and spam. To avoid imposing undue user friction, CAPTCHAs must be easy for humans and difficult for machines. However, the scientific basis for successful CAPTCHA design is still emerging. This paper examines the widely used class of audio CAPTCHAs based on distorting non-continuous speech with certain classes of noise and demonstrates that virtually all current schemes, including ones from Microsoft, Yahoo, and eBay, are easily broken. More generally, we describe a set of fundamental techniques, packaged together in our De captcha system, that effectively defeat a wide class of audio CAPTCHAs based on non continuous speech. De captcha's performance on actual observed and synthetic CAPTCHAs indicates that such speech CAPTCHAs are inherently weak and, because of the importance of audio for various classes of users, alternative audio CAPTCHAs must be developed.

3. A new graphical password scheme against spyware by using CAPTCHA-Haichang Gao
CAPTCHAs protect online resources and services from automated access. From an attacker's point of view, they are typically perceived as an annoyance that prevents the mass creation of accounts or the automated posting of messages. Hence, miscreants strive to effectively bypass these protection mechanisms, using techniques such as optical character recognition or machine learning. However, as CAPTCHA systems evolve, they become more resilient against automated analysis approaches. In this paper, we introduce and evaluate an attack that we denote as CAPTCHA smuggling. To perform CAPTCHA smuggling, the attacker slips CAPTCHA challenges into the web browsing sessions of unsuspecting victims, misusing their ability to solve these challenges. A key point of our attack is that the CAPTCHAs are surreptitiously injected into interactions with benign web applications (such as web mail or social networking sites). As a result, they are perceived as a normal part of the application and raise no suspicion. Our evaluation, based on realistic user experiments, shows that CAPTCHA smuggling attacks are feasible in practice.

4. Modeling user choice in the PassPoints graphical password scheme-Ahmet Emir Dirik
CAPTCHAs are tests that distinguish humans from software robots in an online environment [3, 14, 7]. We propose and implement three CAPTCHAs based on naming images, distinguishing images, and identifying an anomalous image out of a set. Novel contributions include proposals for two new CAPTCHAs, the user study on image recognition CAPTCHAs, and a new metric for evaluating CAPTCHAs.

5.Paul C. Van Oorschot
Automated Turing Tests (ATTs), also known as human-in-the-loop techniques, were recently employed in a login protocol by Pinkas and Sander (2002) to protect against online password-guessing attacks. We present modifications providing a new history-based login protocol with ATTs, which uses failed-login counts. Analysis indicates that the new protocol offers opportunities for improved security and user friendliness (fewer ATTs to legitimate users) and greater flexibility (e.g., allowing protocol parameter customization for particular situations and users). We also note that the Pinkas–Sander and other protocols involving ATTs are susceptible to minor variations of well known middle-person attacks. We discuss complementary techniques to address such attacks, and to augment the security of the original protocol.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

IV.MODULES

The modules of this system include
*Registration
*Authentication
    *Password based authentication
    *Captcha Image Recognition
    *Puzzle solving
*OTP and Alert generation
*Online Bank

V.REGISTRATION

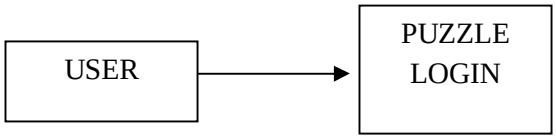
The authentication step first involves registration of a user for net banking. While registering the user is supposed to provide with confidential details such as username, password, mail id, contact number etc with which the authentication is to be done and to alert the user in case of any intrusions by the intruders. Also the user is supposed to submit the photographs of them for high level image based authentication. The user will need to upload seven photographs among which two are original and the other five are copies of the two originals with some modifications. Those modifications are according to the user preferences but it should not be identified different to other users. The modifications i.e the differences between the original and the duplicate photographies should only be known to the customer. After giving all the personal details the customer becomes a registered user by the bank.

VI.AUTHENTICATION---

The user when they are needed to make any transactions in the banking website, They would need to sign in to the banking website. The authentication involves three steps.

Password Based Authentication:

During sign in the user may enter the username and password in any order. for example: If the user name is “JAVA” the user may enter it as AJAV,AVJA,JAAV and so on .i.e the username and password can be entered in any combinations of strings. The application uses a bubble sort algorithm to sort out the username and password in the original order. This helps in preventing the guessing attacks and shoulder surfing attacks.



Captcha Image Recognition:

The next step of authentication is image based. The CAPTCHA images are displayed in the next step to the user. Among the 6 images the user should select the original image to move on to next step. If any intruders try to access your account and if they select the modified images, then an alert is sent to the mail id provided by the user. If the original or correct image is selected then the sign in is continued. It is made to stop computer hackers from using a program to automatically set up hundreds of accounts, such as email accounts. It is named after mathematician. 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.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

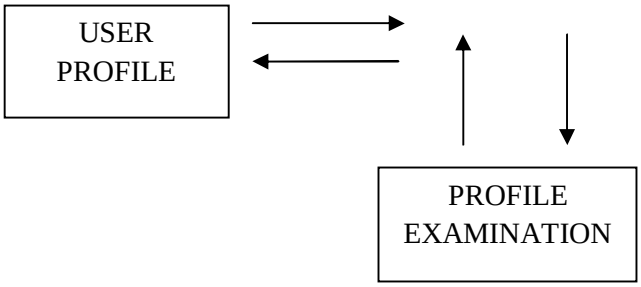


Image Puzzle solving:
The next step is puzzle solving the original image is split into several segments and shuffled and the user should arrange them into a frame and bring the original image. we study how to prevent DoS/DDoS attackers from inflating their puzzle-solving capabilities. To this end, we introduce a new client puzzle referred to as software puzzle. Unlike the existing client puzzle schemes, which publish their puzzle algorithms in advance, a puzzle algorithm in the present software puzzle scheme is randomly generated only after a client request is received at the server side and the algorithm is generated such that: 1) an attacker is unable to prepare an implementation to solve the puzzle in advance and 2) the attacker needs considerable effort in translating a central processing unit puzzle software to its functionally equivalent GPU version such that the translation cannot be done in real time. Moreover, we show how to implement software puzzle in the generic server-browser model.

VII.OTP AND ALERT GENERATION

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; a number of implementations also incorporate two factor authentication by ensuring that the one-time password requires access to something a person has (such as a small key ring fob device with the OTP calculator built into it, or a smartcard or specific cell phone) as well as something a person knows (such as a PIN).After the puzzle step, the OTP is generated with which the user continues his transaction. If the sign in fails at any step the alert is sent to the user through mail and sms and the user after giving a confirmation is proceeded to the further transactions.

OTP GENERATION

$R_0 = L_1$
$L_0 = R_1 \oplus F(L_1, K_0)$

$L_1 =$ 1001 0110 0111
$K_0 =$ 0101 0101 0101

$F_1 =$ 1100 0011 0010
$R_1 =$ 1000 0101 0001

$L_0 =$ 0100 0110 0011

010001100011	100101100111

L_0 R_0
Plain Text: $L_0 R_0$

010001100011	100101100111

L_0 R_0

OTP in BCD form : 0100 0110 00111001 0110 0111
OTP : 463967

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

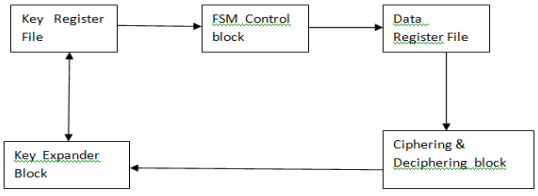
Vol. 7, Special Issue 2, March 2018

VIII.ONLINE BANKING

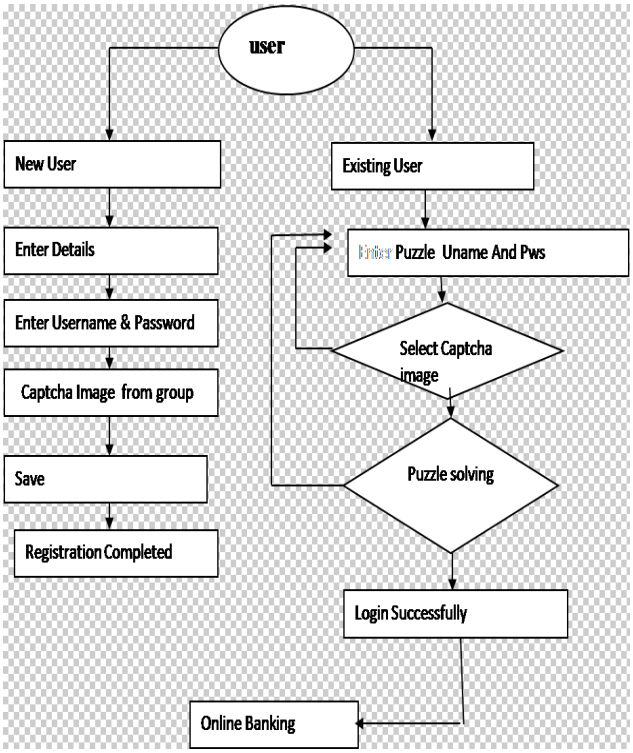
Online banking also known as internet banking, e-banking, or virtual banking, is an electronic payment system that enables customers of a bank or other financial institution to conduct a range of financial transactions through the financial institution's website. The online banking system will typically connect to or be part of the core banking system operated by a bank and is in contrast to branch banking that was the traditional way customers access banking services. Prior to online banking, it wasn't exactly easy to get on-demand reports and summaries for your account activity. Depending on the bank, there might even have been a fee associated with retrieving that info. Yet, with online banking, it's always one click away.Some banks are better than others in this regard. Most of them will provide you with a transaction history at the very least, but the best ones have advanced features like creating categories and viewing how much you've spent in each category (e.g. bills, entertainment, emergency, etc.).

IX.ALGORITHMS USED

***** Bubble Sorting for puzzle login
*****AES algorithm for encrypting image captcha and OTP generation.



SYSTEM ARCHITECTURE



ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

X.FUTRE ENHANCEMENTS

Captcha in this system propose using machine learning classifiers to attacks. At the sometime, we study how efficient statistical classifiers are at recognizing captcha images. In the authors study how good humans are at solving well-known captchas using Mechanical Detecting and removing lines is a well studied field in computer vision since the '70s. Two well-known and efficient algorithms that can be used against captchas with lines are the Canny detection and the Hough Transform Removing noise using a Markov Random Field (Gibbs) .Many image descriptors have been proposed over the last decades: one of the first and most used descriptors is the Harris Corner detector introduced. However, recently it has been replaced by more complex descriptors that are insensitive to scaled rotation (to a certain extent).

XI. SUMMARY AND CONCLUSION

The software puzzle may be built upon a data puzzle,it can be integrated with any existing server-side data puzzle scheme, and easily deployed as the present client puzzle schemes do.CAPTCHA is a wide research field and act as internet rectifier to secure web applications by discern human from bots. CAPTCHA presented here will improve resistance of math calculus. CAPTCHA use, Boolean operations and expressions instead of trigonometric and differential function which will help in reduce the complexity of CAPTCHA and help to achieve better usability and security as compared to math calculus CAPTCHA. Boolean CAPTCHA can be easily used by educated user. No need of technical skill, by using intellectual mind to solve this CAPTCHA and help to reduce time complexity.

REFERENCES

1. H. Gao, J. Yan, F. Cao, Z. Zhang, L. Lei, M. Tang, P. Zhang, X. Zhou,
2. X. Wang, and J. Li, "A simple generic attack on text captchas," in Proc. Network and Distributed System Security Symposium (NDSS). San Diego, USA, 2016.
3. C. Karthik and A. Recasens, Rajendran, "Breaking microsofts captcha," 2015.
4. V. Turchenko and A. Luczak, "Caffe: Convolutional architecture for fast feature embedding," Eprint Arxiv, pp. 675–678, 2014.
5. H. Gao, W. Wang, Y. Fan, J. Qi, and X. Liu, "The robustness of" connecting characters together" captchas." J. Inf. Sci. Eng., vol. 30, no. 2, pp. 347–369, 2014.
6. E. Bursztein, J. Aigrain, A. Moscicki, and J. C. Mitchell, "The end is nigh: Generic solving of text-based captchas," in 8th USENIX Workshop on Offensive Technologies (WOOT 14), 2014.
7. M. Mohamed, N. Sachdeva, M. Georgescu, S. Gao, N. Saxena, C. Zhang, P. Kumaraguru, P. C. Van Oorschot, and W. B. Chen, "A three-way investigation of a game-captcha: automated attacks, relay attacks and usability," in ACM Symposium on Information, Computer and Communications Security, 2014, pp. 195–206
8. B. M. ONeil, "Neural network for recognition of handwritten digits," 2013.