ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

Securing Authentication against Spyware using Captcha and click based Graphical Password

Vandana Maurya[1], Prof.V.B Gaikwad[2]

PG Student, Dept. of Computer Engineering, Terna Engineering College, Mumbai University, India[1]

Asst. Professor, Dept. of Computer Engineering, Terna Engineering College, Mumbai University, India[2]

ABSTRACT: With the rapid development of information and Internet technologies, the emphasis on building very secure system is paramount since services are not on the client's computer, and the server would need to know who is requesting resources and if that entity / user is authorized to do so. 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, a new security primitive based on hard Artificial Intelligence (AI) problems using Captcha and click based graphical password is proposed. It addresses a number of security problems, such as online guessing attacks, dictionary attacks, spyware and shoulder-surfing attacks. It also offers a novel approach to issues related with the well-known image hotspot problem in popular graphical password systems that often leads to weak password choices. It can fit well with some practical applications for improving online security.

KEYWORDS: Graphical password, Captcha, Information security, authentication, spyware, dictionary attacks.

I. INTRODUCTION.

Using hard AI (Artificial Intelligence) problems for security, initially proposed in [1], 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 stands for "Completely Automated Public Turing Test to Tell Computers and Humans Apart." The P for Public means that the code and the data used by a CAPTCHA should be publicly available. This is not an open source requirement, but a security guarantee: it should be difficult for someone to write a computer program that can pass the tests generated by a CAPTCHA even if they know exactly how the CAPTCHA works. The only hidden information is a small amount of randomness utilized to generate the tests. The T for "Turing Test to Tell" is because CAPTCHAs are like Turing Tests [2]. In the original Turing Test, a human judge was allowed to ask a series of questions to two players, one of which was a computer and the other a human. Both players pretended to be the human, and the judge had to distinguish between them. CAPTCHAs are similar to the Turing Test in that they distinguish humans from computers, but they differ in that the judge is now a computer.

Fig.1 Captcha

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

A. *Application*

In November 1999, for example, the Web site slashdot.com released an online poll asking which was the best graduate school in computer science—a dangerous question to ask over the Web. As is the case with most online polls, IP addresses of voters were recorded in order to prevent single users from voting more than once. However, students at Carnegie Mellon found a way to stuff the ballots by using programs that voted for CMU thousands of times: CMU's score started growing rapidly. The next day, students at MIT wrote their own voting program and the poll became a contest between voting "bots." MIT finished with 21,156 votes, Carnegie Mellon with 21,032 and every other school with less than 1,000. Can the result of any online poll be trusted? No, unless the poll requires that only humans can vote.

Another application involves free email services. Several companies offer free email services that have suffered from a specific type of attack: "bots" that signed up for thousands of email accounts every minute. This situation has been improved by asking users to prove they are human before they can get a free email account. Yahoo, for instance, uses a CAPTCHA to prevent bots from registering for accounts.

Some Web sites don't want to be indexed by search engines. There is a HTML tag to prevent search engine bots from reading Web pages, but the tag doesn't guarantee that bots won't read the pages; it only serves to say "no bots, please." Search engine bots, since they usually belong to large companies, respect Web pages that don't want to allow them in. However, in order to truly guarantee bots won't enter a Web site, CAPTCHAs are needed.

Captcha is now a standard Internet security technique to protect online email and other services from being abused by bots. However, this new paradigm has achieved just a limited success as compared with the cryptographic primitives based on hard math problems and their wide applications. Is it possible to create any new security primitive based on hard AI problems? This is a challenging and interesting open problem. In this paper, a new security primitive based on hard Artificial Intelligence (AI) problems using Captcha and click based graphical password is proposed.

II. RELATED WORK

A large number of graphical password schemes have been proposed. According to the task involved in memorizing and entering passwords, they can be categorized into three groups-

1) Recognition based Graphical password
2) Recall based Graphical password
3) Cued recall based Graphical password

A recognition-based scheme requires recognizing and identifying images from set of images. During authentication, the users need to recognize and identify the pictures they have picked earlier. A recall-based scheme requires a user to regenerate his/her password without any cueing. In a cued-recall scheme, an external cue is provided to user to help memorize and enter a password.

Pass faces [4] scheme wherein a portfolio of faces from a database is selected by user to create a password. "Passfaces" is a technique developed by Real User Corporation [4]. Déjà Vu [3] is also used same approach but images used were computer generated "random-art" images.

Draw-A-Secret (DAS) [5] was the first recall-based scheme proposed. Users are freed from having to remember any kind of alphanumeric strings. A user draws password on a 2D grid using stylus or mouse. The system encodes the sequence of grid cells along the drawing path as a user drawn password.

Pass-Go [6] is a grid-based scheme. It improved DAS's usability in which user selects intersections on a grid as a way to input a password.

PassPoints [8] is a click-based cued-recall scheme wherein a user clicks a sequence of points anywhere on an image in creating a password, and clicks close to the chosen click points, within some (adjustable) tolerance distance.

Cued Click Points (CCP) [9] is similar to PassPoints but uses one image per click. The next image displayed is based on the previous click-point so users receive immediate implicit feedback as to whether they are on the correct path when logging in.

The CbPA-protocol in [11] requires solving a Captcha challenge after inputting a valid pair of user ID and password unless a valid browser cookie is received. For an invalid pair of user ID and password, the user has a certain probability to solve a Captcha challenge before being denied access.

An improved CbPA-protocol was proposed in [12] by storing cookies only on user-trusted machines and applying a Captcha challenge only when the number of failed login attempts for the account has exceeded a threshold.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

It was further improved in [13] by applying a small threshold for failed login attempts from unknown machines but a large threshold for failed attempts from known machines with a previous successful login within a given time frame.

Captcha were also used with recognition-based graphical passwords to address spyware [10] wherein a text Captcha is displayed below each image; a user locates her own pass-images from decoy images, and enters the characters at specific locations of the Captcha below each pass-image as her password during authentication.

CaRP [14] is click-based graphical passwords, where a sequence of clicks on an image is used to derive a password. A new CaRP image is generated for every login attempt.

A. Analysis of Graphical password

TABLE 1

SR. NO	TITLE	AUTHOR	SECURITY ISSUES
1	The Science Behind Passfaces Real User Corporation(2005)[4]	(www.realuser.com)	Vulnerable to shoulder surfing attacks and spyware
2	"Déjà Vu: A user study using images for authentication(2000)[3]	R. Dhamija and A. Perrig	Hard to remember a random-art picture, load on server
3	The design and analysis of graphical passwords (1999) [5]	Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin,	Password collision (Two drawings become equivalent if they have the same encoding)
4	Pass-Go: A proposal to improve the usability of graphical passwords (2007)[6]	H. Tao and C. Adams	Shoulder-surfing, phishing and social engineering
5	Do background images improve 'Draw a Secret graphical passwords (2007)[7]	P. Dunphy and J. Yan,	Shoulder-surfing, interference between multiple passwords
6	PassPoints: Design and longitudinal evaluation of a graphical password system(2005)[8]	S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon	People with poor vision and color blindness will face difficulties
7	Graphical password authentication using cued click points (2007)[9]	S. Chiasson, P. C. van Oorschot, and R. Biddle	False accept and false reject
8	Securing passwords against dictionary attacks(2002)[11]	B. Pinkas and T. Sander,	Phishing, Spyware attacks
9	On countering online dictionary attacks with login histories and humans-in-the-loop(2006)[12]	P. C. van Oorschot and S. Stubblebine	Phishing attack, Spyware attacks

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

SR. NO	TITLE	AUTHOR	SECURITY ISSUES
10	Revisiting defenses against large-scale online password guessing attacks(2013)[13]	M. Alsaleh, M. Mannan, and P. C. van Oorschot -	Phishing attack, Spyware attacks
11	A new graphical password scheme against spyware by using CAPTCHA (2009)[10]	H. Gao, X. Liu, S.Wang, and R. Dai,	Login time and memorability is not ideal
12	Captcha as Graphical Passwords—A New Security Primitive Based on Hard AI Problems(2014)[14]	Bin B. Zhu, Jeff Yan, Guanbo Bao, Maowei Yang, and Ning Xu	Shoulder-surfing, Spyware attacks

III. THE PROBLEM DEFINITION

There is no way to prove that a computer program cannot pass a test which a human can pass, since there is a program-the human brain which passes the test. All that can be done is to present evidence that it is hard to write a computer program that can pass the test. The proposed work is a novel approach using Captcha and click based graphical password to address number of security issues such as online guessing attacks, relay attacks, shoulder-surfing attacks and the well known image hotspot problem in popular graphical password systems such as PassPoints.

IV. PROPOSED METHOD

Proposed method uses both Captcha and Graphical password. It is a two-step authentication. The first step requires recognizing a Captcha image and using the recognized objects as cues to type a password. Images used in this method are Captcha challenges, and a new set of Captcha image is generated for every login attempt. Second step requires clicking on system generated graphical image. System disables login after a small number of unsuccessful login attempts in case of unauthorized access.

A. Methodology used

User Authentication is done first using Captcha and then by using graphical password. Basic working steps are as follows:

i. User Registration

Step 1: The authentication server *AS* stores a salt *s* and a hash value *H(P, s)* for each user ID, where *P* is the password of the account and not stored.

Step 2: During Registration process user selects any one Captcha from a set of presented Captcha. When user issues a login request, server generates a set of Captcha images and gives it to a user. Server generates new CAPTCHAs for every login attempt even for the same user. User first identifies his/her Captcha and fills the same in the text field.

ii. User Authentication

Step 3: Entered Captcha text along with userID is sent to Authentication Server. Authentication Server compares the result with the one stored for the user account.

Step 4: Successful authentication for first step takes place if the two Captcha values match.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

Step 5: After successful authentication in first step, second step starts; where authentication Server records the locations of the clickable points in the image and sends the image to user to click his/her password.

Step 6: The coordinates of the user clicked points are captured and sent to Authentication server along with UserID.

Step 7: Authentication Server maps the received coordinates onto the image and recovers a sequence of clickable points of visual objects P' that the user clicked on the image.

Step 8: Then Authentication Server retrieves salt s of the user account and calculates the hash value of P' with the salt and compares the result with the hash value stored for the account.

Step 9: Authentication succeeds if the two hash value match. After this second step of authentication, user gets access to system.

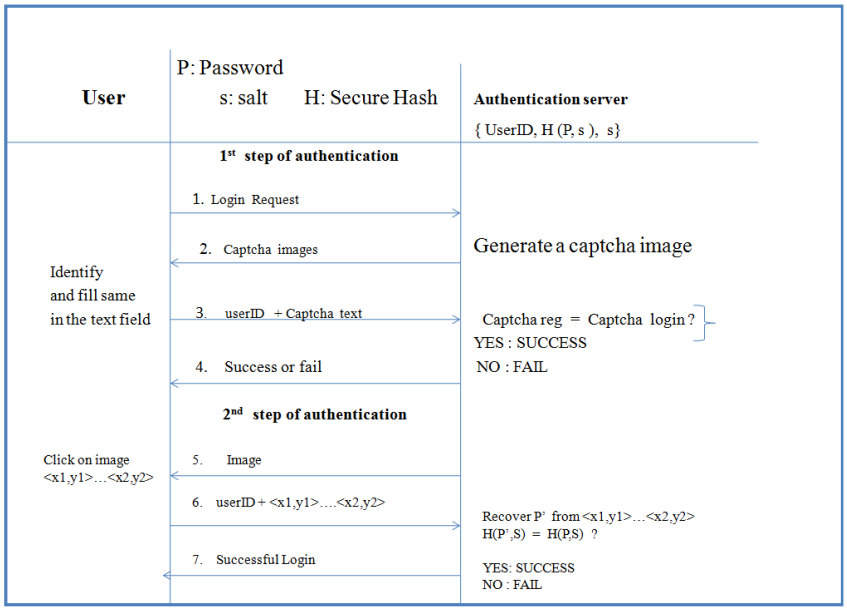

Fig. 2 Working of basic Captcha and graphical password authentication

(2 step authentication)

V. EMPIRICAL EVALUATIONS

A. Implementations

In this proposed method, user Authentication is done first using Captcha and then by using graphical password. In the first step of authentication, user has to select the correct Captcha, which was selected during registration.

Fig.3 First_step_of_authentication

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

After successful completion of first step, system generated graphical image appears on user's screen. User has to click within the correct region to log in into the system.

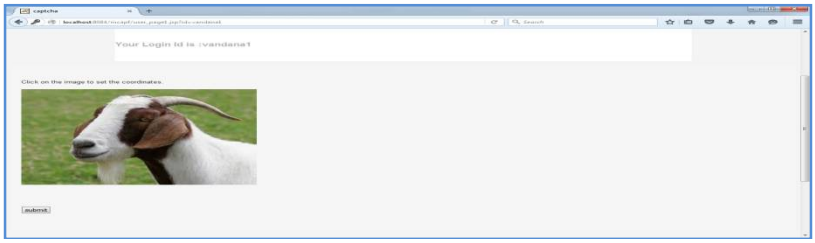

Fig.4 Second_Step_of_authentication

B. Experiments and Results

We conducted an in-lab user study with 40 participants (33 males and seven females) chosen randomly all of whom were in the field of academia (university students and staffs), with an average age of 27 years old (sample range from 21 to 44 years) and up to 3 years experience of using computers. The discussion of the results is as follows.

i. **Number of attempts**

With the way the study was designed, all participants successfully completed all the authentication tasks (register, confirm and login). In the first step of authentication, all participants were able to complete all of the authentication tasks with only one attempt. In the second step of authentication, results were predicted, as participants had to carefully click on their secret areas, which sometimes they did not manage to do.

ii. **Usability**

A major complaint among the users of graphical passwords is that the password registration and log-in process take too long, especially in recognition-based approaches. For example, during the registration stage, a user has to pick images from a large set of selections. During authentication stage, a user has to scan many images to identify a pass image. For example, in recognition based graphical password users have to scan through atleast 25 images. Users may find this process long and tedious. Because of this and also because most users are not familiar with the graphical passwords, they often find graphical passwords less convenient than text based passwords.

iii. **Reliability**

The major design issue for recall-based methods is the reliability and accuracy of user input recognition. In this type of method, the error tolerances have to be set carefully-overly high tolerances may lead to many false positives while overly low tolerances may lead to many false negatives. In addition, the more error tolerant the program, the more vulnerable it is to attacks.

iv. **Storage and communication**

Graphical passwords require much more storage space than text based passwords. Tens of thousands of pictures may have to be maintained in a centralized database. Network transfer delay is also a concern for graphical passwords, especially for recognition-based techniques in which a large number of pictures may need to be displayed for each round of verification.

VI. PERFORMANCE EVALUATION

i. **Login time:** The server records a participant's login time in each trial. Login time is the duration from the time when the server received a login request to the time when the server gave its response to the login request. Average Recorded login time is 22 Seconds. Although these times are greater than the times for traditional username/password login methods, they are still likely to be within the bounds of acceptability to users.

ii. **Security:** John the Ripper password cracking tool version 1.7.9 [27] has been used to check the security of a system. We conclude from the cracking results that the passwords the participants selected for Text and graphical image were reasonably strong**.**

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

iii. **Capability to withstand spyware:** The security provided by proposed method relies on the property of Captcha which is hard for machines to recognize. Although the spyware can gather the information of user's every login containing the string the user entered and the Captcha images displayed on the screen, the spyware can't recognize CAPTCHA's, so it can't ensure which CAPTCHAs correspond to the entered string.

iv. **Keylogger:** Actual Keylogger is used to capture keystrokes. It is found that keylogger can not capture coordinates of a graphical image.

VII. CONCLUSION AND FUTURE WORK

The past decade has seen a growing interest in using graphical passwords as an alternative to the traditional text-based passwords. Although the main argument for graphical passwords is that people are better at memorizing graphical passwords than text-based passwords, the existing user studies are very limited and there is not yet convincing evidence to support this argument. An important usability and security goal in authentication systems is to help users' select better passwords and thus increase the effective password space. The relationship between usability and security is a complex one; too often, improvements in one lead to a reduction in the other.

Proposed method is a new security primitive relying on unsolved hard AI problems to counter online guessing attacks. A new set of Captcha image, which is also a Captcha challenge, is used for every login attempt to make trials of online guessing attacks computationally independent of each other.

Captcha challenge along with graphical image can help reduce spam emails sent from a web email service. The usability and security of the proposed method can be further improved by using Captcha challenges and images of different levels of difficulty based on the login history of the user and machine used to login. Overall, proposed work is one-step forward in the paradigm of using hard AI problems for security.

Overall, the current graphical password techniques are still immature. Much more research and user studies are needed for graphical password techniques to achieve higher level of maturity and usefulness.

REFERENCES

1) L. von Ahn, M. Blum, N. J. Hopper, and J. Langford, "CAPTCHA: Using hard AI problems for security," in *Proc. Eurocrypt*, pp. 294–311, 2003.
2) Turing, A.M. Computing machinery and intelligence. *Mind 59*, 236 (1950), 433–460.
3) R. Dhamija and A. Perrig, "Déjà Vu: A user study using images for authentication," in *Proc. 9th USENIX Security*, pp. 1–4, 2000.
4) The Science Behind Passfaces Real User Corporation [Online]. Available: http://www.realuser.com/published/ScienceBehindPassfaces.pdf RealUser, "www.realuser.com," last accessed in June 2005
5) Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords," in Proc. 8th USENIX Security Symp., pp. 1–15,1999.
6) 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.
7) P. Dunphy and J. Yan, "Do background images improve 'Draw a Secret graphical passwords," in Proc. ACM CCS, pp. 1–12,2007.
8) 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,July 2005.
9) S. Chiasson, P. C. van Oorschot, and R. Biddle, "Graphical password authentication using cued click points," in *Proc. ESORICS*, pp. 359–374,2007.
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, pp. 760–767,2009.
11) B. Pinkas and T. Sander, "Securing passwords against dictionary attacks," in *Proc. ACM CCS*, pp. 161–170,2002.
12) 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.
13) 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.
14) Bin B. Zhu, Jeff Yan, GuanboBao, Maowei Yang, and NingXu ,"Captcha as Graphical Passwords—A New Security Primitive Based on Hard AI Problems", IEEE transactions on information forensics and security, vol. 9, no. 6, pp. 891-904, june 2014.
15) K. Renaud. Evaluating authentication mechanisms, In L. Cranor and S. Garfinkel, editors, "Security and Usability: Designing Secure Systems That People Can Use", chapter 6, pages 103-128. O'Reilly Media, 2005.
16) D. Denning and P. MacDoran,"Location-Based Authentication: Grounding cyberspace for better security", Computer Fraud & Security, Elsevier Science Ltd., February 1996.
17) S. Chakrabarti and M. Singhal "Password-based authentication: Preventing dictionary attacks" Computer, IEEE Computer Society, 40(6):68-74, June 2007.
18) B. Laxton, K.Wang, and S. Savage," Reconsidering physical key secrecy: Tele duplication via optical decoding", In 15th ACM conference on Computer and communications security, 2008.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

19) V. Roth, K. Richter, and R. Freidinger "A PIN-entry method resiliant against shoulder surfing", In 11th ACM conference on Computer and communications security, 2004.
20) A. Adams and M. Sasse, "Users are not the enemy", Communication of the ACM, 42(12):41-46, 1999.
21) D. Florencio and C. Herley, "A large-scale study of WWW password habits", In 16th ACM International World Wide Web Conference (WWW), May 2007.
22) https://en.wikipedia.org/wiki/Short-term_memory
23) https://en.wikipedia.org/wiki/Long-term_memory
24) https://en.wikipedia.org/wiki/Atkinson%E2%80%93Shiffrin_memory_model
25) https://developer.mozilla.org/en-US/docs/Archive/Security/Introduction_to_Public-Key_Cryptography
26) https://en.wikipedia.org/wiki/Dual-coding_theory
27) *John the Ripper Password Cracker* [Online]. Available: http://www. openwall.com/john/