ISSN:0975-9646

Captcha as Textual Passwords with Click Points to Protect Information

Sandeep Kumar Vengala

Computer Science & Engineering.
S.R.Engineering College,
Warangal, Telangana, India.

Goje Roopa(Asst.Prof)

Computer Science & Engineering,
S.R.Engineering College,
Warangal, Telangana, India.

***Abstract*— Most of the proposed graphical authentication system has certain drawbacks for that reason textual passwords are most preferable authentication system where users type passwords to authenticate themselves. An important usability goal of an authentication system is to support users for selecting the better password. User creates memorable password which is easy to guess by an attacker and strong system assigned passwords are difficult to memorize. So researchers of modern days gone through different alternative methods and conclude that graphical passwords are most preferable authentication system because graphical passwords are easy to remember but the problem these authentication system is prone to shoulder surfing attacks. The proposed system combines the existing textual passwords encryption and captcha password with different algorithms and added with click points to protect information, encouraging user to select more random click point which is difficult to guess. Proposed system is not a panacea, but it offers reasonable security and usability and appears to fit well with some practical applications for improving online security and also provide more protection against online dictionary attacks.**

***Keywords*— Authentication, textual passwords, captcha, usable security, click points, dictionary attacks**

I. INTRODUCTION

The benefit of Knowledge based authentication mechanism (KBAM) typically text based password are well known. The goal of an authentication system is to support users in selecting the superior password. An alternative to alphanumeric password is the graphical password. Graphical password uses images or representation of an image as a password. Human brains easily recognize pictures than the text. Most of the time user create memorable password which is easy to guess but strong system assigned password are difficult to remember. [1] An authentication system should allow user choice while influencing user towards stronger passwords.

An important usability goal of knowledge based authentication system is to support users in selecting password of higher security with larger password space. Basically when captcha password added to normal password then it provides more password space and easy to remember, encouraging user to select lengthy password which is easy to remember for the user. Along with that it also adds click points for the user to protect information. In the proposed system, the task of selecting weak password which is easy for an attacker to guess is more tedious, discourages users from making such choices. In consequence, this approach chooses the more secure password the path of least confrontation. Using hard AI (Artificial Intelligence) problems for security, initially proposed in [2], is an exciting new paradigm. Under this paradigm, the most notable primitive invented is Captcha, which distinguishes human users from computers by presenting a challenge, i.e., a puzzle, beyond the capability of computers but easy for humans. Captcha is now a standard Internet security technique to protect online email and other services from being abused by bots. 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. So, if the captcha image as a password is added to the normal password then it provides more security.

Instead of increasing the burden on users it's easier to track the system suggestions for a secure password which is the feature lacking in most of the schemes. Here captcha as textual passwords use previous captcha as graphical passwords concept in which the password is selected not by clicking on the image but by typing as a password. For valid users it provides implicit feedback such that while logging if user unable to recognize the image pattern selected as password it automatically alters the user and user can restart the password entry.

After the successful login of the user, the user is provided with an image to select click points to upload any file. In the same way, to download any file the user has to select the same click points provided while uploading the file.

II. NOMENCLATURE OF AUTHENTICATION

The following figure 1 shows the representation of current authentication methods. The problem with text based password is that user creates memorable password which can be break easily and also the text password has limited length password which means that password space is small.

Biometric based authentication techniques are somewhat expensive, slow and unreliable and thus not preferred by many [4]. Token based authentication system has high security and usability and accessibility then the others. Also the system uses the knowledge based techniques to enhance the security of token based system. But the problem with token based system is that if token get lost, the security get also lost [3].

Therefore the Knowledge based authentication techniques are most preferable technique to improve the real high security. Captcha Password is one of the

knowledge based technique and it is categorized into Recognition based and Recall based [11]. In Recognition based techniques user has to recognize or reproduce the things during the login where as in case of recall based technique user has to recall the things during the login in such a way that whatever they selected during the password creation they have to recall it in the same manner.

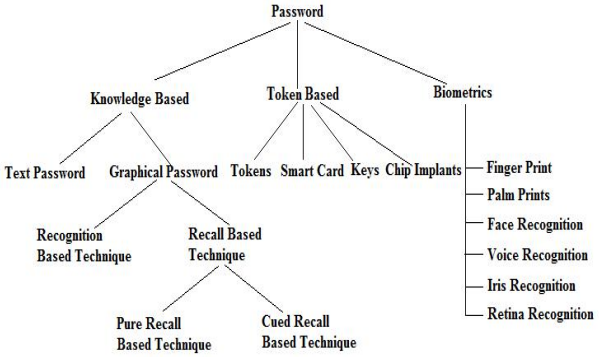

Fig. 1.Categorization of Password Authentication Techniques

III. Background And Related Work

E. Blonder [5] proposed graphical password scheme in which user click on several different predefined location on a predetermined image. During login, the user has to click on the approximate area of those locations. Basically the image helps the user to summon up their passwords and therefore this scheme is considered more suitable than unassisted recall.

Bin B. Zhu [6] proposed captcha as graphical passwords a new security primitive based on hard AI problems, namely, a novel family of graphical password systems built on top of Captcha technology, which we call Captcha as graphical passwords (CaRP). CaRP is both a Captcha and a graphical password scheme. But the drawback of this scheme is it is prone to shoulder surfing attacks. Shoulder surfing attacks can be avoided using dual view technologies but it costs more.

A large number of graphical password schemes have been proposed. They can be classified into three categories according to the task involved in memorizing and entering passwords: recognition, recall, and cued recall. Each type will be briefly described here. More can be found in a recent review of graphical passwords [7].

Among the three types, recognition is considered the easiest for human memory whereas pure recall is the hardest [7]. Recognition is typically the weakest in resisting guessing attacks. Many proposed recognition-based schemes practically have a password space in the range of 213 to 216 passwords [7]. Figure 2 shows the click text with 33 characters in which user select password by clicking on image. A study [8] reported that a significant portion of passwords of DAS and Pass-Go [9] were successfully broken with guessing attacks using dictionaries of 231 to 241 entries, as compared to the full password space of 258 entries. Images contain hotspots [10], [11], i.e., spots likely selected in creating passwords. Hotspots were

ing attacks on
on of passwords
235 entries, as
ls.

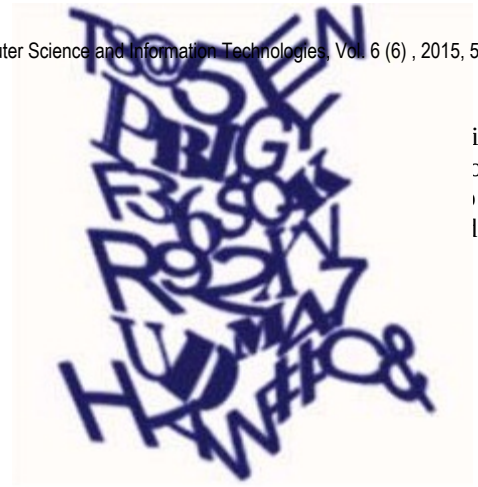

Fig.2.A ClickText image with 33 characters

IV. Proposed System

The proposed system is based on captcha as textual password system that not only guides and helps the user for password selection but also encourages the user to select more random distributed password. The proposed system is based on Captcha Technology which motivates and influence people to behave in a desired manner [14]. The proposed system combines the captcha password and click-point to make authentication system more secure. Basically during password creation the normal password and captcha password is asked to enter. The normal password should remember by the user where as captcha password entered by the user should remember the pattern it is selected.

A. Captcha

Captcha relies on the gap of capabilities between humans and bots in solving certain hard AI problems. There are two types of visual Captcha: text Captcha and Image-Recognition Captcha (IRC). Security of text Captchas has been extensively studied [15]–[19].

B. Captcha in Authentication

It was introduced in [20] to use both Captcha and password in a user authentication protocol, which we call *Captcha-based Password Authentication (CbPA) protocol*, to counter online dictionary attacks. The CbPA-protocol in [14] 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.

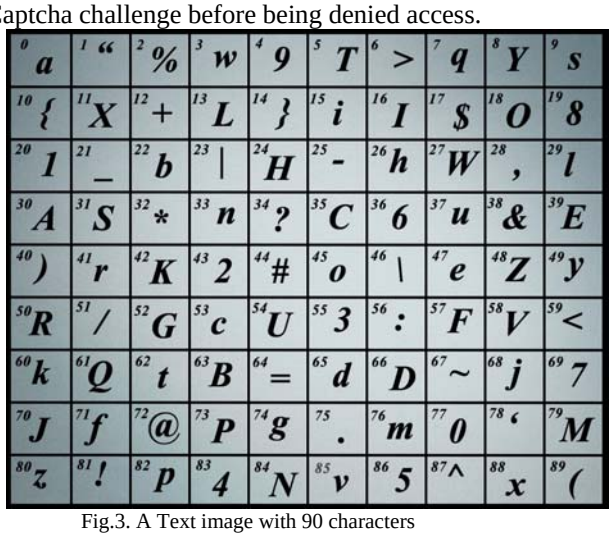

Fig.3. A Text image with 90 characters

Here after entering the valid pair of user ID, we provide the user to enter the password and a captcha password. Figure 3 shows the text image of 90 characters in which user can select different passwords. For normal password and captcha password we provide a minimum selection of 8 characters as a password. The normal password should be remembered by the user where as the captcha password should be recognized by the user. In captcha password every character is provided with a number on top of each letter so that the user can easily remember the password. The user can choose different pattern on the image to select the captcha password. As numbers are provided to each letter, the user can easily remember the captcha password.

For example, a user can easily remember the phone number. So by selecting the characters provided on those numbers the user can easily remember the password.

Figure 4 shows that selecting the captcha password and remembering the password easily. The length of the password selected is 9 characters and it is aXbn#3D0x and it can be easily recognized by characters or by the pattern selected. In this way the user can select very lengthy password and can remember very easily.

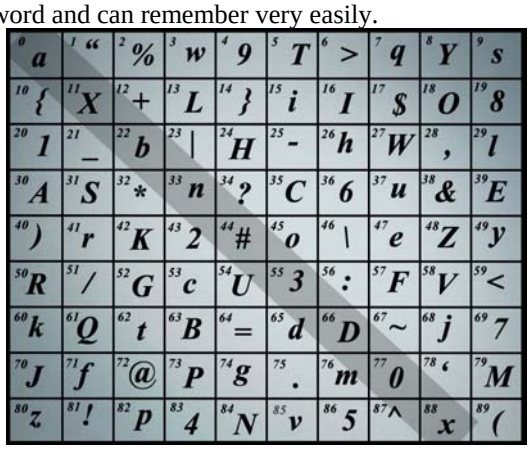

Fig.4. Selection of Captcha Password

In this way the captcha password can be easily recognized by the user and can easily remember. If the encryption algorithms are used behind the captcha password then it can provide more protection against online dictionary attacks. The encryption algorithms like DES, SHA-1, SHA-512 if used along with captcha password then it provide more protection and also can give convenient interface to the user where the password can be easily remembered.

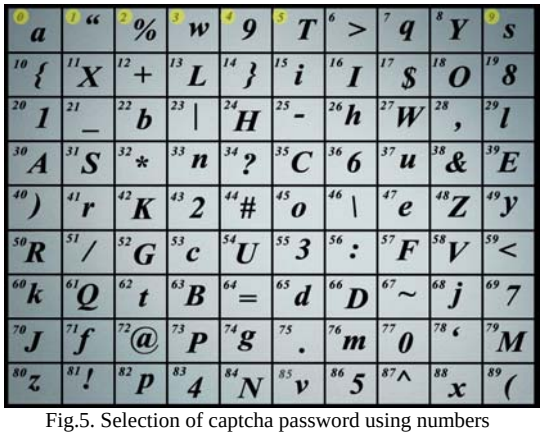

Fig.5. Selection of captcha password using numbers

Figure 5 shows the selection of password based on numbers provided for each character. For example, the user mobile number is 9000312452 then the user can select the characters based on the numbers. Based on those numbers the password will be saaaw”%9T% which can be easily remembered by using the numbers.

C. Click Points to Protect Information

After the successful login of the user then to upload the data the user is provided with an image and asked to click on points before uploading the information. In PassPoints, passwords consist of a sequence of click points on a given image. Users may select any pixels in the image as click-points for their password. To download, they repeat the sequence of clicks in the correct order, within a system-defined tolerance square of the original click-points.

Although PassPoints is relatively usable, security weaknesses make passwords easier for attackers to predict. Although it is vulnerable and can be attacked easily but to view the information first the user has to break the captcha password.

Figure 6 shows the dataflow diagram of the user after the successful login using normal password along with captcha password.

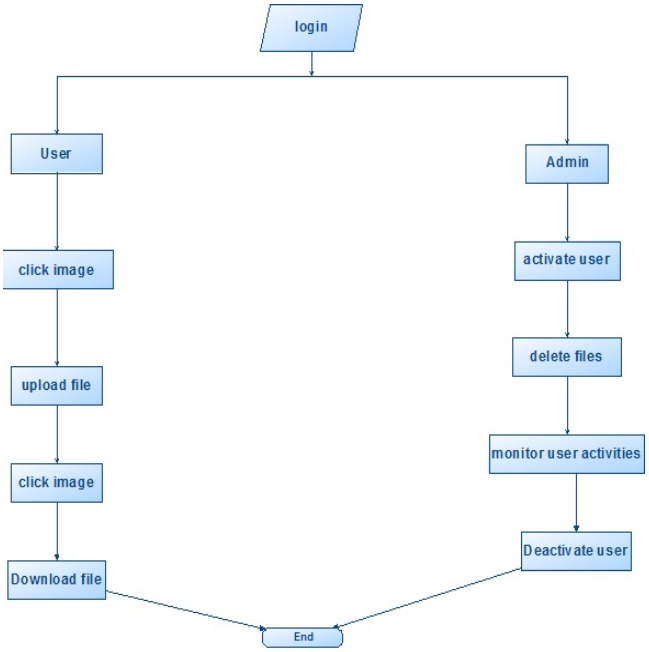

Fig.6. Dataflow diagram of user activities

Figure 7 shows that after the login of the user, an image is provided to select points before uploading file. The file can be saved successfully. To download the file the user has to select the same points otherwise access denied to download the file.

The user can enter to upload or download file only after successful login of captcha password. Click points adds some more protection along with captcha password to protect the information.

Fig.7. Click points selection to upload information

V. Security Analysis

A. Dictionary attack

In Captcha Password scheme dictionary attack is possible but the user can select very lengthy password and can remember easily so it can increase time span to break the password.

B. Guessing

The most basic guessing attack is Brute-force attack. The guessing is not easy here because normal password and captcha password should match to authenticate.

C. Shoulder Surfing

Shoulder surfing is not possible while typing passwords but it can be possible while uploading the file. But to view the information of the user it is not easy because it is protected by the captcha password.

d. Classes of Attack

These are just some example speeds, I'd be interested to hear from people with more information about the speed taken to crack various types of passwords with various hardware.

Class A: 10,000 Passwords/sec
Typical for recovery of Microsoft Office passwords on a Pentium 100

Class B: 100,000 Passwords/sec
Typical for recovery of Windows Password Cache (.PWL Files) passwords on a Pentium 100

Class C: 1,000,000 Passwords/sec
Typical for recovery of ZIP or ARJ passwords on a Pentium 100

Class D: 10,000,000 Passwords/sec
Fast PC, Dual Processor PC.

Class E: 100,000,000 Passwords/sec
Workstation or multiple PC's working together.

Class F: 1,000,000,000 Passwords/sec
Typical for medium to large scale distributed computing, Supercomputers.

Class A, B and C can take long time to break the passwords.

Password		Class of Attack		
Length	**Combinations**	**Class D**	**Class E**	**Class F**
2	9216	Instant	Instant	Instant
3	884,736	Instant	Instant	Instant
4	85 Million	8½ Secs	Instant	Instant
5	8 Billion	13½ Mins	1¼ Mins	8 Secs
6	782 Billion	22 Hours	2 Hours	13 Mins
7	75 Trillion	87 Days	8½ Days	20 Hours
8	7.2 Quadrillion	23 Years	2¼ Years	83½ Days

Table.1. Time to Break the Passwords

Table 1 shows the time taken for different type class of attacks to break the passwords.

As the captcha password is provided with minimum length of 8 characters so the minimum time to decrypt a captcha password is 83½ Days. This is only to break the captcha password but the normal password is combined with the captcha password so it takes even more time to break the password.

VI. Conclusion

A major advantage of proposed scheme is that it provides larger password space using captcha as passwords. For Captcha passwords there is a rising interest is that they are better than the Text based passwords, while the important argument for captcha passwords are that people are better at memorizing captcha passwords than text-based passwords. Also the proposed system removes the shoulder surfing attack. Along with this it also provides protection of information using click points.

References

[1] J. Yan, A. Blackwell, R. Anderson, and A. Grant, "The Memorability and Security of Passwords," Security and Usability: Designing Secure Systems That People Can Use, L. Cranor and S. Garfinkel, eds., ch. 7, pp. 129-142, O'Reilly Media, 2005.

[2] L. von Ahn, M. Blum, N. J. Hopper, and J. Langford, "CAPTCHA: Using hard AI problems for security," in *Proc. Eurocrypt*, 2003, pp. 294–311.

[3] L. O'Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication," Proc. IEEE, vol. 91, no. 12, pp. 2019 2020, Dec. 2003.

[4] L. O'Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication," Proc. IEEE, vol. 91, no. 12, pp. 2019 2020, Dec. 2003.

[5] G. E. Blonder, "Graphical passwords," in Lucent Technologies, Inc., Murray H*ill, NJ*, U. S. Patent, Ed. United States, 1996

[6] Captcha as Graphical Passwords—A New Security Primitive Based on Hard AI Problems Bin B. Zhu, Jeff Yan, Guanbo Bao, Maowei Yang, and Ning Xu, IEEE Transactions on Information Forensics and Security. 9, NO. 6, JUNE 2014

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

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

[9] 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.

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

[11] A. E. Dirik, N. Memon, and J.-C. Birget, "Modeling user choice in

the passpoints graphical password scheme," in *Proc. Symp. Usable Privacy Security*, 2007, pp. 20–28.
[12] J. Thorpe and P. C. van Oorschot, "Human-seeded attacks and exploiting hot spots in graphical passwords," in *Proc. USENIX Security*, 2007, pp. 103–118.
[13] P. C. van Oorschot, A. Salehi-Abari, and J. Thorpe, "Purely automated attacks on passpoints-style graphical passwords," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 3, pp. 393–405, Sep. 2010.
[14] B. Fogg, Persuasive Technologies: Using Computers to Change What We Think and Do. Morgan Kaufmann Publishers, 2003.
[15] J. Yan and A. S. El Ahmad, "A low-cost attack on a Microsoft CAPTCHA," in *Proc. ACM CCS*, 2008, pp. 543–554.
[16] G. Mori and J. Malik, "Recognizing objects in adversarial clutter," in *Proc. IEEE Comput. Society Conf. Comput. Vis. Pattern Recognit.*, Jun. 2003, pp. 134–141.
[17] G. Moy, N. Jones, C. Harkless, and R. Potter, "Distortion estimation techniques in solving visual CAPTCHAs," in *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit.*, Jul. 2004, pp. 23–28.
[18] K. Chellapilla, K. Larson, P. Simard, and M. Czerwinski, "Computers beat humans at single character recognition in reading-based human interaction proofs," in *Proc. 2nd Conf. Email Anti-Spam*, 2005, pp. 1–3.
[19] K. Chellapilla, K. Larson, P. Simard, and M. Czerwinski, "Building segmentation based human-friendly human interaction proofs," in *Proc. 2nd Int. Workshop Human Interaction Proofs*, 2005, pp. 1–10.
[20] B. Pinkas and T. Sander, "Securing passwords against dictionary attacks," in *Proc. ACM CCS*, 2002, pp. 161–170.