SHUFFLED INPUT GRAPHICAL PASSWORD AUTHENTICATION SCHEMES BUILT ON CAPTCHA TECHNOLOGY

Vikas K. Kolekar
Assistant Professor, Department of Computer Engineering, VIIT, Pune, INDIA

Milindkumar B. Vaidya
Assistant Professor, Department of Computer Engineering, AVCOE, Sangamner, INDIA

ABSTRACT

When we consider the online service or desktop application there is major issue of security breaching. Old password schemes has some drawbacks like hacking of password, shoulder-surfing attack as far as password is concern, online password guessing attack, relay attack. Hence there must be system that provides good solution for such password cracking attacks. There are many solutions for it and various password schemes available that achieves this. The main drawback of these schemes is that users have to deal with complicated and tedious steps as far as registration and login of user is concern as its logic contains some intense AI processes. These complicated AI processes are exhaustive for common user of the system. In this paper we proposed authentication scheme which consist of graphical password based captcha challenge image. It consists of both a captcha and a graphical password schemes. We extend the use of captcha as human present recognition as well as graphical password hence it provides all benefits of captcha and make system more powerful from security point of view.

INTRODUCTION

Cracking password is regular practice. These practices are like online guessing attack, online dictionary attack, shoulder surfing etc. Such attacks raise a big question to the security of system. In the current era, captcha is used as standard internet security technique to protect online email, online registration and other services from being abused by bots. Hence it is a challenging and open problem to design such system that are efficient and having smart approach towards hard AI problems as far as security primitives are concern. This motivated us to focus on underexplored capabilities of captcha. In this paper we extend the capabilities and schemes discussed by Bin B. Zhu et.al in [1]. To explore the solutions for security and enhance its features captcha as password technique found great advantages which is efficient to avoid bot and online guessing attacks. Automatic trail and human guessing attacks are also serious problems from security point of view. There must be a system that provides a smart and efficient solution for these attacks.

EXISTING SYSTEM

Already captcha based systems are developed where captcha is used for login authentication. Passface system [3], in this for proper login process user needs to recognize correct faces in several rounds where order is not important. These bunches of faces are decided at time of registration. System named Story [4] is similar to Passface but at time of login recognizing sequential order of face clicks are important. Déjà vu [5] was also system which uses large set of computer generated random art images. Requirement of cognitive authentication [6] was in focus, in this system user requires a path to be generated through a panel of images. When drawbacks of above said systems are considered. There are also some systems that discussed in [7] [8] [9] works on it. These systems used recall-based schemes in which user needs to regenerate the same interaction result without cueing. After recall based schemes, cued-recall techniques were used. In this an external cue is provided to help memorize and enter a password. There are systems like Pass Points [10], Cued Click Points (CCP) [11] and Persuasive Cued Click Points (PCCP) [12] which work on cued-recall technique. Among these types, recognition is considered the easiest for human memory whereas pure recall is the hardest. Online guessing attacks are difficult to defend against recognition schemes. Experimentally [13] it is proved that recognition schemes can be broken by guessing attack using dictionary with massive entries and hotspot still remain the problem. Basically there are two types of catches: 1. Text Captcha, 2.

Image Recognition Captcha. Among this image recognition by machine is critical task. Hence image recognition part is fixed when we consider captcha as a password scheme. To use captcha in authentication there was system [14] that uses captcha and password in a user authentication protocol, which was called Captcha-based Password Authentication (CbPA) protocol. Drawback of this protocol is that captcha is an independent entity used together with a text or graphical password. On the contrary, our proposed system consists of captcha and a graphical password which are intrinsically combined into a single entity. To provide good solution for brute force attack, automatic guessing attack and human guessing attack proposed system implements different and dynamic approach.

PROPOSED SYSTEM

Shuffle Input is a recognition based scheme with shuffled input. In this scheme we used captcha as graphical password and as a part of contribution we introduced the following options to it.

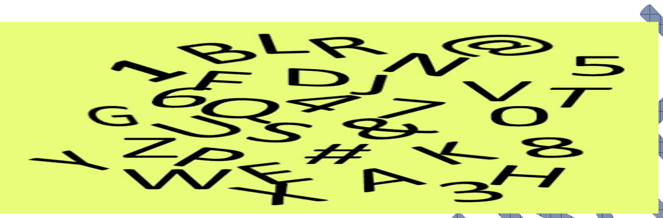

Figure 1: Captcha challenge image for Shuffle Input scheme.

OPTION 1: SHUFFLED PASSWORD

In this option user will get captcha challenge image having alphabets, numbers and special characters on it. In option 1, user can provide his password in shuffled way. For example, if password, P = {"h", "e", "l", "l", "o"} then user can provide "llohe" or "helol" etc. While login user first has to select the option 1 from drop down menu followed by clicking shuffled password. Then authentication server verifies user name and fetch its original password. After that it checks the option if it is registered option then it allows all possible combinations of password alphabets. Each time user can provide combination of his original password hence it is a smart solution for shoulder-surfing as well as dictionary attack.

OPTION 2: REVERSED PASSWORD

In this option user will get captcha challenge image having alphabets, numbers and special characters on it. In option 2, user can provide his password in reverse way. For example, if password, P = {"h", "e", "l", "l", "o"} then user can provide "olleh". While login into system, user first has to select the option 2 from drop down menu followed by clicking reverse password. Then authentication server verifies user name and fetch its original password. After that it checks the option if it is registered option then it allows reverse of password alphabets. Each time user can provide reverse of his original password hence it is a smart solution for shoulder-surfing and dictionary attack.

OPTION 3: SKIPPED PASSWORD

In this option user will get captcha challenge image having alphabets, numbers and special characters on it. In option 3, user can provide his password by skipping particular words from his password in sequence. For example, if P = {"h", "e", "l", "l", "o"} is password then user can jump over one character in sequence then user can provide "hlo" etc. To login user first has to select the option 3 from drop down menu followed by clicking skipped sequence of password. Then authentication server verifies user name and fetch its original password. After that it checks the option if it is registered then it allows skipped sequence of password alphabets. Each time user can provide skipped sequence of password of his original password hence it is a smart solution for shoulder surfing, dictionary attack and online guessing attacks.

SECURITY ANALYSIS

The complexity of proposed scheme i.e. shuffled input scheme is exponentially dependent on number of objects/characters M in the scheme and polynomially dependant on size N of captcha object/character.

Hence, it can be represented as: $C=\alpha MP(N)$, where, α is a parameter >1 and P( ) is polynomial function. The complexity to break captcha challenge image is $\alpha MP(N)/(\alpha kP(N))$. Where, k is length of password object/ characters. As we increase the password space the complexity to break the captcha challenge image also increases.

CONCLUSION

We used click based captcha as graphical password and based on that we proposed and implemented shuffled input password scheme. With the correct use of image processing and AI techniques, we provided solution to online password guessing attack, dictionary attack, and relay attack. Application of proposed system is used to offer reasonable security and usability and appears to fit well with some practical systems for improving online security. This concept is also useful for desktop applications. Overall, we provided smart solutions as far as password security and attacks are concerned with the help of AI.

ACKNOWLEDGEMENT

We would like to thank family members and friends who knowingly or unknowingly helped us in this work.

REFERENCES

[1] Bin B. Zhu, Jeff Yan, Guanbo Bao, Maowei Yang, and Ning Xu, "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.

[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] (2012, Feb.) The Science Behind Passfaces [Online]. Available: http://www.realuser.com/published/ScienceBehindPassfaces.pdf

[4] D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes," in Proc. 13th USENIX Security Symposium, San Diego, CA, 2004.

[5] R. Dhamija and A. Perrig, "Déjà Vu: A user study using images for authentication," in Proc. 9th USENIX Security, 2000.

[6] D. Weinshall, "Cognitive authentication schemes safe against spyware," in Proc. IEEE Symp. Security Privacy, May 2006, pp. 300–306.

[7] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The design and analysis of graphical passwords," in Proc. 8th USENIX Security Symp., pp. 1–15,1999.

[8] 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.

[9] P. Dunphy and J. Yan, "Do background images improve 'Draw a Secret' graphical passwords?," in Proc. ACM CCS, 2007.

[10] 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, Jul. 2005.

[11] S. Chiasson, P. C. van Oorschot, and R. Biddle, "Graphical password authentication using cued click points," in Proc. ESORICS, 2007, pp. 359–374.

[12] S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot, "Influencing users towards better passwords: Persuasive cued click-points," in Proc. Brit. HCI Group Annu. Conf. People Comput., Culture, Creativity, Interaction, vol. 1, pp. 121–130, 2008.

[13] P. C. van Oorschot and J. Thorpe, "On predictive models and User-Drawn Graphical passwords," ACM Trans. Inf. Syst. Security, vol. 10, no. 4, 2008.

[14] B. Pinkas and T. Sander, "Securing passwords against dictionary attacks," in Proc. ACM CCS, 2002, pp. 161–170.

[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] 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

[17] 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, pp. 1–10.

[18] 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, pp. 760–767.

[19] M. Szydlowski, C. Kruegel, and E. Kirda, "Secure input for web applications," in Proc. ACSAC, 2007, pp. 375–384.

[20] 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.

[21] G. E. Blonder, "Graphical passwords," Lucent Technologies, Inc., Murray Hill, NJ, U. S.Patent,Ed. United States, 1996.

[22] S. Chiasson, R. Biddle.and P. van. Oorschot, "A Second Look at the Usability of Click-Based Graphical Passwords," Proceedings ACM Symp.Usable Privacy and Security(SOUPS),July 2007.

[23] S. Chiasson, A. Forget, E. Stobert, P. van Oorschot, and R. Biddle, "Multiple Password Interference in Text and Click-Based Graphical Passwords," Proceedings ACM ConferenceComputer and Comm. Security (CCS), Nov. 2009.

[24] L.Sobrado and J.C.Birget, "Graphical passwords," The Rutgers Scholar, An ElectronicBulletin for Undergraduate Research, vol. 4, 2002.

[25] E.Stobert, A.Forget, S.Chiasson, P.van Oorschot, and R.Biddle, "Exploring Usability Effects of Increasing Security in Click-Based Graphical Passwords," Proceedings AnnualComputer Security Applications Conference(ACSAC), 2010.

[26] S.Chiasson, A.Forget, R.Biddle, and P.C.van Oorschot, "User Interface Design AffeectsSecurity: Patterns in Click-Based Graphical Passwords," International Journal of Information Security, vol. 8, no. 6, pp. 387-398. 2009.

[27] W. Jansen, "Authenticating Mobile Device Users Through Image Selection," Data Security,2004.

[28] D.Weinshall and S.Kirkpatrick, "Passwords Youll Never Forget,but Cant Recall," Proceedings of Conference on Human Factors in Computing Systems(CHI). Vienna, Austria:ACM, 2004, pp. 1399-1402.

[29] W.Jansen, S.Gavrila, V.Korolev, R.Ayers, and R.Swanstrom, "Picture Password: A VisualLogin Technique for Mobile Devices," National Institute of Standards and TechnologyInteragency Report NISTIR 7030, 2003.

[30] K. Gilhooly, "Biometrics: Getting Back to Business," Computerworld. May 09, 2005.

[31] M. Motoyama, K. Levchenko, C. Kanich, D. McCoy, G. M. Voelker, and S. Savage, "Re: CAPTCHAs—Understanding CAPTCHA-solving Services in an Economic Context," in Proc. USENIX Security, 2010, pp. 435-452.

J. Elson, J. R. Douceur, J. Howell, and J. Saul, "Asirra: A CAPCTHA that exploits interest-aligned manual imag