International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com Volume 2, Issue 6 (Nov-Dec 2014), PP. 12-14

CARP: AN IMAGE BASED SECURITY USING I-PAS

Sayli N Kokate[1], Manasi P Khade[2], Priyanka D Patil[3], Ashwini B Gawali[4], Archana C Lomte[5]
Computer Department
JSPM's BSIOTR
Pune,India
[1]sayleekokate24@gmail.com, [2]mkhade1993@gmail.com, [3]priyanka.patil119@gmail.com,
[4]ashgawali0192@gmail.com, [5]archanalomte@gmail.com

Abstract— A CAPTCHA means "Completely Automated Public Turing test to tell Computers and Humans Apart". It is a type of challenge-response test used in computing to determine whether or not the user is human. CaRP is both a Captcha and a graphical password scheme. CaRP addresses a number of security problems altogether, such as online guessing attacks, relay attacks, and, if combined with dual-view technologies, shoulder-surfing attacks. Particularly, a CaRP password can be found only probabilistically by automatic online guessing attacks, even if the password is in the search set. CaRP also offers an approach to address the well-known image hotspot problem in popular graphical password systems, such as PassPoints, which often leads to weak password choices. Thus, a variant to the login/password scheme, using graphical scheme was introduced. But it also suffered due to shoulder-surfing and screen dump attacks. Thus it introduces a framework to proposed (IPAS) Implicit Password Authentication System, which is protected to the common attacks suffered by other authentication schemes.

Index Terms — Authentication, Graphical Password, Security, CaRP, Captcha, dictionary attack, password guessing attack, security primitive.

I. INTRODUCTION

Authentication is a process of determining whether a particular individual or a device should be allowed to access a system or an application or just an object running in a device. This is an important process which assures the basic security goals, confidentiality and integrity. Graphical-based password techniques have been proposed as a potential alternative to text-based techniques. On the other hand, it is also difficult to break graphical passwords using normal attacks such as dictionary attack, brute force and spyware which have been affecting text-based and token-based authentication. The security level of graphical based authentication schemes is higher than other authentication techniques. In general, the graphical password techniques can be classified into two categories: recognition-based and recall based graphical techniques.

Captcha technology, which is also call CaRP (Captcha as graphical Passwords) .CaRP, is click-based graphical passwords, where a sequence of clicks on an image is used to derive a password. Unlike other click-based graphical passwords, images used in CaRP are Captcha challenges, and a new CaRP image is generated for every login attempt. Carp 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 general and considered as a top cyber security risk. Graphical-based password techniques have been proposed as a probable alternative to text-based techniques, supported partially by the fact that humans can remember images better than text. CaRP is not a solution, but it offers reasonable security and usability and appears to fit well with some real applications for improving online security.

Authentication System implicitly presented information to the user. If the user "clicks" the same grid-of-interest compared with the server, the user is implicitly authenticated. No password information is exchanged between the client and the server in IPAS. IPAS may require human-interaction and careful selection of images and "click" regions

II. BACKGROUND AND RELATED WORK

A. VARIOUS AUTHENTICATION SCHEMES

There are several authentication schemes available in the literature. They can be classified as follows:

1) What you know
2) What you have and
3) What you are

The traditional username/password or PIN based authentication scheme is an example of the "what you know type". Smartcards or electronic tokens are examples of "what you have type of authentication" and finally biometric based authentication schemes are examples of the "what you are" type of authentication. They can be classified into three categories according to the task involved in memorizing and entering passwords: recognition, recall, and cued recall.

A recognition-based scheme requires identifying among the visual objects belonging to a password selection. A typical scheme is Passfaces wherein a user selects a selection of faces from a database in creating a password. During authentication, a panel of candidate faces is presented for the user to select the face belonging to her selection. This process is repeated a number of rounds, each round with a different panel. A successful login requires correct selection in each round.

A recall-based scheme requires a user to regenerate the same interaction result without cueing. Draw-A-Secret (DAS) was the first recall-based scheme proposed. A user draws her password on a 2D grid. The system encodes the sequence of grid cells along the drawing path as a user drawn password.

In a cued-recall scheme, an exterior cue is provided to help memorize and enter a password. PassPoints is a click-based cued-recall scheme wherein a user clicks a sequence of points anywhere on an image in creating a password, and re-clicks the same sequence during authentication. Cued Click Points (CCP) is similar to PassPoint sbut uses one image per click, with the next image selected by a deterministic function. Among the three types, recognition is considered the easiest for human memory whereas pure recall is the hardest.

B. CAPTCHA AS GRAPHICAL AUTHENTICATION

Captcha was also used with recognition-based graphical passwords to address spyware, wherein a text Captcha is displayed below each image; a user locates her own pass-

images from distraction images, and enters the characters at specific locations of the Captcha below each pass-image as her password during authentication. These specific locations were selected for each pass-image during password creation as a part of the password. Captcha is an independent entity, used together with a text or graphical password. On the contrary, a CaRP is both a Captcha and a graphical password scheme, which are basically combined into a single entity.

Captcha is used to protect complex user inputs on an un-trusted client. This protects the communication channel between user and Web server from key loggers and spyware, while CaRP is a family of graphical password schemes for user authentication

CaRP 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.

CaRP requires solving a Captcha challenge in every login. This impact on usability can be mitigated by adapting the CaRP image's difficulty level based on the login history of the account and the machine used to log in.

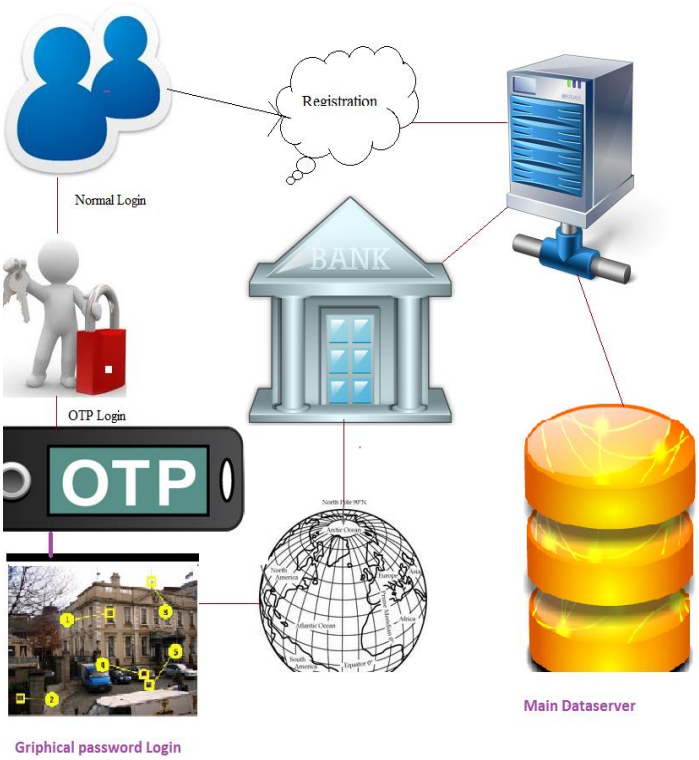

Figure 1. Graphical Authentication

III. Recognition Techniques

A. ClickText Techniques:

ClickText is a recognition-based CaRP scheme built on to for text Captcha. Its alphabet comprise characters without any visually-confuse characters. For example, Letter "O" and digit "0" may cause confusion in CaRP images, and thus one character should be excluded from the alphabet. A ClickText password is a sequence of characters in the alphabet, e.g., "MA#9KD39", which is similar to a text password. A ClickText image is created by the original Captcha engine as if a Captcha image were generated except that all the alphabet characters should appear in the image.

B. Pure Recall-Based Techniques:

In this users need to reproduce their passwords without any help or reminder by the system.Following are some techniques of Pure Recall-Techniques

1. Draw-A-Secret Technique(DAS):

In this scheme, the password is a shape drawn on a two-dimensional grid of size G * G as in Figure. Each cell in this grid is represented by different rectangular coordinates (x, y). The values of touch grids are stored in sequential order of the drawing.

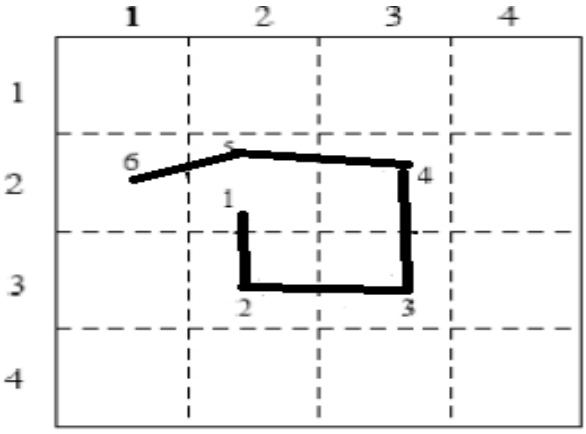

Figure 2. Secret 4*4 Grid

2. Grid selection:

Grid selection where the selection grid is large at the beginning, A fine grained grid from which the person selects a drawing grid, a rectangular area to zoom in on, in which they may enter their password as shown in Figure. This technique would increase the password space of DAS, which improves the security level at the same time.

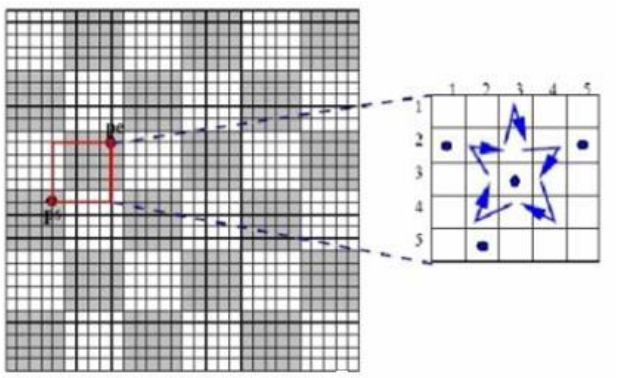

Figure 3. Grid Selection

3. Passdoodle:

Passdoodle is a graphical password of handwritten drawing or text, normally sketched with a stylus over a touch sensitive screen as shown in Figure

Figure 4. Passdoodle

C. Cued Recall-Based Techniques

In this technique, the system gives some hints which help users to reproduce their passwords with high accuracy. These hints will be presented as hot spots (regions) within an image. The user has to choose some of these regions to register as their password and they have to choose the same region following the same order to log into the system. The user must remember the "chosen click spots" and keep them secret.

D. PassPoint

The Passpoint system has a large password space, which improves the security level compared with other similar systems. For example, five or six click points on an image can produce more passwords than 8-character text-based passwords with standard 26-character alphabet. For more security, the Passpoint system stores the image password in a hashed (encrypted) form in the password file.

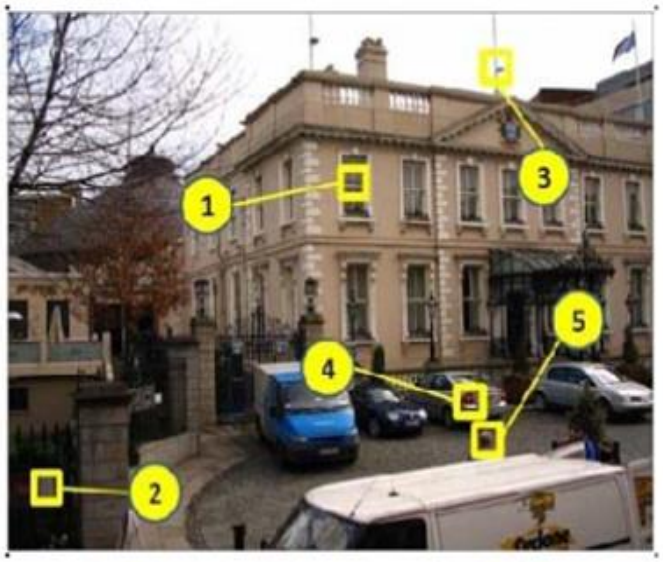

Figure 5. Pass Point

IV. Conclusion

We have proposed CaRP, a new security primitive based on I-pas. CaRP is both a Captcha and a graphical password scheme. The notion of CaRP introduces a new family of graphical passwords, which adopts a new approach to counter online guessing attacks: a new CaRP image, which is also a Captcha challenge. No password information is exchanged between the client and the server in IPAS If the user "clicks" the same grid-of-interest compared with the server, the user is implicitly authenticated. Since the authentication information is conveyed implicitly, IPAS can tolerate shoulder-surfing and screen dump attack, which none of the existing schemes can tolerate. A password of CaRP can be found only probabilistically by automatic online guessing attacks including brute-force attacks, a desired security property that other graphical password schemes lack. Hotspots in CaRP images can no longer be exploited to mount automatic online guessing attacks, an inherent vulnerability in many graphical password systems. CaRP forces adversaries to resort to significantly less efficient and much more costly human-based attacks. In addition to offering protection from online guessing attacks, CaRP is also resistant to Captcha relay attacks, and, if combined with dual-view technologies, shoulder-surfing attacks. CaRP can also help reduce spam emails sent from a Web email service.

References

[1] Sabzevar, A.P. & Stavrou, A., 2008," Universal Multi-Factor Authentication Using Graphical Passwords", IEEE International Conference on Signal Image Technology and Internet Based Systems (SITIS).

[2] Renaud, K. (2009)."On user involvement in production of images used in visual authentication." J. Vis. Lang. Comput. 20(1): 1-15.

[3] Masrom, M., F. Towhidi, et al. (2009). "Pure and cued recall-based graphical user authentication", Application of Information and Communication Technologies, 2009. AICT 2009. International Conference.

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

[5] S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, N. Memon, ``PassPoints: Design and longitudinal evaluation of a graphical password system", International J. of Human-Computer Studies (Special Issue on HCI Research in Privacy and Security), 63 (2005) 102-127.

[6] Xiaoyuan, S., Z. Ying, et al. (2005). "Graphical passwords: a survey", Computer Security Applications Conference, 21st Annual.

[7] Birget, J. C., H. Dawei, et al. (2006). "Graphical passwords based on robust discretization", Information Forensics and Security, IEEE Transactions on 1(3): 395-399.

[8] 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.

[9] 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.

[10] 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, pp. 1–9.

[11] J. Bonneau, "The science of guessing: Analyzing an anonymized corpus of 70 million passwords," in Proc. IEEE Symp. Security Privacy, Jun. 2012, pp. 20–25.

[12] D. Hong, S. Man, B. Hawes, and M. Mathews, "A password scheme strongly resistant to spyware," in Proceedings of International conference on security and management. Las Vergas, NV, 2004.

[13] S. Man, D. Hong, and M. Mathews, "A shoulder-surfing resistant graphical password scheme," in Proceedings of International conference on security and management. Las Vegas, NV, 2003.

[14] L. D. Paulson, "Taking a Graphical Approach to the Password," Computer, vol. pp. 19, 2002.

[15] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Basic results," in Human-Computer Interaction International (HCII 2005). Las Vegas, NV, 2005.