International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume 2, Issue 1 (January '2016)

CCP: GRAPHICAL PASSWORD AUTHENTICATION

Kanifnath Kolhe,
Department Of Computer Engineering,
ISB&M School Of Technology,
Pune, India.

Aditya Pisal,
Department Of Computer Engineering,
ISB&M School Of Technology,
Pune, India.

Santosh Anarase,
Department Of Computer Engineering,
ISB&M School Of Technology,
Pune, India.

Prof.Komal Jagdale,
Department Of Computer Engineering,
ISB&M School Of Technology,
Pune, India.

Abstract: Graphical password is one of the alternative solutions to alphanumeric password as it is very tedious process to remember alphanumeric password. When any application is provided with user friendly authentication it becomes easy to access and use that application. One of the major reasons behind this method is according to psychological studies human mind can easily remember images than alphabets or digits. In this paper we are representing the authentication given to cloud by using graphical password. We have proposed cloud with graphical security by means of image password. We are providing one of the algorithms which are based on selection of username and images as a password. By this paper we are trying to give set of images on the basis of alphabet series position of characters in username. Finally cloud is provided with this graphical password authentication.

Keywords: Graphical Password, CCP, Cloud Security, Psychological, Authentication, Image Password

I. INTRODUCTION

Security is most important in our daily life. CAPTCHA standing for Completely Automated Public Turing test to tell Computers and Humans Apart, is an automatic challenge-response test to distinguish between humans and machines. Captcha is used for protection against different attack i.e. bot. In image based Captcha is click based graphical passwords, where sequence of clicks on an image is used to derive a password. It provides protection against online dictionary attacks on password. In this for login every time click on images. Captcha can be applied on touch screen devices where on typing passwords is not more secure, especially for secure internet applications. In early system only text password is used which is very difficult to remember if enter a long password. If we use smaller password then it can be easily identify and we also use common password for many accounts so for that Image based Captcha provide more security during authentication.

a) Cued Click Points

In this paper, we propose a new click-based graphical password scheme called Cued Click Points (CCP). A password consists of one click-point per image for a sequence of images. 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. CCP offers both improved usability and security. Users had high success rates, could quickly create and re-enter their passwords, and were very accurate when entering their click-points. Participants rated the system positively and indicated that they preferred CCP to a Pass Points-style system. They also said that they appreciated the immediate implicit feedback telling them whether their latest click-point was correctly entered. CCP appears to allow greater security than Pass Points; the workload for attackers of CCP can be arbitrarily increased by augmenting the number of images in the system. As with most graphical passwords, CCP is not intended for environments where shoulder-surfing is a serious threat.

II. SHORT SURVEY OF RELEVANT SURVEY

A. GRAPHICAL PASSWORD LEARNING FROM FIRST TWELVE YEARS[1]

Starting around 1999, a great many graphical password schemes have been proposed as alternatives to text-based password authentication. We provide a comprehensive overview of published research in the area, covering both usability and security aspects as well as system evaluation. The article first catalogues existing approaches, highlighting novel features of selected schemes and identifying key usability or security advantages. We then review usability requirements for knowledge-based authentication as they apply to graphical passwords, identify security threats that such systems must address and review known attacks, discuss

methodological issues related to empirical evaluation, and identify areas for further research and improved methodology.

B. *PASS-GO: A PROPOSAL TO IMPROVE THE USABILITY OF GRAPHICAL PASSWORDS*

Inspired by an old Chinese game, Go, we have designed a new graphical password scheme, Pass-Go, in which a user selects intersections on a grid as a way to in- put a password. While offering an extremely large full password space (256 bits for the most basic scheme), our scheme provides acceptable usability, as empirically demonstrated by, to the best of our knowledge, the largest user study (167 subjects involved) on graphical passwords, conducted in the fall semester of 2005 in two university classes. Our scheme supports most application environments and input devices, rather than being limited to small mobile devices (PDAs), and can be used to derive cryptographic keys. We study the memorable password space and show the potential power of this scheme by exploring further improvements and variation mechanisms.

C. *ON PREDICTIVE MODELS AND USER DRAWN GRAPHICAL PASSWORDS*

In commonplace text-based password schemes, users typically choose passwords that are easy to recall, exhibit patterns, and are thus vulnerable tobrute-force dictionary attacks. This leads us to ask whether other types of passwords (e.g., graphical) are also vulnerable to dictionary attack because of users tending to choose memorable passwords. We suggest a method to predict and model a number of such classes for systems where passwords are created solely from a user's memory. We hypothesize that these classes define weak password subspaces suitable for an attack dictionary. For user-drawn graphical passwords, we apply this method with cognitive studies on visual recall. These cognitive studies motivate us to define a set of password com- plexity factors (e.g., reflective symmetry and stroke count), which define a set of classes. To better understand the size of these classes and, thus, how weak the password subspaces they define might be, we use the Draw-A-Secret (DAS) graphical password scheme of Jermyn et al. [1999] as an example. We analyze the size of these classes for DAS under convenient parameter choices and show that they can be combined to define apparently popular subspaces that have bit sizes ranging from 31 to 41a surprisingly small proportion of the full password space (58 bits). Our results quantitatively support suggestions that user-drawn graphical password systems employ measures, such as graphical password rules or guidelines and proactive password checking.

III. EXISTING SYSTEM

Graphical password first found in 1995 by Greg Blonder [1]. Graphical password has three types there are as follows:

A. *Recognition Base Technique*

Recognition base technique contain group of images. User can select images from that group for password. Figure 1 show the recognition base technique. Using recognition base technique user set our password at the time of registration and selects same images at the time of authentication [2] [5].

Figure.1 Recognition Base System

B. *Recall Base Technique*

Using recall base technique user can draw a secrete pattern or generate a shape over the 2D grid at the time ofregistration and generate a same shape at the time of authentication. This 2D grid is provided by the system [5].

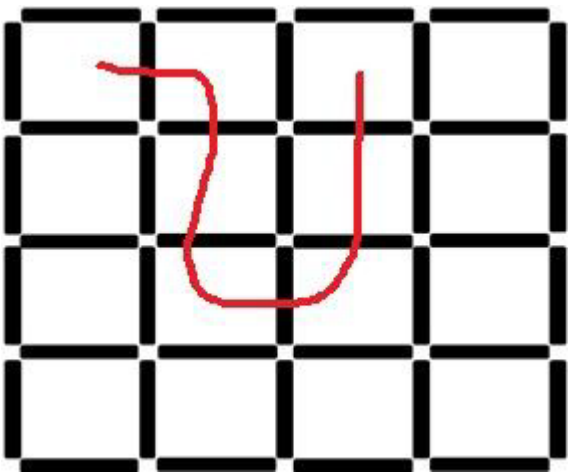

Figure.2 Recall Base Technique

C. *Cued Recall Base Technique.Please*

In this technique, system gives some hints which helps user to reproduce their password with high accuracy. Thesehints will be presented as hot spots within image. The user has chosen some of these regions to register their password.But this technique is not easy to use; because the click position is not on specific point then user cannot access hisinformation [6] [8].

Figure3. Cued Recall Base Technique

IV. DISADVANTAGES OF EXISTING SYSTEM

This paradigm has achieved just a limited success as compared with the cryptographic primitives based on hard math problems and their wide applications.

Using hard AI (Artificial Intelligence) problems for security, initially proposed in, 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.

V. PROPOSED SYSTEM

The proposed system is a three level security combination of graphical password using the technique cued click point and a one-time session key. It overcomes the existing system problems and enhances the authentication process.

We have designed a new graphical password scheme, Pass-Go, in which a user selects intersections on a grid as a way to in- put a password. While offering an extremely large full password space (256 bits for the most basic scheme), our scheme provides acceptable usability, as empirically demonstrated by, to the best of our knowledge, the largest user study (167 subjects involved) on graphical passwords, conducted in the fall semester of 2005 in two university classes. Our scheme supports most application environments and input devices, rather than being limited to small mobile devices (PDAs), and can be used to derive cryptographic keys. We study the memorable password space and show the potential power of this scheme by exploring further improvements and variation mechanisms.

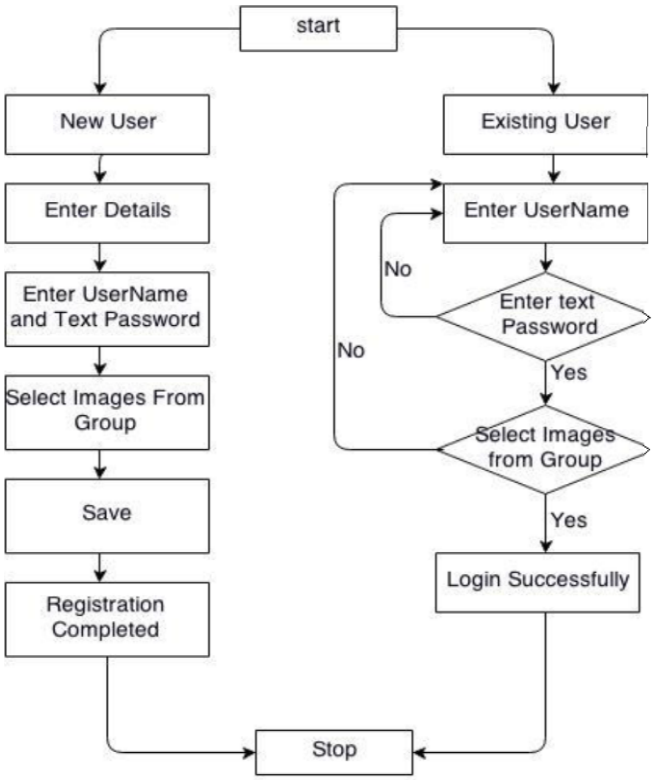

Figure4. System Architecture

VI. CONCLUSION

We have proposed CaRP, another security primitive depending on unsolved hard AI issues. CaRP is both a Captcha and a graphical secret word plan. The thought of CaRP presents another group of graphical passwords, which receives another way to deal with counter web speculating assaults: another CaRP picture, which is additionally a Captcha test, is utilized for each login endeavor to make trials of a web speculating assault computationally free of one another. A watchword of CaRP can be discovered just probabilistically via programmed internet speculating assaults including savage power assaults, a sought security property that other graphical secret word plans need. Hotspots in CaRP pictures can never again be abused to mount programmed internet speculating assaults, an inborn defenselessness in numerous graphical secret word frameworks. CaRP powers enemies to fall back on fundamentally less productive and significantly more expensive human based assaults. Notwithstanding offering assurance from internet speculating assaults, CaRP is additionally impervious to Captcha transfer assaults, and if joined with double view technologies, shoulder-surfing assaults. CaRP can likewise lessen spam messages sent from a Web email administration.

VII. REFERENCES

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

[2] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, The design and analysis of graphical passwords, in Proc. 8th USENIX Security Symp., 1999, pp. 115

[3] 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. 273292,2008.

[4] 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. 102127, Jul. 2005.

[5] P. C. van Oorschot and J. Thorpe, On predictive models and userdrawn graphical passwords, ACM Trans. Inf. Syst. Security, vol. 10, no. 4, pp.133, 2008.

[6]] K. Golo_t, Click passwords under investigation, in Proc. ESORICS, 2007,pp. 343358.

[7] 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. 2028.39

[8] J. Thorpe and P. C. van Oorschot, Human-seeded attacks and exploiting hot spots in graphical passwords, in Proc. USENIX Security, 2007,pp.103118

[9] Birget, J.C., D. Hong, and N. Memon. Graphical Passwords Based on Robust Discretization. IEEE Trans. Info. Forensics and Security, 1(3), September 2006.