Graphical Password Authentication Using Cued Click Points

Rashmi Kale **Saba Naaz** **Chanchal Mathuria** **Rakhee Minj** **Nilesh Shelke**

***Abstract*—It has been proposed and examined the usability and security of Cued Click Points (CCP), a cued-recall graphical password technique. Users click on five points per image for a sequence of images. The next image is based on the previous click-point. We present the results of an initial user study which revealed positive results. Performance was very good in terms of speed, accuracy, and number of errors. Users preferred CCP to Pass Points (Wieden beck et al., 2005), saying they thought that selecting and remembering only one point per image was easier, and that seeing each image triggered their memory of where the corresponding point was located. It also suggest that CCP provides greater security than Pass Points because the number of images increases the workload for attackers.**

Key words: Authentication, Computer Security, Cued Box Graphical Passwords.

I. INTRODUCTION

Various graphical password schemes have been proposed as alternatives to text-based passwords. Research and experience have shown that text-based passwords are fraught with both usability and security problems that make them less than desirable solutions . Psychological studies have revealed that the human brain is better at recognizing and recalling images than text. Graphical passwords are intended to capitalize on this human characteristic in hopes that by reducing the memory burden on users, coupled with a larger full password space offered by images, more secure passwords can be produced and users will not resort to unsafe practices in order to cope .

In this paper, it has been proposed a new click-based graphical password scheme called Cued Click Points (CCP). It can be viewed as a combination of Pass Points, Pass faces and Story . A password consists of five click-points per image for a sequence of two images. The next image displayed is based on the previous click points so users receive immediate implicit feedback as to whether they are on the correct path when log in. CCP offers both improved usability and security .

Cued Click Points: A preliminary security analysis of this new scheme is also presented [1]. Hotspots (i.e. areas of the image that users are more likely to select) are a concern in click-based passwords, so CCP uses a large set of images that will be difficult for attackers to obtain. For this proposed system, hotspot analysis requires proportionally more effort by attackers, as each image must be collected and analyzed individually. 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 [2][3].

Cued Click Points (CCP), the user study and its results are available in, and an initial security analysis is given in provides an interpretation and discussion of the results including possible enhancements, while conclusions and future work appears [4].

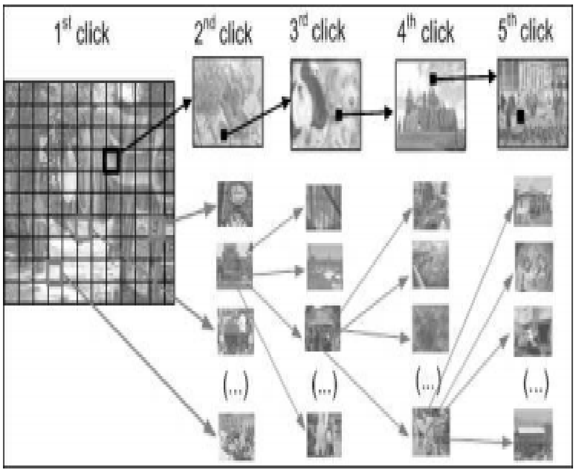


Fig.1 Cued Click Points

Drawbacks in text based passwords are as follows:

Passwords are subject to *replay attacks*: an adversary who sees your password once, perhaps by looking over your shoulder as you type it or eavesdropping on the network as your password goes by, can replay the password later. (More secure approaches use a cryptographic trick called a *zero-knowledge proof*, in which you can prove that you know a secret value but without revealing the secret to an eavesdropper.)People have a hard time picking good passwords [5].

A good password is supposed to be easy for you to remember but very, very difficult for an adversary to guess . The best password is a truly random string, but those are too hard to remember, so we tend to build patterns into our passwords, which make them easier to guess. And brute force password-guessing gets easier every year because computers get faster [6][7].

Background and Related Work: Graphical password schemes can be grouped into three general categories based on the type of cognitive activity required to remember the password recognition, recall, and cued recall [8]. Recognition is the easiest for human memory whereas pure recall is most difficult since the information must be accessed from memory with no triggers. Cued recall falls somewhere between these two as it offers a cued which should establish context and trigger the stored memory. Among existing graphical passwords, CCP most closely resembles aspects of Pass faces, Story, and Pass Points. Therefore these graphical password schemes are presented in more detail [9].

The three; in terms of implementation, it is most similar to Pass Points. It also avoids the complex user training requirements found in a number of graphical password proposals, Pass faces is a graphical password scheme based primarily on recognizing human faces [10].

During password creation, users select a number of images from a larger set. To log in, users must identify one of their pre-selected images from amongst several images. Users must correctly respond to a number of these challenges for each login. Davis et al .implemented their own version called Faces and conducted a long-term user study [11]. Results showed that users could accurately remember their images but that user-chosen passwords were predictable to the point of being insecure.

The idea of click-based graphical passwords originated with Blonder who proposed a scheme where a password consisted of a series of clicks on pre-defined regions of an image. Later, Wiedenbeck et al. proposed Pass Points, wherein passwords could be composed of several (e.g. five) points anywhere on an image. They also proposed a "robust discretization" scheme, with three overlapping grids, allowing for login attempts that were approximately correct to be accepted and converting the entered password into a cryptographic verification key.

Intuitively, it seems obvious that some areas of an image are more attractive to users as click-points [12]. If this phenomenon is too strong, the likelihood that attackers can guess a password significantly increases. If attackers learn which images are being used, they can select a set of likely hotspots through image processing tools or by observing a small set of users on the target image and then building an attack dictionary based on those points.

Recognition based techniques

Dhamija & Perrig They proposed a graphical authentication method based on the hash visualization technique. In their system the user asked to select a certain number of images from a set of random pictures generated by a program later the user will require to identify the preselected images in order to be authenticated [13]. A weakness of this system is that the server needs to store the seeds of the portfolio images of each user in plain text. Also the process of selecting a set of pictures from the picture database can be tedious and time consuming for the user.

Authentication Using Graphical Passwords:

Effects of Tolerance and Image Choice Graphical passwords are an alternative to alphanumeric passwords in which users click on images to authenticate themselves rather than type alphanumeric strings [14]. In their tolerance study, results show that accurate memory for the password is strongly reduced when using a small tolerance (10 x 10 pixels) around the user's password points. This may occur because users fail to encode the password points in memory in the precise manner that is necessary to remember the password over a lapse of time. In their image study they compared user performance on four everyday images. The results indicate that there were few significant differences in performance of the images. This preliminary result suggests that many images may support memorability in graphical password systems [15].

Graphical Passwords:

Graphical passwords refer to using pictures (also drawings) as passwords. In theory, graphical passwords are easier to remember, since humans remember pictures better than words [16][17]. Also, they should be more resistant to brute force attacks, since the search space is practically infinite. In general, graphical passwords techniques are classified into two main categories: recognition-based and recall based graphical techniques. In recognition-based techniques, a user is authenticated by challenging him/her to identify one or more images he or she chooses during the registration stage. In recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage. Pass face is a recognition-based technique, where a user is authenticated by challenging him/her into recognizing human faces. An early recall-based graphical password approach was introduced by Greg Blonder in 1996. In this approach, a user creates a password by clicking on several locations on an image.

During authentication, the user must click on those locations. Pass Points builds on Blonder's idea, and overcomes some of the limitations of his scheme.

Authentication

(From Greek: *authentikos*, "real, genuine," from "author") is the act of confirming the truth of an attribute of a single piece of data (datum) or entity. In contrast with identification which refers to the act of stating or otherwise indicating a claim purportedly attesting to a person or thing's identity, authentication is the process of actually confirming that identity.

It might involve confirming the identity of a person by validating their identity documents, verifying the validity of a Website with a digital certificate, tracing the age of an artifact by carbon dating, or ensuring that a product is what its packaging and labeling claim to be [18].

In other words, authentication often involves verifying the validity of at least one form of identification.

Cued Box:

Two major cue types are used to analyze attention based on the type of visual input. An endogenous cue is presented in the center of the screen, usually at the same location as the center of focus.

It is an arrow or other directional cue pointing to the left or right box on the screen. This cue relies on input from the central visual field [19].

An exogenous cue is presented outside of the center of focus, usually highlighting the left or right box presented on the screen. An exogenous cue can also be an object or image in the periphery, a number of degrees away from the centre, but still within the visual angle.

Computer Security:

A computer security is defined as the process of preventing a computer system from various viruses. It is security applied to computing devices such as computers and smart phones, as well as computer networks such as private and public networks, including the whole Internet. The field includes all the processes and mechanisms by which digital equipment, information and services are protected from unintended or unauthorized access, change or destruction, and is of growing importance due to the increasing reliance of computer systems in most societies. It includes physical security to prevent theft of equipment and information security to protect the data on that equipment[20].

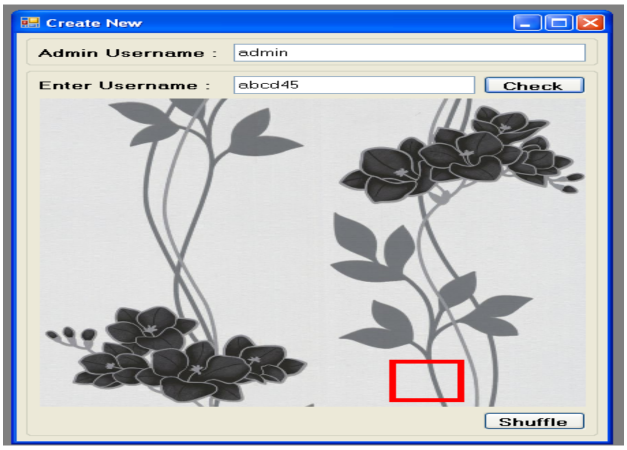
It is sometimes referred to as "cyber security" or "IT security". Those terms generally do not refer to physical security, but a common belief among computer security experts is that a physical security breach is one of the worst kinds of security breaches as it generally allows full access to both data and equipment .

Cyber security is the process of applying security measures to ensure confidentiality, integrity, and availability of data.

Cyber security assures protection of assets, which includes data, desktops, servers, buildings, and most importantly, humans. The goal of cyber security is to protect data both in transit and at rest. Countermeasures can be put in place in order to ensure security of data. Some of these measures include, but are not limited to, access control, awareness training, audit and accountability, risk assessment, penetration testing, vulnerability management, and security assessment and authorization.

Vulnerability management is the cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities. This practice generally refers to software vulnerabilities in computing system.

So it has been proposed in this paper that by providing the security to the whole computer screen by using graphical password computer system will more secure.



Create New

Admin Username : admin

Enter Username : abcd45

Fig. 2 Password creation

In this fig.2 it uses two images with five clicks on both the images.

It also maintain the order of the clicks on it. There is a cued block which is randomly created using system random number generation method.On every click the cued is automatically shifted to next position generated according to random number.

After five clicks are completed the next image will be displayed to user, again this image is anything this is also supplied from the collection of several images.

CONCLUSION

A major advantage of persuasive cued click point scheme is its large password space over alphanumeric passwords. There is a great interest for graphical passwords since they are better than text based passwords.

Though the main arguments for graphical passwords are that people are better at memorizing graphical passwords than text based passwords. Online password guessing attacks on text password only systems have been observed for decades.

Graphical password authentication system is apparently more effective in preventing password guessing attacks; it also offers more

REFERENCES

[1]. Birget, J.C., D. Hong, and N. Memon. Graphical passwords Based on Robust Discretization. IEEE Transactions on Information Forensics and Security, vol. 1, no. 3 September 2006.

[2]. Blonder, G.E. Graphical Passwords. United States Patent 5,559,961, 1996.

[3]. Chiasson, S., Biddle, R., and van Oorschot, P.C. A Second Look at the Usability of Click-based Graphical Passwords. Technical Report TR-07-10. School of Computer Science, Carleton University. March 2007.

[4]. Cranor, L.F., Garfinkel, S. Security and Usability. O' Reilly Media, 2005.

[5]. Davis, D., F. Monrose, and M.K. Reiter. On User Choice in Graphical Password Schemes. 13th USENIX Security Symposium, 2004.

[6]. Jermyn, A., et al. The Design and Analysis of Graphical Passwords. 8thUSENIX Security Symposium, 1999.

[7]. Nelson, D.L., U.S. Reed, and J.R. Walling. Picture Superiority Effect. Journal of Experimental Psychology: Human Learning and Memory 3, pp. 485-497, 1977.

[8]. Pass faces. http://www.realuser.com last accessed: December 1, 2006.

[9]. Peters, M. Revised Vandenberg & Kuse Mental Rotations Tests: forms MRT-A to MRT-D. Technical Report ,Department of Psychology ,University of Guelph, 1995.

[10]. Renaud, K. Evaluating Authentication Mechanisms. Chapter 6 in [4].

[11]. Renaud, K., De Angeli, A. My password is here! An investigation into visio-spatial authentication mechanisms. Interacting with Computers 16, pp. 1017-1041, 2004.

[12]. Suo, X, Y. Zhu, and G.S. Owen. Graphical Passwords: A Survey. Annual Computer Security Applications Conference (ACSAC), 2005.

[13]. Tari, F., Ozok, A.A., Holden, S.H. A Comparison of Perceived and Real Shouldersurfing Risks between Alphanumeric and Graphical Passwords. Symposium on Usable Privacy and Security (SOUPS), 2006.

[14]. Thorpe, J. and P.C. van Oorschot. Human-Seeded Attacks and Exploiting HotSpots in Graphical Passwords. USENIX Security Symposium, 2007 (to appear).

[15]. Preliminary version available as Technical Report, TR-07-05. School of Computer Science, Carleton University, Feb. 2007.

[16]. van Oorschot, P.C., Stubblebine, S. On Countering Online Dictionary Attacks with Login Histories and Humans-in-the-Loop. ACM Transactions on Information andSystem Security (TISSEC), pp. 235-258, August 2006,

[17]. Weinshall, D. Cognitive Authentication Schemes Safe against Spyware (Short Paper). IEEE Symposium on Security and Privacy, 2006.

[18]. Wiedenbeck, S., Birget, J.C., Brodskiy, A., and Memon, N. Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice. Symposium on Usable Privacy and Security (SOUPS), 2005.

[19]. Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A., and Memon, N. Pass Points: Design and longitudinal evaluation of a graphical password system. International Journal of Human-Computer Studies 63, pp. 102-127, 2005.Cued Click Points 17

[20]. 20. Yan, J., A. Blackwell, R. Anderson, and A. Grant. Password Memorability and Security: Empirical Results IEEE Security & Privacy Magazine, Sept.-Oct 2004.