ISSN:0975-9646

Cued Click Points: Graphical Password Authentication Technique for Security

Shendage Swapnil Sunil, Dhainje Prakash, Yevale Ramesh Shivaji.

PG Student, Department of CSE,SIETC, Paniv, Solapur University,Maharashtra, India[1]
Principal, SIETC, Paniv, Solapur University,Maharashtra, India[2]
Lecturer, SIETC, Paniv, Solapur University,Maharashtra, India[3]

Abstract. A Graphical Based Password is one alternative for textual password. Graphical input devices enable the user to decouple the position of inputs from the temporal order in which those inputs occur, and we show that this decoupling can be used to generate password schemes with substantially larger password spaces. Users click on one point per image for a sequence of images. The next image is based on the previous click-point. Performance was very good in terms of speed, accuracy, and number of errors. CCP also provides greater security than Pass Points because the number of images increases the workload for attackers.

Keywords: Graphical Passwords, Computer Security, Authentication, Usable Security

1 INTRODUCTION

A graphical password is a secret that a user inputs to a computer with the aid of the computers' graphical input (e.g., mouse, stylus, or touch screen) and output devices. Graphical Password can be formed in the combination of Image Icons or Pictures. In other words, graphical password is an authentication system that works by having the user select from images, in a specific order, presented in a graphical user interface (GUI). For this reason, the graphical-password approach is sometimes called graphical user authentication (GUA). Graphical passwords are particularly useful for systems that do not have keyboards.

Today, text passwords have many uses, but these uses can be grouped into two types:

• *Authentication*. The first and most common is as a method of user authentication—that is, to confirm the claimed identity of a human user. The output of this process is one bit: “1” means that the user is as claimed, “0” indicates that he is not.

• *Key generation*. The second is as a method of key generation by the human user, for the purpose of using the resulting key in a cryptographic algorithm. A common example of this type is file or disk encryption using a password: the user inputs her password, and this password is used to encrypt or decrypt certain stored contents of the device. Unlike authentication, key generation requires an output of many more bits (e.g., 50), and each bit should be unpredictable to an adversary who does not know the password.

In both cases, the output should be repeatable by a user who knows the password. Graphical passwords supporting both types of use are needed.

In this paper, we propose a new click-based graphical password scheme called Cued Click Points (CCP). It can be viewed as a combination of PassPoints , Passfaces, and Story. 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.

2 GRAPHICAL PASSWORDS

A graphical password is an authentication system that works by having the user select from images, in a specific order, presented in a graphical user interface. A graphical password is easier than a text-based password for most people to remember. Graphical passwords offer better security than text-based passwords because many people, in an attempt to memorize text-based passwords, use plain words.

3 GRAPHICAL AUTHENTICATIONS TECHNIQUES

The graphics authentication techniques can further be divided into two categories of graphical techniques:

- *Recognition based*
- *Recall based*

3.1 RECALL BASED TECHNIQUE:

We would discuss two types of picture password technique in this section:

- *Reproducing a drawing*
- *Repeating a selection*

3.1.1 *Reproduce A Drawing:*

Jermyn proposed a technique, called “Draw-A-Secret (DAS)”, which allows the user to draw their unique password. The basic concept behind Draw a Secret (DAS) [Figure 2,3,4] is that humans excel at image recognition and memory, so "passwords" should be designed to leverage that ability. Initial implementations simply tracked the ability of people to use a stylus to draw a free-form shape on a touchsensitive screen. But the people behind the new work have previously refined the technique by parsing the shapes with a flexible grid, which allowed them to more accurately recognize key features such as changes in the stroke's direction. The primary limitation of this DAS system is the user's ability to accurately redraw a complex shape from memory.

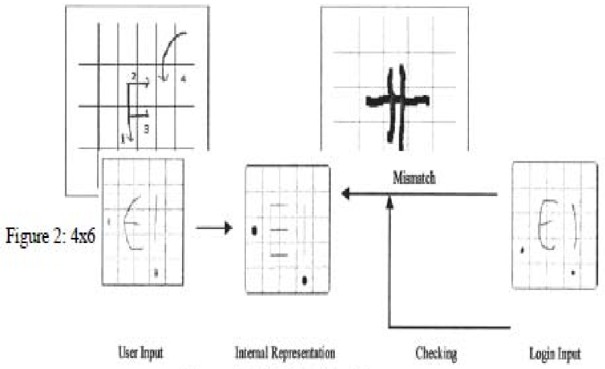

Figure 2: 4x6

Figure 4: DAS Checking Scheme

3.1.2 ***Repeating A Selection:***

Blonder [1] designed a graphical password scheme in which a password is created by having the user click on several locations on an image. During authentication, the user must click on the approximate areas o those locations. Passlogix [2] has developed a graphical password system based on this idea. In their implementation the users must click on various items of the image in the correct sequence in order to be authenticated. The “PassPoint” system by Wiendenback [3-4] extended Blonder’s idea by eliminating the predefined boundaries and allowing arbitrary images to be used. As a result, a user can click on any place on an image (as opposed to some pre-defined areas) to create a password. This technique is based on the discretization method proposed by Birget [5]. Adrian Perrig was reported to be working on a system (called Map Authentication) that was based on navigating through a virtual world [6]. In this system the user can build their own virtual world.

4 POSSIBLE ATTACKS ON GRAPHICAL PASSWORD TECHNIQUES

Graphical passwords are not widely used in practice.The possible techniques for breaking graphical pass-words are given below and a comparison with text-based pass-words.

4.1 DICTIONARY ATTACKS

This is the major problem with the text based passwords. Recognition based graphical passwords involve the user to input using mouse instead of keyboard; it is impractical to carry out dictionary attacks against this type of graphical passwords. For some recall based graphical passwords, it is possible to use a dictionary attack but an automated diction-ary attack will be much more difficult than a text based dictionary attack.

4.2 GUESSING

This is the serious problem usually associated with the text based passwords. Graphical Passwords tend to predict. It is found that people often choose weak and predictable graphical passwords. Similar predictability is found among the graphical passwords created with the DAS technique.

4.3 BRUTE FORCE ATTACK

In some graphical password techniques password space is similar to or larger than that of text-based passwords. The main defense against brute force attack is to have a sufficiently large password space. A brute force attack is difficult to carry against graphical passwords than text-based passwords. Automatically generated accurate mouse movement is required in brute force attack to reproduce human input, which is mostly difficult in case of recall based graphical passwords.

4.4 SPYWARE ATTACK

Key listening spyware cannot be used to break graphical passwords. It is not clear whether “mouse tracking” spyware will be an effective tool against graphical passwords or not. However, mouse motion alone is not enough to break graphical passwords. Such information has to be associated with application information, such as position and size of window, as well as time information.

5. BACKGROUND

Graphical password systems are a type of knowledge-based authentication that attempts to leverage the human memory for visual information. In such systems, users identify and target previously selected locations within one or more images. The images act as memory cues to aid recall.

Passfaces [7] is a graphical password scheme based primarily on recognizing human faces. 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 decoys. Users must correctly respond to a number of these challenges for each login.

Example systems include PassPoints and Cued Click-Points (CCP)

In PassPoints, a password consists of a sequence of five click-points. Users may select any pixels in the image as click-points for their password. To log in, they repeat the sequence of clicks in the correct order, within a system-defined tolerance square of the original click-points.

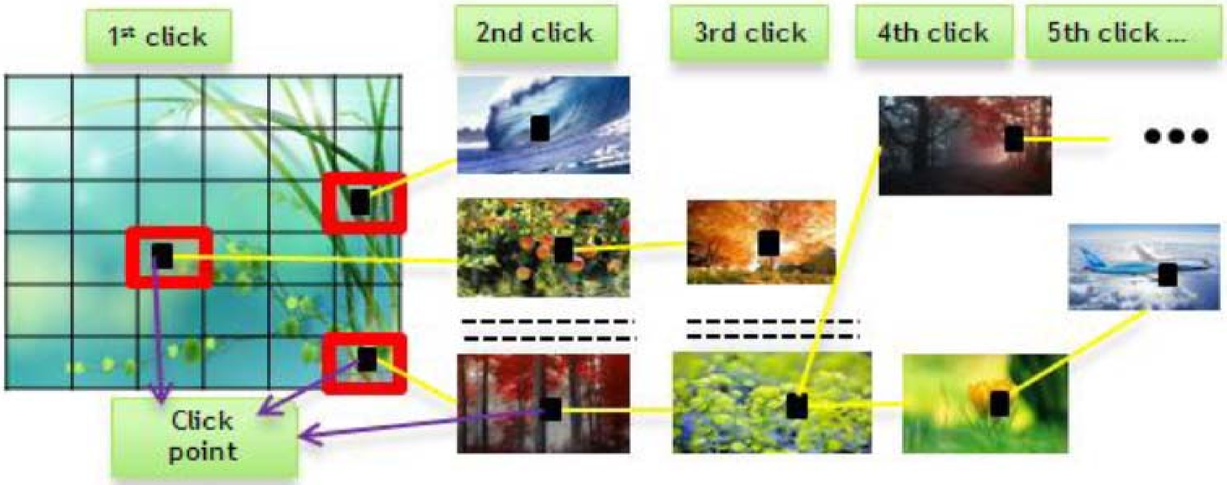

Fig 2. In CCP, user selects one click-point per image. The next image displayed is determined by the current clickpoint.

6. Clued Clicked Points

Cued Click Points (CCP) is an alternative to PassPoints. In CCP, users click one point on each of 5 images rather than on five points on one image. It offers cued-recall and introduces visual cues that instantly alert valid users if they have made a mistake when entering their latest click-point.

A wrong click leads down an incorrect path, with an explicit indication of authentication failure only after the final click. Users can choose their images only to the extent that their click-point dictates the next image. If they dislike the resulting images, they could create a new password involving different click-points to get different images. For implementation, CCP initially functions like PassPoints. During password creation, a discretization method is used to determine a click-point's tolerance square and corresponding grid. For each click-point in a subsequent login attempt, this grid is retrieved and used to determine whether the click-point falls within tolerance of the original point. With CCP, we further need to determine which next-image to display.

Using CCP as a base system, we added a persuasive feature to encourage users to select more secure passwords, and to make it more difficult to select passwords where all five click-points are hotspots. As with text passwords, PassPoints can Only safely provide feedback at the end and cannot reveal the cause of error. Providing explicit feedback in PassPoints before the final click-point could allow

PassPoints attackers to mount an online attack to prune potential password subspaces, whereas CCP's visual cues should not help attackers in this way. Another usability improvement is that being cued to recall one point on each of five images appears easier than remembering an ordered sequence of five points on one image.

Conclusion & Future Work

An important usability and security goal in authentication systems is to help user's select better passwords and thus increase the effective password space. By taking advantage of users' ability to recognize images and the memory trigger associated with seeing a new image, CCP has advantages over PassPoints in terms of usability. CCP offers a more secure alternative to PassPoints. CCP increases the workload for attackers by forcing them to first acquire image sets for each user, and then conduct hotspot analysis on each of these images.

In future development we can also add challenge response interaction. In challenge response interactions, server will present a challenge to the client and the client need to give response according to the condition given. If the response is correct then access is granted. Also we can limit the number a user can enter the wrong password.

References

1. Blonder, G.E. Graphical Passwords. United States Patent 5,559,961, 1996.
2. Passlogix, "www.passlogix.com," last accessed in June 2005.
3. Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy and Nasir Memon, "Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice", SOUPS'05 Conference, July 6-8, 2005, Pittsburgh, PA, USA.
4. Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy and Nasir Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system", *International Journal of Human-Computer Studies* (Special Issue on HCI Research in Privacy and Security) 63, 102-127, 2005. - Elsevier Ltd, http://www.science<tirect.com.
5. Jean-Camille Birget, Dawei Hong and Nasir Memon, uGraphical Passwords Based on Robust Discretization", IEEE Transactions on Information Forensics and Security, Vol. 1, No.3, September 2006.
6. L. D. Paulson, "Taking a Graphical Appraoch to the Password," *Computer*, vol. 35, pp. 19, 2002.
7. Passfaces. http://www.realuser.com Last accessed: December 1, 2006.