Graphical Password Authentication Based on Polygon Visualization

Harshil Shah*, Chirag Lakhani**, Sagar Haldankar***
Project Guide: Prof. Sainath Patil****

* (Dept. of Information Technology, Vidyavardhini's College of Engineering. & Tech., Vasai Rd.
Email: shahharshil46@gmail.com)
** (Dept. of Information Technology, Vidyavardhini's College of Engineering & Tech., Vasai Rd.
Email: chiraglakhani09@yahoo.in)
*** (Dept. of Information Technology, Vidyavardhini's College of Engineering & Tech., Vasai Rd.
Email: sagardh4u@gmail.com)
**** (Dept. of Information Technology, Vidyavardhini's College of Engineering & Tech., Vasai Rd.
Email: patil_sai@yahoo.co.in)

ABSTRACT
When users input their passwords in a public place, they may be at risk of attackers stealing their password, either by direct observation or by recording the individual's authentication session. This is referred to as shoulder-surfing and is a known risk, of special concern when authenticating in public places. Until recently, the only defense against shoulder-surfing has been vigilance on the part of the user. This paper reports on the design and evaluation of a game-like graphical method of

Authentication that is resistant to shoulder-surfing. The Convex Hull Click (CHC) scheme allows a user to prove knowledge of the graphical password safely in an insecure location because users never have to click directly on their password images. However, the protection against shoulder-surfing comes at the price of longer time to carry out the authentication.

Keywords – **authentication, Convex Hull Click scheme, graphical passwords, security, shoulder-surfing**

1. Introduction

Traditionally, alphanumeric passwords have been used for user authentication. While today other methods including biometrics and smart cards are possible alternatives, passwords are likely to remain dominant at least for some time because of concerns about reliability, privacy, security, cost and ease of use of other technologies. Passwords are expected to comply with two fundamentally conflicting requirements:

1. Passwords should be easy to remember, and the user authentication protocol should be executable quickly and easily by humans.

2. Passwords should be secure, i.e., they should look random and should be hard to guess; they should be changed frequently, and should be different on different accounts of the same user; they should not be written down or stored in plain text [1].

Because it is difficult for humans to remember random strings, users tend to ignore requirements for secure passwords. This leads to poor password practices, including short, simple passwords that are easy to break either by a dictionary attack or personal knowledge of the password owner, use of the same password over months or years, reuse of identical or nearly identical passwords on multiple systems, and propensity to write down passwords and store them insecurely [1].

In an effort to improve password security by making passwords easier to remember, researchers have developed graphical passwords. In a typical graphical password scheme a user chooses several images to be his or her password. When logging in, the user must

click on the password images among a larger group of distractor images. If the user clicks on the correct images, he or she is authenticated. Users' memory for a graphical password may be better than for an alphanumeric password. Secure alphanumeric passwords (i.e., random strings) are based on pure recall from memory, a skill that is notoriously difficult for humans [1].

By contrast, graphical passwords are based on recognition of previously known images, a skill at which humans are proficient. While alphanumeric passwords systems are vulnerable to shoulder-surfing if the attacker can see the keyboard, graphical password systems may be more vulnerable in certain settings. For example, clicking on images on a large, vertical display screen may make users' actions easier to capture [1].

2. Background to the research

2.1 Graphical Password Systems

A common approach to design of graphical password systems is a challenge-response scheme. In a challenge-response scheme the user creates a password by choosing several images from a large portfolio of images. The chosen images become the user's password. To log in the user must successfully respond to a series of challenges. In a challenge the user is simultaneously shown several images on the screen, where one of the images is a password image of the user and the rest are decoy images. The user responds by clicking anywhere on the password image. In each subsequent challenge the user is shown another password image surrounded by different decoys. The user logs in successfully if all challenges are responded to correctly [5].

However, a possible drawback is the amount of time for carrying out a series of challenges. A larger password space, and therefore higher security, can be achieved only by a large number of decoy images in each challenge or a large number of challenges. Both of these increase the login time. Another potential drawback is that users may be strongly attracted to certain images [2, 3]. If different users tend to choose the same images for their password, the entropy of the system decreases, making it less secure.

2.2 Shoulder-Surfing Problem and Defenses against It

Shoulder-surfing occurs when an attacker learns a user's password by watching the user log in. Using an alphanumeric password, though the user's password is not displayed on the screen, a practiced attacker can "read" the user's keystrokes as the user types the password. The user's only defense is to shield the keyboard with an object or one's body. Using a graphical password, the user would have to shield the screen. The same considerations apply to entering PINs at ATMs. High tech versions of shoulder-surfing are also a threat, although it is not known how prevalent the threat is. Technology-based attacks include using binoculars or a low power telescope to enhance vision, using video cameras, video mobile phones, keystroke logging software, or Trojan software to record a login, and listening to a user input a PIN or account number on a telephone keypad. Remote electro-magnetic sensors can also be used to capture actions without the user's knowledge.

As indicated above, both alphanumeric and graphical passwords are vulnerable to shoulder-surfing. The degree of the threat depends on the situation. For example, a graphical password might be quite vulnerable if the user enters the password by clicking on images on a large screen in a physical environment where observation is easy. On the other hand, a graphical password entered with a stylus on a smaller screen would probably be much harder for a human attacker or a video camera to capture because the device can be held closer to the body; the user's hand tends to obstruct observation.

3. Convex Hull Click Scheme

Our shoulder-surfing resistant scheme, the Convex Hull Click Scheme (CHC), is a graphical password scheme that guards against shoulder-surfing attacks by human and technical. CHC is based on several rounds of challenge-response authentication.

The system uses a large portfolio consisting of several hundred Icons. The icons are displayed using only the image without text. To create a password the user chooses several icons from the portfolio to be his or her pass-icons (Figure 1). The number of pass-

icons is determined by the system administrator. The user has to remember the pass-icons he or she selected.

At login time a large number of icons from the portfolio are randomly arranged in the password window (Figure 1). These icons include mostly non-pass-icons along with a few pass-icons. The number of pass-icons displayed is a random number between three and the total number of pass-icons. (At least three pass-icons are guaranteed to be displayed on the window, since forming a convex hull requires at least three icons.) The login takes place in a series of challenge-response rounds. The number of rounds is controlled by the administrative setting, so this is easily changed, with more rounds providing higher security.

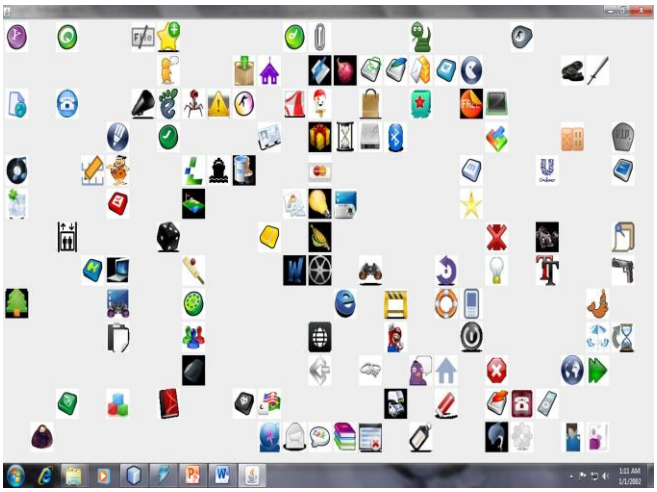

Figure 1. Graphical password interface used in the experiment.

When the login begins, the user must visually locate three or more of his or her pass-icons. The user's next step is to mentally create the convex hull formed by those pass-icons. A convex hull is the area encompassed by the edges joining a set of three or more points. In CHC the pass-icons serve as the points, and the edges are lines visualized in the user's mind. For illustrative purposes, Figure 2 shows a highlighted convex hull formed by three passicons. (Note that highlighting is not used when a user interacts with the system.) Figure 3 shows a convex hull formed by five pass-icons. In the response of challenge, the user clicks anywhere within the convex hull. The user does *not* click on the pass-icons themselves and therefore does not give away to an attacker the identity of the pass-icons. Some convex hulls may be very narrow, as shown in the excerpt of the password window in Figure 4. This can make clicking accurately in the convex hull difficult. However, if this occurs the implementation guarantees that there is always at least one more pass-icon in the window that can be used to form a wider convex hull.

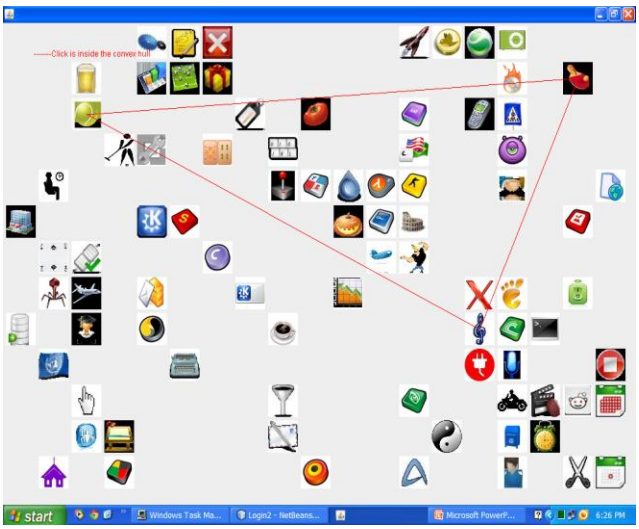

Figure 2. Example of a convex hull with 3 pass-icons.

Figure 3. Example of a convex hull with 5 pass-icons.

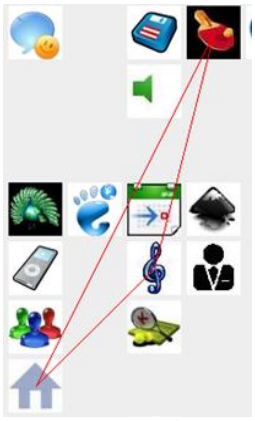

Figure 4.A Narrow Convex Hull

When the user has responded to the challenge, another challenge appears, and this continues until all challenges have been completed. The password window changes between the rounds of challenges. The non-pass-icons move to new random positions in the window. In addition, some portion of them randomly leaves the window, and a random number of new ones enter the window. Thus, the total number of icons visible in the window changes from one challenge to the next. Pass-icons likewise move to new positions. They may move out of the window and other pass-icons may enter it, with the constraint that there must always be three or more displayed in the window. The reason for moving icons into and out of the window is to make it harder for an attacker to guess the pass-icons. An individual cannot use the same pass-icons in every challenge, and therefore the attacker cannot easily determine which ones are the pass-icons. Further, guessing becomes more difficult given the constant changes of the non-pass-icons.

The rearrangement of the icons between challenges is done in a fluid, game-like animation.

If the user responds correctly to each of the challenges he or she is authenticated, but if the user fails any challenge the login fails. The user is given feedback at the end of the login that indicates whether the logon is correct or not. As in all password systems, the user is not given specific information about the location of the error.

Beyond its shoulder-surfing resistant properties, there are three main considerations about the security of CHC. First, the password space can be made very large, and therefore more secure, by increasing the number of icons, the number of passicons, or both. The only practical limits are the size of the window and the ability of users to locate their pass-icons among a large number of icons. Second, a brute-force attack is infeasible. An attacker could try to record all possible passwords that do not contain the click points observed by shoulder-surfing. After successive observations, the attacker could rule out more and more passwords. However, eventually the attacker would have to record a significant portion of all possible passwords, which would require far too much memory. Third, in challenge-response authentication there is always the possibility of accidental login (i.e., an attacker could click in the convex hull by luck). This is different from guessing the password. To make accidental login unlikely we do three things: (1) icons are randomly placed in the password window so that all locations except near the border of the window have about the same probability of being in the convex hull of the pass-icons, (2) large convex hulls that cover half the window or more are only rarely generated, and (3) to log in the user has to respond to multiple challenges.

Two additional security considerations about CHC are worth mentioning. First, potentially an attack against the system could be mounted using an eye-tracker[4]. The eye-tracker could map where the user is looking while creating the convex hull and, at least in some cases, discover the pass-icons. current eye-trackers cannot be used without being detected by the user. Many eye-trackers use head mounted cameras. Recently eye-tracking cameras have been integrated into a panel attached below a monitor. Nevertheless, these integrated cameras are still quite obvious and, to our knowledge, they are only integrated into stand-alone monitors. Second, a known security problem of all human usable challenge-response systems is that the system needs to know the password explicitly (in order to make challenges and to check correctness of the responses), and therefore the password cannot be encrypted.

4. Implementation of CHC

4.1 User Registration Phase:

4.1.1 The new user fills up a registration form consisting of username, address, contact number and other such personal details.

4.1.2 On submitting this form, the user is presented with a window showing 100 icons arranged in a 10*10 grid. The 100 icons are selected based on following logic:

4.1.2.1 The icons are sorted in ascending order according to number of times they are displayed for selection. Those with same display count are further sorted in ascending order according to the number of times the icon has been selected as passicon.

4.1.2.2 The top 100 images from the above result are displayed in the grid.

4.1.3 The user has to select a specified minimum number of images as his password. The minimum number can be modified by the administrator.

4.1.4 The user can refresh the images shown to him for a maximum number of 5 times.

4.2 Challenge Response Phase

The system presents multiple rounds of challenge-response to the user. In each round system chooses decoy icons and user passicons randomly.

Steps followed by system for presenting a challenge response round are as follows:

4.2.1 Divide whole screen into a grid of cells where each cell is 50 pixels wide and has height of 50 pixels and determine the total number of images **T** that can fit into the screen.

4.2.2 System selects number of user passicons say N to be displayed in a particular round based on a range provided by administrator.

4.2.3 System chooses a number **R1** between **T/2** and **T/4** and retrieves first R1 images from the database based on number of times image displayed in previous rounds

4.2.4 System jumbles up the array of (R1+N) images and places them on the screen grid such that the no two user images are 8- way connected.

4.2.5 If the click point is below the bottommost icon, or to the left of leftmost icon or to the right of rightmost icon or above the topmost icon then click is clearly outside the convex hull.

4.2.6 If click point does not satisfy the above mentioned conditions then system will determine the slope of an imaginary line connecting center of every other passicon to that of bottommost passicon.

4.2.7 Now system will order up the user passicons, starting with bottommost icon, followed by positive slope icons and then by negative slope icons, thus forming a closed figure or polygon. Each of the positive and negative sloped icons will be arranged in ascending order.

4.2.8 Now system calculates the slope of the line connecting the click point with the center of bottommost passicon and determines two passicons forming the polygon, one whose slope is just greater than the line say PassIcon1, and another whose slope lies just before that of the line say PassIcon2.

4.2.9 Now system calculates the intersecting point say IPT1 between Line1 and Lin2 such that Line1 is connecting the bottommost icon and click point and Line2 is connecting the PassIcon1 and PassIcon2.

4.2.10 if the click point is below that IPT1 and on the Line1 then click is inside the polygon otherwise click is outside the polygon.

Sample demonstrating the procedure is as shown below:

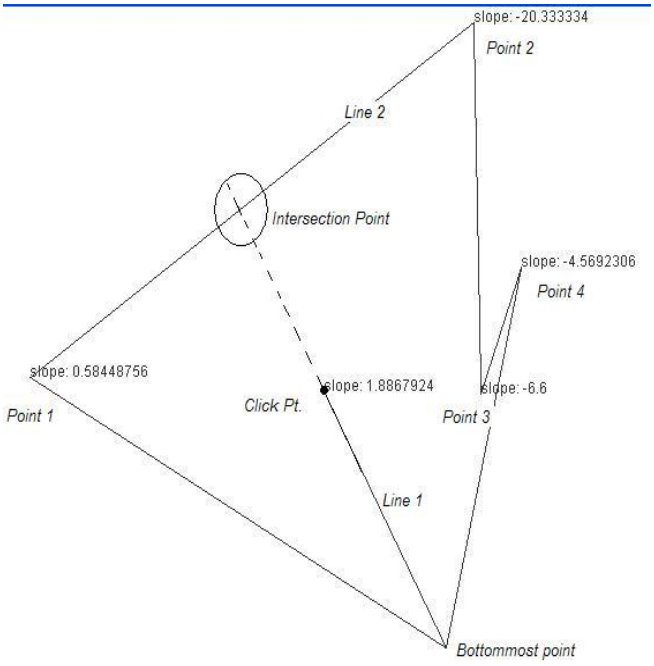

Figure 5.Inside outside Test for Click Point using Slope based method

5. Conclusion

The Convex Hull Click Scheme is an effort to develop security innovations with people in mind. The contribution of this paper is the design of a graphical password system that extends the challenge response paradigm to resist shoulder-surfing. In doing so it aims to motivate the user with a fun, game-like visual environment designed to develop positive user affect and counterbalance the drawback of the longer time to input the password. Future work should target increasing the speed of input of the password.

5. Acknowledgement

We are heartily thankful to our internal guide Prof. Sainath Patil for his guidance & support. His valuable suggestion and timely advice inspired us towards sustained efforts for our project work. Special thanks to Prof. Chandan Kolvankar, Head of The Department, Information Technology. Finally we are grateful to our principal Dr. Mohan Bhave and the entire Information Technology Department for providing us with excellent infrastructure for carrying out project work.

References

[1]. Susan Wiedenbeck and Jim Waters , Leonardo Sobrado and Jean-Camille Birget. : *Design and Evaluation of a Shoulder-Surfing Resistant Graphical Password Scheme, 2006*

[2]. Davis, D., Monrose, F., and Reiter, M.K. On user choice in graphical password schemes. In *Proc. of the 13th USENIX Security Symposium*, San Diego, 2004.

[3]. De Angeli, A., Coventry, L., Johnson, G., and Renaud, K. Is a picture worth a thousand words? Exploring the feasibility of graphical authentication systems. International Journal of Human-Computer Studies, 63, 1-2 (2005), 128-152.

[4]. Wagstaff, J. Shoulder-surfing: the old new phishing. http://loosewire.typepad.com/blog/2005/04/shoulder_surfin.html. Accessed December 9, 2005.

[5]. Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A., and Memon, N. PassPoints: design and longitudinal evaluation of a graphical password system. *International Journal of Human- Computer Studies*, 63, (2005), 102-127.