ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 3, March 2014

Shoulder Surfing Resistant Password Authentication Mechanism (Using Convex hull Click Scheme)

Professor Sandeep Samleti[1], Chandan Kumar[2] ,Vijay Prakash[3], Nitin Kumar[4], Sunil Kumar[5]

Department of Information Technology, Army Institute of Technology Pune, India[1,2,3,4,5]

Abstract: when users input their passwords in a public place, they may be at risk of attackers stealing their password. An attacker can capture a password by direct observation or by recording the individuals 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 was the alertness on the part of the user. Shoulder surfing resistant password authentication mechanism assure shoulder-surfing resistant authentication to user. It allows user to authenticate by entering pass-word in graphical way at insecure places because user never have to click directly on password icons. Usability testing of this mechanism showed that novice users were able to enter their graphical password accurately and to remember it over time. However, the protection against shoulder-sur_ng comes at the price of longer time to carry out the authentication.

Keywords: shoulder-surfing, password, graphical

I. INTRODUCTION

A. Need

Password are used provide authentication in any system, mobile device. Alphanumeric passwords are in use for user authentication. While today other methods including biometrics and smart cards are possible alternatives, passwords are likely to remain dominant for some time because of concerns about reliability, privacy, security, and ease of use of other technologies. However, in the use of passwords dilemmas often arise in the tradeoff between security and usability. The dilemma arises because passwords are expected to comply with two basic conflicting requirements:

(1) Passwords must be easy to recall and remember..
(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.

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, e.g., a text file containing the users passwords stored on insecure computers or PDAs, post its notes stuck on or near the computer monitor or inside a desk drawer.

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 choose 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 ability to recall from memory, a task that is difficult for humans. By contrast, graphical passwords are based on recognition of previously known images, a skill at which humans are proficient. However, the problem of shoulder-surfing is a recognized drawback of graphical passwords. 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.

B. Application

This project allows user to authenticate securely in places where his or her activity can be recoded or directly observed.

II. LITERATURE SURVEY

C. Technologies already in use

Existing Mechanism: - Nowadays alphanumeric passwords are getting used for user authentication. Textual alpha-numeric passwords were first introduced in the 1960s as a solution to security issues. While today possible alternatives are biometrics, Face recognition mechanism, Retina scan and smart cards , passwords are likely to remain in use for some time because it provides reliability, privacy, security, and ease of use of other technologies such as biometric, face recognition, retina scan needs hardware support. However, the use of passwords dilemmas often arises in the tradeoff between security and usability. Passwords should be easy to remember, and authentication protocol should be quickly and easily executable by humans. Passwords should be secure, i.e., they should look random and should be hard

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 3, March 2014

to guess; they should be changed frequently, and should be different on different accounts of the same user. In an effort to improve password researchers have developed graphical passwords. However, the problem of shoulder-surfing is a recognized drawback of graphical passwords.

D. Shoulder surfing

In computer security, shoulder surfing is simply looking over someone's shoulder, to get any useful information or data. It is commonly used to obtain passwords, PIN, security codes, and similar data. To prevent shoulder surfing while entering password graphical password, biometric mechanism are used. Graphical Password scheme can be implemented with Convex Hull Click Scheme .It uses convex hull algorithm. In mathematics, the convex hull is minimum set of point which cover all the randomly distributed point on plane, the convex hull may be visualized as the shape formed by a rubber band stretched around randomly distributed points. To implement the convex hull various algorithm can be used such as: Algorithms Known convex hull algorithms are listed below, ordered by the date of first publication. Time complexity of each algorithm is stated in terms of the number of inputs points n and the number of points on the hull h. Note that in the worst case h may be as large as n.

1. Gift wrapping aka Jarvis march O(nh): One of the simplest algorithm discovered independently by Chand and Kapur in 1970 and R. A. Jarvis in 1973. It has O(nh) time complexity, where n is the number of points in the set, and h is the number of points in the hull. Worst case the complexity is (n^2).
2. Graham scan O(n log n): A more sophisticated, but more efficient algorithm, published by Ronald Graham in 1972. If the points are already sorted by one of the coordinates or by the angle to fixed vector, then the algorithm takes O(n) time.
3. Quick Hull-O (n log (n)): Discovered independently in 1977 by W. Eddy and in 1978 by A. Bykat. Just like the quicksort algorithm, it has the expected time complexity of O(n log n), but may degenerate to (nh) =O(n2) in the worst case.
4. Divide and conquer O(n log n): Another O(n log n) algorithm, published in 1977 by Preparata and Hong.
5. Chan's algorithm O(n log h): A simpler optimal output-sensitive algorithm discovered by Chan in 1996.
6. Monotone chain aka Andrew's algorithm O(n log n): Published in 1979 by A. M. Andrew. The algorithm can be seen as a variant of Graham scan which sorts the points lexicographically by their coordinates. When the input is already sorted, the algorithm takes O(n) time.
7. Incremental convex hull algorithm O(n log n): Published in 1984 by Michael Kallay.

E. Occurance

Shoulder surfing is particularly effective in crowded places because it is relatively easy to observe someone as they:

1. Fill out a form.
2. Enter their PIN at an ATM or a POS terminal.
3. Enter a password at a cybercafé, public and university libraries, or airport kiosks.
4. Enter a code in a public place such as a swimming pool or airport.
5. Public transport is a particular area of concern.

Shoulder surfing can also be done using binoculars or other vision-enhancing devices. CCTV cameras can be concealed in ceilings, walls to observe entry. Secure, the European Association for Visual Data Security, recommends that when you are in a situation with heightened risk, take steps to protect yourself by angling your screen away from the gazes of other people or using a screen shield to reduce the visibility of your screen. Secure also recommends that corporate IT security guidance includes directions on how to mitigate.

III. PROPOSED MODEL

F. Objective

To develop an application which provide security against shoulder surfing during authentication in android mobile phone.

G. Achieve real time appplications

1) Graphical password system

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 users 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 de- coy 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. The advantage of this kind of challenge-response system is that it relies on recognition memory. In each challenge the user simply views displayed images and chooses the known image. 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. If different users tend to choose the same images for their password, the entropy of the system decreases, making it less secure.

2) 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 observation, video recording, or electronic capture. Like Pass faces, CHC is based on several rounds of challenge-response authentication. Like Roth et al.s PIN-entry scheme, users never point directly to the items that form their passwords. In CHC the graphical elements used in authentication are icons or images randomly distribute on

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 3, March 2014

the screen. In a challenge the user must recognize some minimum number of his or her password icons, or pass-icons, out of a much larger number of randomly arranged icons. The user solves the problem by clicking within the convex hull of the pass-icons. Several such challenges are presented in sequence, and if the user responds correctly to everyone then the user is authenticated. The system uses a large portfolio consisting of several hundred icons. In our implementation the icons used were all icons of software applications, but the portfolio of icons could be any kind of small icons, even user-provided ones. Icon will be displayed to user and user selects his password icons as in Fig(3.1).

Figure 3.1: SELECT PASSWORD ICONS

At login time a large number of icons from the portfolio are randomly arranged in the password window. These icons include mostly non-pass-icons along with a few pass-icons as in Fig (3.2).To randomly throw the icons all over the screen we will use random function in java.

Figure 3.2: RANDOM DISTRIBUTED ICONS

When the login begins, the user must visually locate three or more of his or her pass-icons. The users 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 users mind. For illustrative purposes, Figure(3.3) shows a highlighted convex hull formed by three pass icons and user have to click inside the this virtually created convex inside his or mind. To provide more security more level this step can added in implementation. At each stage user have to perform this activity correctly if user fails to perform it correctly then he or she will not be authenticated. To check the wether user entered inside the convex we pass the coordinates of password icons in convex hull algorithm and the coordinate of position of click of user. Ther are various convex hull alogorithm can be used such as Grahm scan ,Quick hull both have time complexity of O(nlog(n)).

Figure 3.3: VIRTUAL AREA IN WHICH USER SHOULD CLICK

3) USABILITY OF CHC

It can be used for novices and expert both, novices could learn, remember, and enter passwords successfully using CHC. As no of total icons increased the time of login increased and as no of password icons increases time of login decreases because it is easier to find convex hull with grater no of icons. According to a survey conducted mean time of login with three password icon is found to be 11.72 sec, with four icons is 11.55 and with five icons is 9.71 sec for five roudnd. All the user were able to enter the password correctly in all 10 attempts. It was found that more the user will practice the more the login time will be decreased.So,It was advised that user should practice it for quick login. It is Secure to Brute force attack beacause of large no of icons and stages and it is secure to shoulder surfing attack.

No of Icons	Mean Time	Std Deviation
3	11.72	3.77
4	11.55	4.74
5	9.71	3.82

Table 3.1: Means and standard deviations (seconds) of challenges with 3, 4, and 5 pass- icons

IV. CONCLUSION

The Convex Hull Click Scheme is an effort to develop security innovations. The contribution of this paper is the design of a graphical password system that extends the challenge response paradigm to resist shoulder-surfing. Future work should target increasing the speed of input of the password.

REFERENCES

[1] Design and Evaluation of a Shoulder-Surfing Resistant Graphical Pass-word Scheme by Susan Wiedenbeck and Jim Waters College of IST Drexel University Philadelphia, PA 19104 USA sw53,jw65@drexel.edu , Leonardo Sobrado and Jean-Camille Birget Computer Science Department Rutgers University at Camden Camden, NJ 08102 USA lsobrado, birget@camden.rutgers.edu.

[2] S3PAS:A Scalable Shoulder-Surfing Resistant Textual-Graphical Pass- word Authentication Scheme by Huanyu Zhao and Xiaolin Li Scalable software Systems Laboratory Department of Computer Science Oklahoma State University, Stillwater, OK 74078, USA Email: huanyu, xiaolin@cs.okstate.edu

[3] 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.

[4] Shoulder Surfing attack in graphical password authentication by ARASH HABIBI LASHKARI Computer Science and Data Communication (MCS) University Malaya (UM) Kuala Lumpur, Malaysia ahabibil@hotmail.com Dr. OMAR BIN ZAKARIA Computer Science and Data Communication (MCS), University of Malaya (UM), Kuala Lumpur, Malaysia omarzakaria@um.edu.my, SAMANEH FARMAND Computer Science and Information Technology (IT), University Malaya (UM) Kuala Lumpur, Malaysia mobina23@gmail.com , DR. ROSLI SALEH Computer Science and Data Communication (MCS), University of Malaya (UM), Kuala Lumpur, Malaysia roslisalleh@utm.edu.my.

[5] Convex Hull algorithm"and \shoulder surfing in computer security\ :

[6] wikipedia.org.