Graphical Password with Convex Hull

Anusha S, Shobha C Nannoji, Ranjini P, Tejashwini T V, Vishwesh J*

Department of CSE, GSSSIETW, Mysuru, Karnataka, India

DOI: https://doi.org/10.21467/proceedings.1.31

* Corresponding author email: vishweshj@gsss.edu.in

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 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 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 password 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-surfing comes at the price of longer time to carry out the authentication.

Index Terms- Shoulder-surfing, password, graphical

1 INTRODUCTION

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.

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 chooses 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.

2 LITERATURE SURVEY

It's the foremost preliminary step for proceeding with any research work writing. While doing this go through a complete thought process of your Journal subject and research for it's viability by following means: Chippy.T, R. Nagendran- usable security has unique usability challenges because the need for security often means that standard human-computer-interaction approaches cannot be directly applied. An important usability goal for authentication systems is to support users in selecting better passwords. Users often create memorable passwords that are easy for attackers to guess, but strong system-assigned passwords are difficult for users to remember. So researchers of modern days have gone for alternative methods wherein graphical pictures are used as passwords. Graphical passwords essentially use images or representation of images as passwords. Human brain is good in remembering picture than textual character. There are various graphical password schemes or graphical password software in the market. However, very little research has been done to analyze graphical passwords that are still immature. There for, this project work merges persuasive cued click points and password guessing resistant protocol. The major goal of this work is to reduce the guessing attacks as well as encouraging users to select more random, and difficult passwords to guess. Well known security threats like brute force attacks and dictionary attacks can be successfully abolished using this method. (refer table no 2.1 row no.4)

Shushuang Man, Dawei Hong, Manton Matthews- proposed a new graphical password scheme. It is defined as a challenge-response Hence, a password in ourscheme is time-variant. User who knows the password is able to meet the challenge and to respond correctly. As consequence, our graphical password scheme is shoulder-surfing resistant. An attacker still cannot tell whatthe password is, even if he/she has filmed a user's login process. Primary experiments on our graphical password scheme showed the scheme is promising. (refer table no 2.1 row 1)

Dawei Hong, Shushuang Man Barbra Hawes, Manton Mathews- Spyware is now serious threat to computer security. In particular, the Internet is used to remotely login to server on which sensitive data and applications are stored. Spyware may well steal passwords for login to such aserver when user login to the server through the internet. We propose a new password scheme which is strongly resistant to spyware. In theory, a password in the scheme is a set of random strings. We programmed the scheme and conducted experiment. The result is promising. (refer table no.2.1 row no. 2)

HaichangGao, Xidian Univ., Xi'an, China, Xiuling Chang, Xiyang Liu, Aickelin, U -Shoulder-surfing is a known risk where an attacker can capture a password by direct observation or by recording the authentication session. Due to the visual interface, this problem has become exacerbated in graphical. There have been some graphical schemes resistant or immune to shoulder-surfing, but they have significantusability drawbacks, usually in the time and effort to log in. In this paper, we propose and evaluate a new shoulder surfing rsistant scheme which has a desirable usability for PDAs. Our inspiration comes from the drawing inputmethod in DAS and the association mnemonics in Story for sequence retrieval. The new scheme requires users to drawa curve across their password images orderly rather than click directly on them. The drawing input trick along with thecomplementary measures, such as erasing the drawing trace, displaying degraded images, and starting and ending withrandomly designated images provide a good resistance to shoulder-surfing. A preliminary user study showed that use was able to enter their passwords accurately and to remember them over time. (refer table no.2.1 row no.5).

Alain Forget, Sonia Chiasson, & Robert Biddle -presented Cued Gaze-Points (CGP) as a shoulder-surfing resistant cued-recall graphical password scheme where users gaze instead of mouse-click. This approach has several ad- vantages over similar eye-gaze systems, including a larger password space and its cued-recall nature that can help users remember multipledistinct passwords. Our 45 participant lab study is the first evaluation of gaze-based password entry via user-selected points on images. CGP's usability is poten- tially acceptable, warranting further refinement and study. (refer table no 2.1 row no.3)

D. Davis, F. Monrose, and M. Reiter-- Biometric based authentication techniques, such as fingerprints, iris scan, or facial recognition. The major drawback of this approach is that such systems can be costly, and the identification process can be slow. Knowledge based techniques are the most widely used authentication techniques and include both text-based and picture-based passwords. Graphical password systems are a type of knowledge-based authentication that attempt to leverage the human memory for visual information which reduced memory burden. (refer table no.2.1 row no.6).

XiaoyuanSuo Ying Zhu G. Scott. Owen- Graphical passwords are often predictable, a serious problem typically associated with text-based passwords. For example, studies on the Passface technique have shown that people often choose weak and predictable graphical passwords.

similar predictability among the graphical passwords. More research efforts are needed to understand the nature of graphical passwords created by real world users.

Table 2.1: Survey Papers

No	NAME	AUTHOR	DISADVATAGES	ADVANTAGES
1	Shoulder Surfing Resistant Password Authentication Mechanism	Shushuang Man, Dawei Hong, Manton Matthews	Graphical Password Scheme Is Shoulder-surfing Resistant	They should look random and should be hard to guess
2	A Password Scheme Strongly Resistant To Spyware	Dawei Hong, ShushuangMan Barbra Hawes, Manton Mathews.	Spyware is now serious threat to computer security.	We propose a new password CHC scheme which is strongly resistant to spyware
3	Shoulder-surfing Resistance With Eye-gaze Entry In Cued-recall Graphical Passwords	Alain Forget, Sonia Chiasson, & Robert Biddle	over similar eye-gaze systems, including a larger password space and its cued-recall nature that can help users remember multiple distinct passwords	We present Cued Gaze-Points (CGP) as a shoulder-surfing resistant cued-recall graphical password scheme where users gaze instead of mouse-click
4	Defenses Against Large Scale Online Password Guessing Attacks By Using Persuasive Click Points	Chippy.T, R.Nagendran	Users often create memorable passwords that are easy for attackers to guess, but strong system-assigned passwords are difficult for users to remember	Researchers of modern days have gone for alternative methods where in graphical pictures are used as passwords.
5	A New Graphical Password Scheme Resistant To Shoulder-surfing	HaichangGao , Xidian Univ., Xi'an, China, Xiuling Chang, Xiyang Liu, Aickelin,U	Shoulder-surfing is a known risk where an attacker can capture a password by direct observation or by recording the authentication session.	Graphical schemes resistant or immune to shoulder-surfing, but they have significant usability drawbacks, usually in the time and effort to log in.
6	Graphical Password Authentication With Recognition And Recall	D. Davis, F. Monrose, and M. Reiter	The major drawback of this approach is that such systems can be costly and the identification process can be slow.	Picture-based passwords is a Graphical password systems are a type of knowledge-based authentication that attempt to leverage the human memory for visual information which reduced memory burden.

3 EXISTING SYSTEM

3.1 Graphical Password

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 distracter 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. By contrast, graphical passwords are based on recognition of previously known images, a skill at which humans are proficient.

.

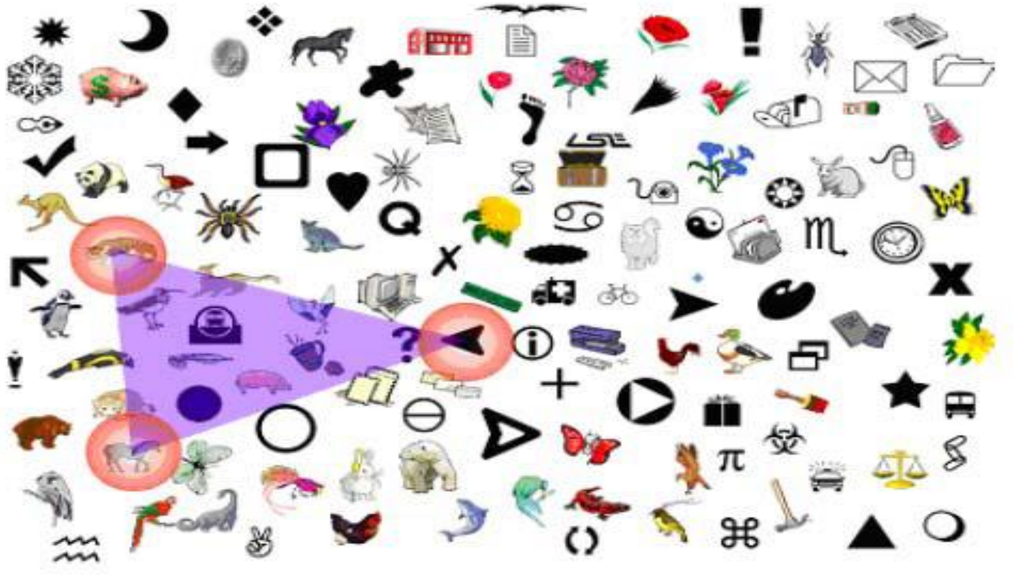

Fig: Example for Graphical password

3.2 DISADVANTAGES OF EXISTING SYSTEM

The disadvantage of traditional graphical password is that they are prone to Shoulder Surfing.Shouldersurfing refers to someone watching over the user's shoulder as the user enters a password, thereby capturing the password.

4 PROPOSED SYSTEM

An 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, which includes the password images of the user and the rest being decoy images. The user responds by clicking on the decoy images which will be inside a closed plane formed by using the password images. In each subsequent challenge the user is shown a different password window. The user logs in successfully if all challenges are responded to correctly.

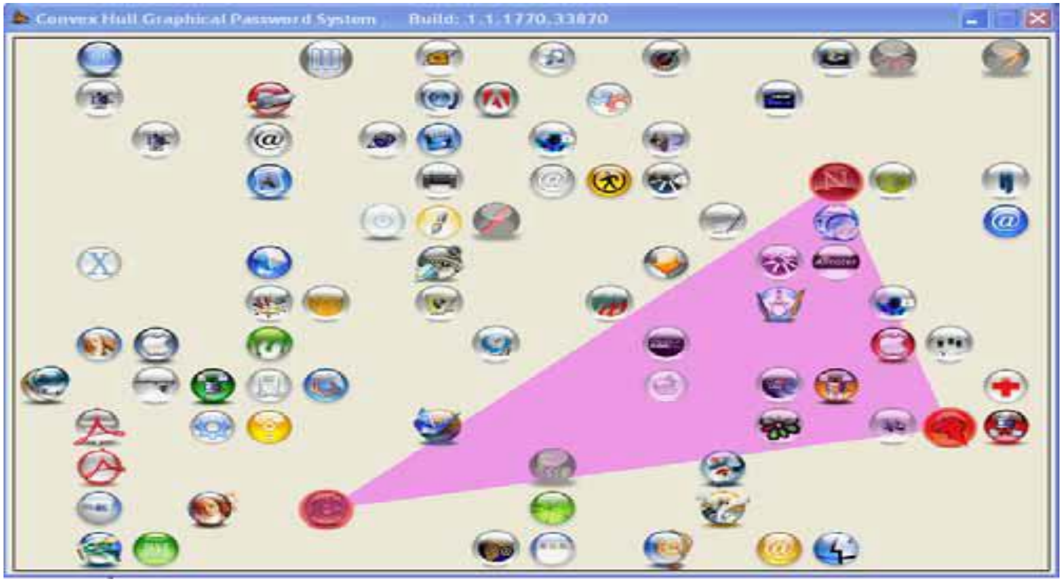

Figure 2.2: Graphical Password CHC Scheme

5 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 the 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 andJim Waters College of IST Drexel University Philadelphia,PA 19104 USA sw53, jw65@drexel.edu , LeonardoSobrado and Jean-Camille Birget Computer Science Department Rutgers University at Camden Camden, NJ 0810 USA lsobrado,birget@camden.rutgers.edu.

[2] S3PAS:A Scalable Shoulder-Surfing Resistant Textual-Graphical Pass- word Authentication Scheme by HuanyuZhao and Xiaolin Li Scalable software Systems Laboratory Department of ComputerScience 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] sShoulder Surfing attack in graphical password authentication by ARASH HABIBI LASHKARI Computer Science and Data Communication (MCS) University Malaya (UM) Kuala Lumpur, Malaysia ahabibil@hotmail.comDr. OMAR BIN ZAKARIA. Computer Science and Data Communication (MCS), Universit ofMalaya (UM),KualaLumpur, 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.