IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

Authentication Using Graphical Password

Komal Patil[1], Pranita Khape [2], Swapnali Pawar[3], Chaitrali Kamble[4], Prof.B.L.Sutar[5]

B.E Student, Department of Computer Science & Engineering, DACOE, Karad[1,2,3,4]

Professor, Department of Computer Science & Engineering, DACOE, Karad [5]

Abstract: The conventional password systems are vulnerable to shoulder surfing, many shoulder surfing graphical password systems have been proposed. However, as most users are more familiar with textual passwords than pure graphical passwords, text-based graphical password systems have been proposed. Unfortunately, none of the existing text-based shoulder surfing resistant graphical password systems is both secure and efficient enough. In this paper, we propose an improved text-based shoulder surfing resistant graphical password system by using colors. In the proposed system, the user can easily and efficiently login system. Next we analyze the security and usability of the proposed system, and show the resistance of the proposed system to shoulder surfing and accidental login[6].

Keywords: pass-colour, pass-character, graphical, shoulder surfing resistant.

I.INTRODUCTION

The shoulder surfing attack is an attack that can be performed by the hacker to obtain the user's password by watching over the user's shoulder as he enters his password.

As conventional password systems are vulnerable to shoulder surfing, sobrado and Birget proposed three shoulder surfing resistant graphical password systems. Since then, many graphical password systems with different degree of resistance to shoulder surfing have been proposed, each has its advantages as well as disadvantages.

Seeing the most users are more familiar with textual passwords than pure graphical passwords, Zhao et al proposed a text-based shoulder surfing resistant graphical password system, S3APS. In S3APS, the user has to mix his textual password on the login screen to get the session password. However, the login process of Zhao et al.'s system is complex and tedious. And then, several text-based shoulder surfing resistant graphical password systems have been proposed. Unfortunately, none of existing text-based shoulder surfing resistant graphical password systems is both secure and efficient enough. In this paper, we will propose an improved text-based shoulder surfing resistant graphical password system by using colors. The operation of the proposed system is simple and easy to learn for users familiar with textual passwords. The user can easily and efficiently to login the system without using on-screen keyboard. The rest of this paper is organized as follows. In section 2, we will review related works. In section 3 we will describe the proposed system. Next, we will analyze the security and usability of the proposed system in section 4. Finally, conclusions are made in section 5.

II.RELATED WORKS

In 2002, Sobrado and Birget proposed three shoulder surfing resistant graphical password systems, the Movable Frame, the Intersection system have high failure rate. In the Triangle system, the user has to choose and memorize several pas-icons as his password. To login the system, the user has to correctly pass the predetermined number of challenges. In each challenge, the user has to find three pass-icons among a set of randomly chosen icons displayed on the login screen, and then click inside the invisible triangle created by those three pass-icons.

In 2006, Wiedenbeck et al. Proposed the Convex Hull Click System(CHC) as an improved version of the Triangle system with superior security and usability. To login the system, the user has to correctly respond several challenges. In each challenge, the user has to find any three pass-icons displayed on the login screen, and then click inside the invisible convex hull formed by all the displayed pass-icons. However, the login time of Conve-Hull Click system may be too long. As most users are familiar with textual passwords and conventional textual password authentication systems have no shoulder surfing resistance, Zhao et al., in 2007, proposed a text-based shoulder surfing resistant graphical password system, S3APS, in which the user has to find his textual password and then follow a special rule to mix his textual password to get a session password to login the system. However, the login process of Zhao et al.'s system is complex and tedious.

In 2011, Sreelath et al. Also proposed a text-based shoulder surfing resistant graphical password system by using colours. Clearly, as the user has to additionally memorize the order of several colours, the memory burden of the user is high. In the same year, Kim et al. proposed a text-based shoulder surfing resistant graphical password system, and employed an analysis method for accidental login resistance and shoulder surfing resistance to analyze the security of their system. Unfortunately, the resistance of Kim et al.'s system to accidental login is not satisfactory. In 2012, Rao et al. proposed a text-based

DOI 10.17148/IJARCCE.2016.53229

shoulder surfing resistant graphical password system, PPC. To login the system, the user has to mix his textual password to produce several pass-pairs, and then follow four predefined rules to get his session password on the login screen. However, the login process of PPC is too complicated and tedious.

To detect and find a blood cell count and produce an accurate cell count report. This would be very helpful to a physician in identifying the cause of his patient's diseases. Analysis and processing of a microscopic image, in order to provide an automated procedure to support the medical activity and easily identify the intensity of diseases. Also maintain the patient detail and manage detail.

III. PROPOSED SYSTEM

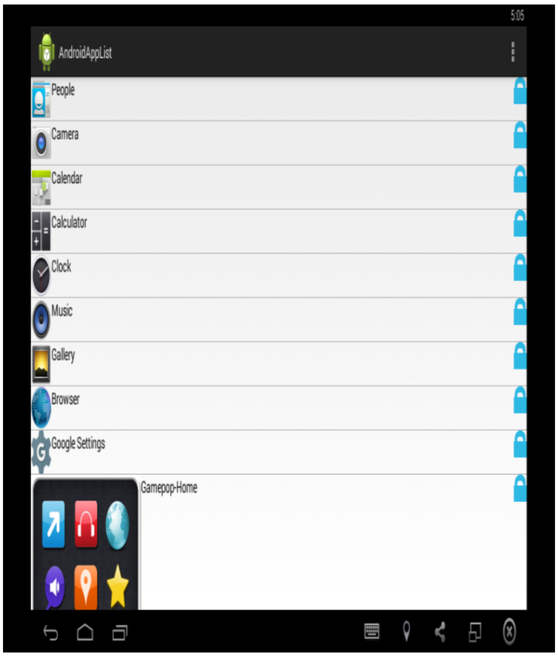
In this section, we will describe basics of our proposed system. We are using the combinations of text and colours. The alphabet used in the propose system contains 64 characters, including 26 upper case letters, 26 lower case letters, 10 decimal digits, and symbols “@” and “$”.

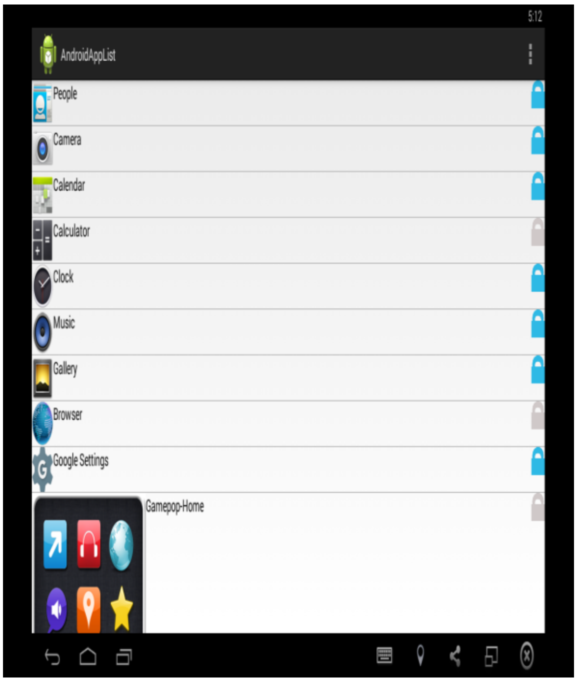
The proposed system involves two phases, the registration phase and the login phase, which can be described as in following.

A. Registration Phase-

Registration phase occurs only once when you install our application on your mobile. The user has to set his textual password K of length L(4<=L<=15) characters, and choose one colour as his pass-colour from 8 colours assigned by the system. The remaining 7 colours not chosen by the user are his decoy-colours. After successful completion of registration phase, there will be two options on the mobile screen.

The first is **lock apps**, and second is **change password**. In case, if user forgot the password then the user has to answer the security question for re-enabling system.



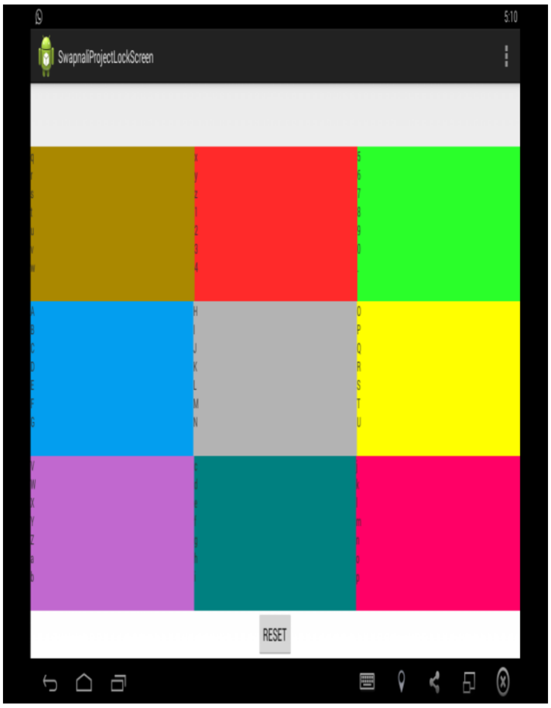


Login Phase-

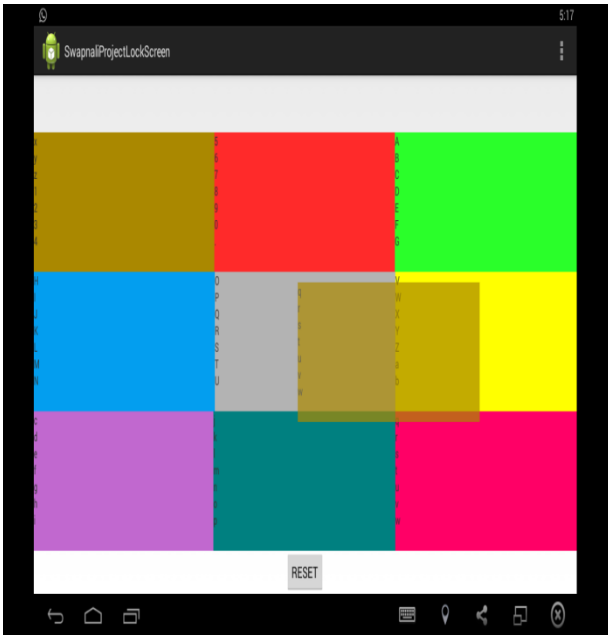
When the user requests to login in the system, the system will display our graphical password screen that is rectangle having 8 small blocks containing 8 characters in each block.

User has to drag the block which contains the pass-character into the block whose colour that is pass-colour selected by the user during registration. After dragging all the pass-characters into the pass-colour block press the button in the center.

After successfully login user can interact with an application.



DOI 10.17148/IJARCCE.2016.53229



IV.ANALYSIS

The analysis of usability and the security of the proposed scheme is analyzed in this section.

A.Password space-

The password length L with total number of all passwords is $4*64^{L}$. Therefore, the password space of our proposed scheme is-

$$P = \sum_{l=4}^{15} 4 \times 64^{L}$$

B.Resistance to shoulder surfing (R)-

There are number of combinations of pass-colours, so the resistance of shoulder surfing is—

$$R = P \times T$$

Where, T is Total number of combinations of colours,
P is password space.

V.APPLICATIONS

On various mobile of having android operating system.

VI.FUTURE WORK

We want to apply this scheme to the desktop lock screen.

VII.CONCLUSION

Our system ensures security of mobile data from unauthorized access.

REFERENCES

1. [6]A Simple Text-Based Shoulder Surfing Resistant Graphical Password Scheme Yi-Lun Chen, Wei-Chi Ku*, Yu-Chang Yeh, and Dun-Min Liao Department of Computer Science, National Taichung University of Education, Taiwan * Email: wcku@mail.ntcu.edu.tw
2. Professional Android Application Development, Reto Meier
3. http://www.google.com