Three Level Security of Data on Cell Phones

Mrs. Nutan Deshmukh[1], Tejaswini Thorat[2]
Shamali Shinde[3] ,Saleha Patwegar[4,]Rutuja Saste[5]
[1] Professor at Computer Department,
[2345] SPPU, COMPUTER Department,
Cummins College of Engineering for Women, Pune, India
[1]*nutan.deshmukh@cummincollege.in*
[2]*tejaswini.thorat1996@gmail.com,*
[3]*shamalishinde96@gmail.com,*
[4,]*salehapatwegar1995@gmail.com,*
[5]*rutujasaste68@gmail.com*

In today's networking age, it is necessary to provide security to information system. A graphical based authentication mechanism is a strong alternative for biometric, token-based, knowledge-based authentication. We are developing a unique user knowledge base, flexible, three level security system that can be useful in any organization to ensure its security through its three levels. The three levels are text based password, image based password, colour based graphical password. This levels present study of using images as password and implementation of strong secure system by using three level security. A user has the flexibility to select the number of levels of protection according to his needs. We have developed strong security system for mobile applications. Also we have phone tracking system in which if the phone is lost then it can be tracked using google maps. In this app if anyone other than owner of mobile phone tries to access the data and fails then the image of that intruder is captured through front camera and will be sent to the email id along with the location of the device.

Keywords— Security, Registration, Cued image points, Colour based authentication, text based authentication

I. INTRODUCTION

In computer and mobile security systems, the vulnerable links to be considered are the human factors. The three main fields where human computer interactions take place are security operations, authentication and developing secure systems. Here the main problem occurs in authentication. In authentication user has to submit a user name and a text password, but here the difficulty is of remembering the passwords. In general the users tend to pick short passwords so that they can remember them easily and thus these passwords can be easily guessed or broken.

The main purpose of our project is to make the security system more strong and avoid the disadvantages of text based authentication. We try to propose a multifactor authentication system that combines the benefits of various security levels and provides a safe authentication. Proposed system is user knowledge based system i.e. user has to learn by himself to use the application for strong authentication purpose.

II. PROBLEM STATEMENT

Three level security in mobile phone applications:

1) Text based Password

2) Image based password

3) Colour based graphical password

III. MOTIVATION

Three level security is important to secure the transactions and the important data and applications in the user's android system. There is no facility of providing three levels of security to any application in mobile. If wrong password is entered by user then his picture and the location will be sent to the registered email id which is provided while logging into the system.

IV. LITERATURE SURVEY

The purpose of this project is to authenticate important files in mobile devices that validates user to access the mobile application only when they have entered correct password. This project involves three levels of authentication. There are varieties of passwords available today, among those password systems some have failed due to bot attacks, hacking while few of them have sustained it but up to a limit. In short, all authentication systems available today can be broken up to a limit. Hence the aim of the project is to achieve the highest security in authentication of mobile application. In this user has to choose the number of levels of security. These levels are nothing but the number of images on which user has to set the password.

- Nowadays some existing password systems failed due to bot attacks.
- Single password system for apps and files in mobile phones.
- Most passwords are logical like we use dates, numbers, and last names to set passwords which can be guessed or hacked easily.

As the world is shifting to mobile-first generation and therefore is has become important more than ever to protect the applications as some this applications hold sensitive data. In mobile phones each application and its data is separated, also known as sandbox approach. Therefore it is important to protect the applications from unauthorised access because the access to applications means access to some crucial data of the user [1]. Text-based passwords remain the dominant authentication method in computer systems, despite significant advancement in attackers' capabilities to perform password cracking [4]. Graphical password systems are a type of knowledge-based authentication that attempts to leverage the human memory for visual information. A comprehensive review of graphical passwords is available elsewhere. Of interest herein are cued-recall click-based graphical passwords (also known as loci metric). In such systems, users identify and target previously selected locations within one or more images. The images act as memory cues to aid recall. Example systems include Pass Points and Cued Click-Points (CCP) [3]. Humans have a better ability to memorize images with long-term memory (LTM) than verbal representations. Image-based passwords were proved to be easier to recollect in several user studies. Most of these image-based passwords are vulnerable to shoulder surfing attacks (SSAs). This type of attack either uses direct observation, such as watching over someone's shoulder or applies video capturing techniques to get passwords, PINs, or other sensitive personal information [1]. The personal identification number (PIN), typically consisting of four decimal digits, is especially susceptible to observational attacks, due to its short length and the simplicity of the ten-digit keypad. The whole secret PIN could be leaked through even a single authentication session. Since PINs are so popularly used in a variety of common devices, such as smartphones, automated teller machines (ATM), and point of-sale (PoS) terminals, there is a great need for a secure PIN entry scheme that does not significantly sacrifice usability. Various security enforcement methods have been proposed to deal with this situation, but achieving both security and usability still remains a challenging goal [2].

V. PROPOSED SYSTEM

The architecture of the proposed system involves the following flow it initially consists of the registration process for user details. When the registration is done successfully, different levels of passwords are set for various applications. The login procedure is carried out by the user to get the access to the applications locked at the time of registration. If the user forgets the password the system generates an OTP and sends it to the user's registered phone number.

Modules:

Module 1: Registration

This is the first module of the application and the user details like email-id and phone number are taken.

Module 2: Text based password

The text password is included in the registration page. The user can set the password by using the special symbols, alphabets and digits. The password will be stored in the SQLite database.

Module 3: Image based password

The image based password increases the complexity level of the passwords and authentication. There are six levels of images through which the user can select the number of images and set password on that number of images. The cued point concept has been used in this module.

Module 4: Color based password

The color based password is formed by the combination of various colors and digits.

The basic concept behind this module is the user has to match the graphical password generated by the system. The password generated will be in the form of two colors into a circle(outer and inner colors) and a digit.

These are the four main modules of the application.

VI. ARCHITECTURE DIAGRAM

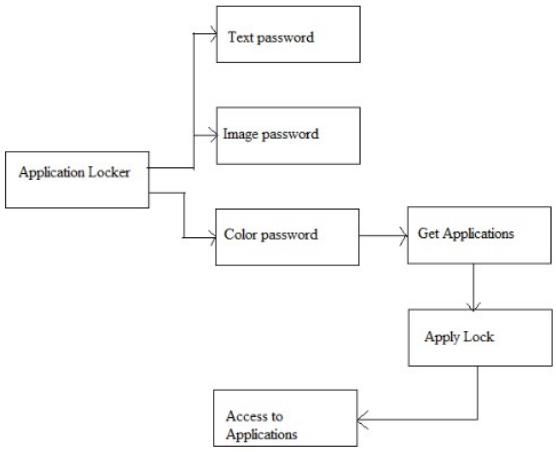

Figure 1: Architecture Diagram

VII. ALGORITHMS

The algorithms used are as follows:

1. Pseudo code for generating tolerance box for selecting pixel.

Take area, centroid, bounding boxes (bbox) and total number of blobs (n) as input from Blob Analysis block.

Let Track=empty set of vectors of type t where t= (area, centroid, box, hitcount, miscount, active, occluded)

m= Track.SizeFor i =1 to n c=0
For j=1 to m
If (percentage background in Track[j].area<50)
Then Track[j].occluded=true
End

If (|area[i]–Track[j].area|/area[i] <.05 and |centroid[i] – Track[j].centroid|/centroid[i]<.05) Then Track[j].active =true, c=1, break from loop
End
End

If c=0
Then k=Track.size++,
Track[k].area = area[i]; Track[k].centroid = centroid[i];
Track[k].bbox = bbox[i]; Track[k].hitcount = 1;
Track[k]. active = true;
End End m= Track.Size
For j=1 to m
If (Track[j].active==true)
Then
Track[j].hitcount=Track[j].hitcount+1;
Track[j].miscount=0;
If (Track[j].hitcount> 4)

Don't update pixels of Track[j].bbox in buffered Background

End

If (Track[j].hitcount> 40)

Then raise alarm for Track[j]

End

If (Track[j].active==false and misscount>3)

Then delete Track[j]

End

End

Update the buffered background

Let us suppose that after blob analysis we get 'N' number of blobs, each with its enclosing region 'Rn (t, l, h, w)', its area 'An' and centroid 'Cn(i, j)'.

2. Pseudo code for colour based -

There are six circles on window. Circles will be inner and outer with different colours and inside circle there will be number.

Random password is generated by system of various colour combination and number. i.e one inner colour , number ,outer colour.

At the first level we are giving complexity level for authentication.

Now in the backend this level number will be added in the number in randomly generated combination.

System will check whether password is correct or not.

I f it is correct then user will be able to access the application.

VIII. RESULTS

1. Set Password:

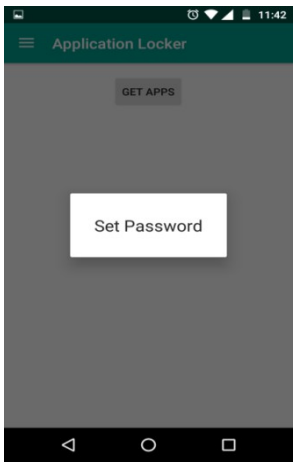

Figure 2: Set password

2. Set the complexity of image based level and text based password:

Figure 3: Registration

3. Selecting the cued point (Setting image based password):

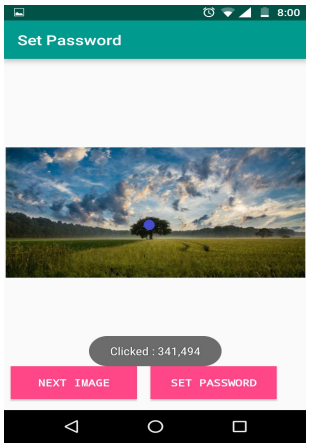

Figure 4: Set cued points

4. Lock the application:

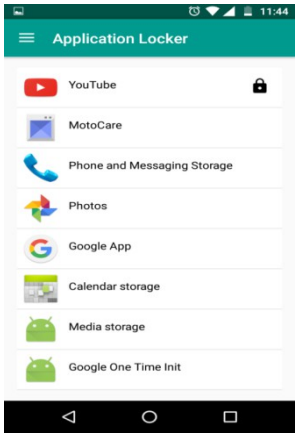

Figure 5: Application locked

5. Enter text based password (Level 1):

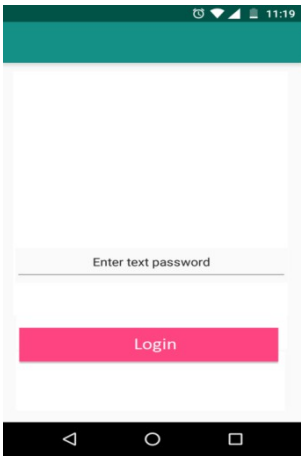

Figure 6: Level 1

6. Enter image based password (Level 2):

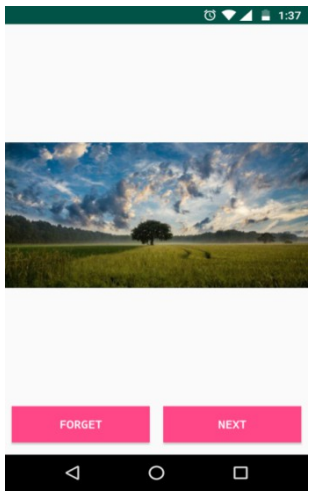

Figure 7: Level 2

7. Select the colour combination for colour based graphical password (Level 3):

Figure 8: Password generated

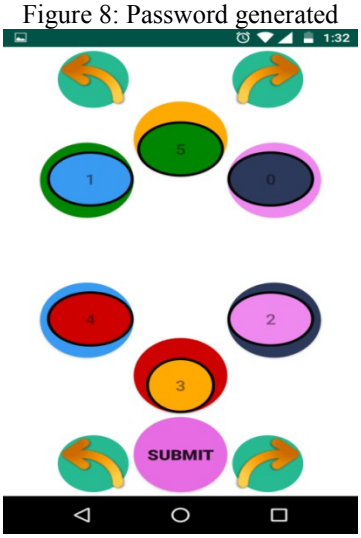

Figure 9: Select correct colour combination

CONCLUSION

The purpose of this project was to develop a strong authentication system to avoid unauthorized access by the intruders and thus to protect the applications.

When the user successfully enters all the passwords then only he will be authenticated to use the application.

The three level security makes the system highly secure and user friendly. It is time consuming and cannot be suitable for general security purposes, but will definitely be a boon in areas where high security is the main issue. The first level provides authentication using text based password. The Second level provides image based password which is easy to remember and yet complex. User has flexibility to set complexity of this level. The third level i.e. colour based graphical password is user knowledge based password level. User has to understand the system and know what the password will be.

This system maximises the effective password level use and the user application and data are protected from unauthorised access and intruding.

FUTURE SCOPE

In future, the efforts can be made in developing a system that permits the user to set different passwords for different applications. The user can also select the number of levels he wants to apply for certain application.

REFERENCES

[1] Michael T. Raggo, “Mobile Data Loss Threats and Countermeasures”, 2016

[2] Ashwini Deshpande, Suchita Singh, Amrita Kharga, Dr.Lata Ragha, “Session Passwords Using Three Level Authentication System”, March 2016

[3] Hung-Min Sun, Shiuan-Tung Chen, Jyh-Haw Yeh and Chia-Yun Cheng, “A Shoulder Surfing Resistant Graphical Authentication System”, IEEE Transactions on Dependable and Secure Computing, 2015

[4] Taekyoung Kwon, Member, IEEE, and Jin Hong, “Analysis and Improvement of a PIN-Entry Method Resilient to Shoulder-Surfing and Recording Attacks”, IEEE Transactions on Information Forensics and Security, February 2015

[5] Nagesh.D Kamble, J.Dharani, “Implementation of Security System Using 3-Level Authentication”, IJEDR, Volume 2, Issue 2, ISSN: 2321-9939, 2014

[6] N. Subash Reddy, Ravi Mathey, “Security Analysis and Implementation of 3-Level Security System Using Image Based Authentication”, December-2014

[7] Vamsi Krishna Vemuri1, S D Vara Prasad, “A Secure Authentication System by Using Three Level security”, IJESC, 2014

[8] Sonia Chiasson, Member, IEEE, Elizabeth Stobert, Student Member, IEEE, Alain Forget, Robert Biddle, Member, IEEE, and Paul C. van Oorschot, Member, IEEE, “Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism”, IEEE Transactions on Dependable and Secure Computing, Vol. 9, No. 2, March/April 2012

[9] Patrick Gage Kelley, Saranga Komanduri, Michelle L. Mazurek, Richard Shay, Timothy Vidas Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Julio L´opez, “Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms”, IEEE Symposium on Security and Privacy, 2012

[10] https://www.tutorialspoint.com/android/android_studio.htm - android studio use

[11] https://www.researchgate.net/home

[12] https://www.academia.edu/