Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 3, Issue 1, pp: (271-273), Month: January-April 2016, Available at: www.noveltyjournals.com

A Survey on Smart Security Mechanism Using Graphical Passwords

[1] Aboli Dhanavade, [2] Rutuja Jumale, [3] Shweta Bhimnath, [4] Ajay Nadargi

Department Of Computer Engineering, Sinhgad institute of technology, Lonavala

***Abstract*: Security to any of our personal thing is our most basic need. It is not possible to directly apply that standard Human-computer—interaction approaches. Important usability goal for authentication system is to support users in selecting best passwords. Users often select text-passwords that are easy to remember but they are more open for attackers to guess. Human brain is good in remembering pictures rather than textual characters. So a best alternative is being designed that is Graphical passwords. But Graphical passwords are still immature. Conventional password schemes are also vulnerable to Shoulder-surfing attacks, many shoulder-surfing resistant graphical passwords schemes have been proposed. Next, we have analyze the security and usability of the proposed scheme, and show the resistance of the proposed scheme to shoulder-surfing and different accidental login.**

***Keywords:* Shoulder-surfing, Security, Authentication, Text-passwords.**

1. INTRODUCTION

Advanced changes have been brought about by digital technology to the companies all over the world touching all the Organizational elements. Graphical Passwords is a name for a SMART SECURITY mechanism. Due to the advent of technology, everything around us is becoming smart such as Smart phones, Smart Automobiles, so why not Smart Passwords for our smart appliances.

A great deal of hype for Graphical Passwords has come due to the primitive's methods suffered from an innumerable attacks which are imposed easily. Despite the vulnerabilities, the users always prefer to go for the short passwords for the ease of remembrance and also lack for the awareness of how attackers tend to attacks. Shoulder surfing attacks, Masquerading and many more the other means used by the intruders. To overcome these problems, advanced methods of Graphical passwords have been proposed in these Graphical images as passwords a sequence of images and tap regions or Persuasive cued click points are interpreted as the whole Graphical password. Also to mitigate the shoulder-surfing attacks color scheme based graphical passwords are used. Different levels are set to upgrade the level of difficulty for the attackers. The Quality associated with the graphical passwords is that psychologically humans can remember graphical passwords far better than text and so is the best alternative chosen. Graphical passwords provide more resistance.

The major goal of this work is to reduce the guessing attacks as well as encouraging users to select more random, and difficult graphical passwords to guess.

2. BACKGROUND ON GRAPHICAL PASSWORD SYSTEM

The idea of graphical passwords, was first described by Greg Blonder is to let the user click on a few chosen regions in a image that appears on the screen. In Blonder's style graphical passwords, only pre-processed images can be used; the click regions are only chosen from the certain pre-designed regions in the image. This implies the user cannot provide images of their own for making passwords and they cannot choose click places that are not among the preselected ones. Our design allows the use of any image. Moreover, we let users choose any places that attract them as the click regions,

such places are easier to remember. Graphical password system can be classified as either Recognition based (image-based scheme), cued recall-based scheme (image-based scheme) or pure recall-based scheme(grid-based scheme)

- **Recall based techniques:**

Three types of click based graphical passwords techniques are there:

i. Pass Points:

It is a click based graphical password system where password consists of ordered sequence of 5 click-points on a pixel-based image.

ii. Cued-Click Points:

For this technique, user selects one point per image for 5 images. One image is displayed at a single time. The image is replaced by the next image as soon as the user selects a click point.

iii. Persuasive Cued-Click Points:

For this advanced technique a single image consists of 5 click points, one on each of five images.

3. RELATED WORK

Here we examine some of the possible techniques for breaking the graphical passwords and do a comparison with the text based passwords.

1. Dictionary attacks:

It is a method of breaking into a computer by reading every word in a dictionary as a password. So graphical passwords is less vulnerable to this attack.

2. Guessing:

Graphical passwords cannot be easily predicted because of the unpredictable nature of passwords created by the real world users.

3. Shoulder Surfing:

Recognition based techniques are designed to resist the shoulder-surfing attacks.

4. PROPOSED SYSTEM

Graphical password systems are the type of knowledge-based authentication that attempt to upgrade the human memory for visual information. In Pass Points, passwords consists of a sequence of 5 click-points on the given image. User may select any pixel in the image as the click-points for the password. To log in, the user repeats the sequence of click-points in the correct order, within a system-defined tolerance square of the original defined click-point.

We are also taking care of shoulder attack by using random number generation method.

i. Password setting:

We are getting images from the Dropbox and user will choose the sequence of image co-ordinates as the password. Then the user will set that password for application installed in his mobile.

ii. Password Comparing:

At the time of accessing the application, application will download images from drop box and user will enter the sequence of the click-points. We will use tolerance box for it so that even if the user's click size changes it will be adjusted.

iii. To overcome shoulder attack:

Color Based Shoulder Surfing prevention in this section after entering the graphical password, user will have to set one more password. This password length is going to be 8 to 15 characters. And these characters are arranged in a circle with

8 different colors. User has to choose his pass color. So when user unlocks the application using graphical password. He needs to enter this password also properly by rotating the circle clockwise or anti clockwise.

5. PROPOSED ARCHITECTURE

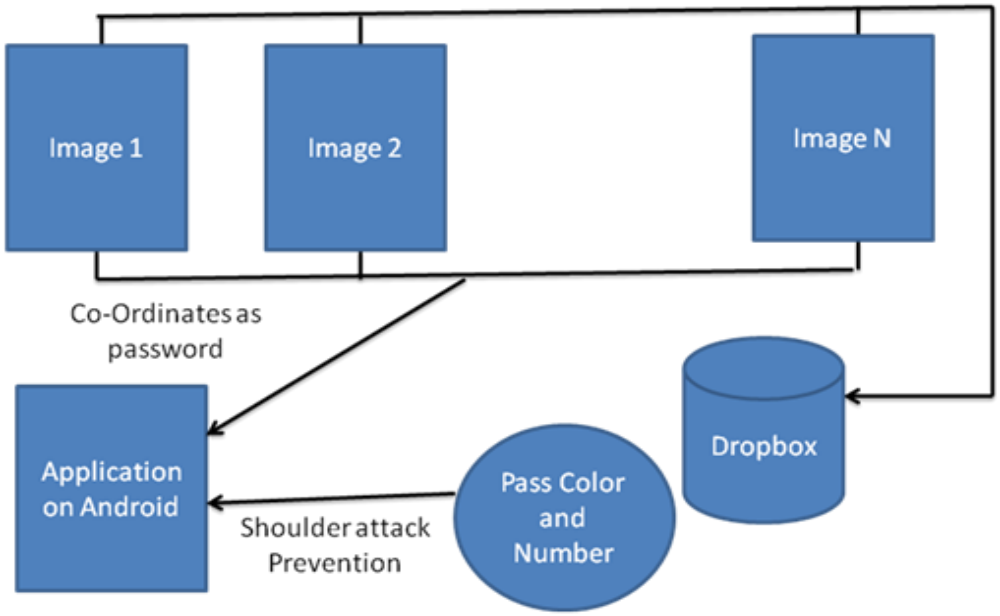

Fig.: Proposed System Architecture

In the figure mentioned above we obtain the pre-defined number of images as the password with the pre-determined click-points. We have also prevented the danger of shoulder surfing attack.

6. CONCLUSION

By taking advantage of user's ability to memorize the images as password we are using password in the form of image. By using these graphical passwords we have an advantage over alphanumeric passwords. And henceforth we provide a usable, memorable, and a secure mechanism.

ACKNOWLEDGEMENT

We would like to thank our project guide Prof. Ajay Nadargi for his abundant co-operation and guidance. We are extremely grateful to our guide who whole heartedly supported the project and gave freely of his precious time while making this project. The technical guidance provided by him was more than useful and made the project successful. We would also like to thank our Department of Computer Engineering, Sinhgad Institute of Technology, Lonavala.

REFERENCES

[1] Chippy.T, R.Nagendran, "Defenses against large scale online password guessing attacks by using persuasive cued click points."

[2] "Cued Click Point Technique for Graphical Password Authentication"Vaibhav Moraskar1, Sagar Jaikalyani2, Mujib Saiyyed3, Jaykumar Gurnani4, Kalyani Pendke

[3] Simple Text-Based Shoulder Surfing Resistant Graphical Password Scheme CCP IEEE 2013

[4] IEEE_Attacks_PassPoints_Graphical_Passwords

[5] http://link.springer.com/article/10.1007%2Fs10207-009-0080-7.