Available online www.ejaet.com

European Journal of Advances in Engineering and Technology, 2015, 2(3): 33-37

Research Article ISSN: 2394 - 658X

LockZoo-Security App for Handheld Devices

Akanksha J Kulkarni, Dipali R Shinde, Sanjivani R Gaidhani, Yogita B Labhade and Monali Borade

Department of Computer Engineering, Matoshri College of Engineering & Research Centre, Nasik, India
akankshajkulkarni@gmail.com

ABSTRACT

Security of apps is becoming one of the major concerns today. Android mobile phones are the most popular way to access social sites, mails very easily. Many applications are available for android users to protect their applications. But, these applications are not enough to provide high end security. So this paper focuses on the new techniques for providing better security to the android apps that will remove the attacks such as shoulder surfing, sharing of password attack, guessing attacks etc. To address these attacks this paper introduces different password schemes. This paper elaborates the survey done for 4 techniques and the attacks they can withstand.

Key words Android application security, Password, shoulder surfing, apps

---

INTRODUCTION

Various conventional applications use text and numbers as a password to secure mobile applications. But these passwords are susceptible to snoop, dictionary attacks, social engineering and shoulder surfing. Graphical passwords are introduced as alternative techniques to textual passwords. Most of the graphical schemes are vulnerable to shoulder surfing [1]. To address this problem, text can be combined with images or colors to generate passwords for authentication. For each login, new password is generated and stored. In this paper four techniques are proposed to generate the password using the combination of text, numbers, colors and CAPTCHA. Amongst them two authentication schemes are for session passwords which are resistant to shoulder surfing. These methods are suitable for Personal Digital Assistants and also use CAPTCHA for authentication that are resistant to online password guessing attack. These schemes are specially developed for android users using which they can secure their desired applications. This paper discusses various authentication techniques that provide intense security and solution on password cracking attacks. Previously many works are done to provide security to android application. Captcha is a standard Internet security technique to protect online services from being abused by hackers. CaRP password can be found only probabilistically by automatic online guessing attacks even if the password is in the search set [2]. By using robust discretization implementation of graphical password schemes is done in very flexible and versatile manner than any another. But those schemes lead to direct shoulder surfing. CAPTCHA as a graphical password lead to the better use of graphical password scheme and to resist spyware. By Using a CAPCTHA as a password improved the security of the online systems accessed on mobile devices. On the other hand, there occurred some challenges for drawing the CAPTCHA in overlapping images. Some graphical password are used on basis of Persuasive click points including usability and security but these passwords based on recall based technique [3].Also Persuasive Cued Click points Graphical Passwords having usability and security but user has to reproduce the information filled or selected at the time of registration [3]. Graphical passwords in the form of images were used for security but, those are not as such consistent in the usability and security evaluation of various schemes [3]. Previously used Graphical Passwords were difficult to guess the click points. But on the contrary, user had to remember the order of the click points that are clicked at the time of the registration [4].

EXISTING METHODOLOGY

There are various applications that provides password as a security tool for a mobile, especially for android phones. Applications like AppLock, Fast AppLock and Smart AppLock provide passwords to secure android apps. These apps provide security to android applications but not up to the mark. They protect android applications by giving passwords, but there is no any security tool to protect the password! But these apps provide security in the form of numbers and patterns only. While in some phones Face Lock, Image password facility is also there. By studying existing techniques and algorithms, the literature survey came to a conclusion with the aim of removing limitations of existing techniques such as,

- Some methods only provide password to secure the apps but cannot secure the password.
- There are some attacks in exiting system such as dictionary attack, guessing attack etc.
- Graphical passwords do not show consistency in the usability and security
- The scope is limited to secure the application only.
- Direct Shoulder Surfing is the problem of Graphical password based on Robust Discretization.
- Difficult to user, to remember the order of click points which are clicked at the time of registration.

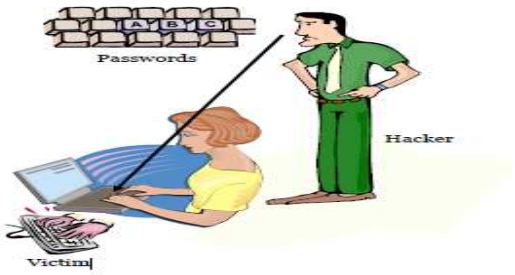

Fig. 1 Shoulder Surfing

PROPOSED SYSTEM

To design system for users, there are pattern matching schemes, numbers based password schemes, but these are not free from eves dropping, dictionary attacks, social engineering and shoulder surfing etc. Also there are no such applications or system that provides different locking scheme to different android applications along with capability to withstand against such mentioned attacks, Rest of the part of this section describes two important characteristics of proposed system System features and attacks.

(i) System Features

- Protection to Android phone password
- Providing different passwords to different application
- GPS for location tracking
- Photo Capturing
- Security Keys

(ii) Attack Intent

- Human guessing Attacks
- Shoulder surfing
- Automatic Online guessing attacks
- Security of underlying CAPTCHA

(iii) System Architecture

- After selection of apps for providing security, next step is to set the password to the selected apps. To set the password, Proposed System has four different password schemes, as follows
  - Pair Based Authentication
  - Hybrid Textual Authentication
  - Graphical Password
  - CAPTCHA
- After selection of scheme, user will set his original password according to the selected password scheme. After this, that particular app/s will lock.
- While unlocking of an app, user has to enter the combinations of original password according to the selected password scheme.
- If the entered combinations (password) is matched with the original password, then that app will unlock, but if wrong password, the Proposed System will give two more attempts to enter the correct password.
- But if someone crossed this limit, then System needs to take security steps such as, sending location through GPS, sending pictures with the help of primary or secondary camera

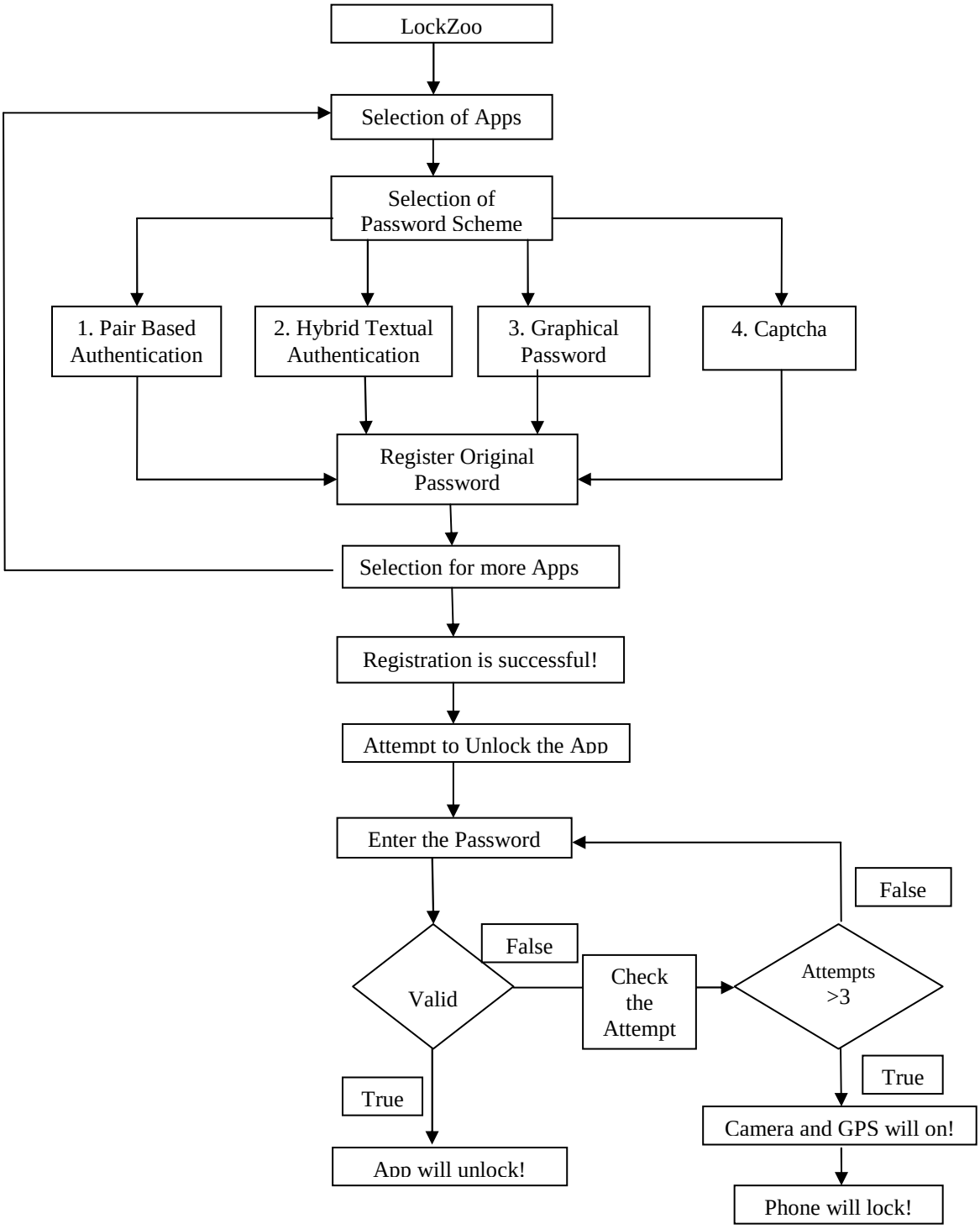

Fig. 2 Architecture of the Proposed System

PASSWORD SCHEMES

Pair Based Authentication

Pair-based authentication (grid) is the 1st technique that LockZoo will provide to protect the password. When user will login or open the any application then the interface like 8*8 or 6*6 will be shown. It consists of alphanumeric characters and special characters too. Instead of typing the password user will click on the grid letters to enter his password but that also in different way. The limitation for the original password is that it should be in the even number of characters. Mechanism is like, LockZoo indirectly divides user's original password in the pair of two. Consider that user's original password is “abcd”, then 2 pairs will formed as “ab” and “cd”.then user will create his new password by clicking the intersection point of the each of the 2 formed pairs. That is intersection point of ‘a’ and ‘b’ from the grid will the first letter of the new password [5]. This scheme will remove the shoulder Surfing attack, sharing of password attack.

Fig. 3 Pair based Authentication

Fig. 4 Color Grid

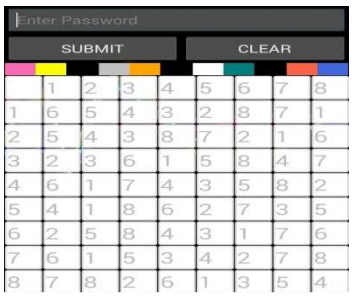

Fig. 5 Color Matrix

Hybrid Textual Authentication

Hybrid Textual Authentication Scheme (using colors) is the 2nd scheme that LockZoo will provide. The fix set of colors will be given to the user and user has to rate the color. According to the rating provided to the colors further operation will precede. The similar mechanism as Pair-based Authentication scheme (grid) will be followed here. According to the rating, again one grid will formed which is the combination of numbers only. In the Pair Based Authentication (Grid) user has to click on the intersection point of the two color ratings [5]. That is similar process will be carried out. This scheme will remove the shoulder surfing attack, sharing of password attack.

Graphical Password

In this section, we will describe a simple and efficient shoulder surfing resistant graphical password scheme based on texts and colors. The alphabet used in the propose scheme contains 64 characters, including 26 upper case letters, 26 lower case letters, 10 decimal digits, and symbols "." and "/".The system displays a circle composed of 8 equally sized sectors, and places 64 characters among the 8 sectors randomly so that each sector contains 8 characters. The 64 characters are in three typefaces in that, the 26 upper case letters are in bold typeface, the 26 lower case letters and the two symbols "." and "/" are in regular typeface, and the 10 decimal digits are in italic typeface. In addition, there is button for rotating in clockwise or in counter clockwise direction [6]. Graphical Password will remove the shoulder surfing attack.

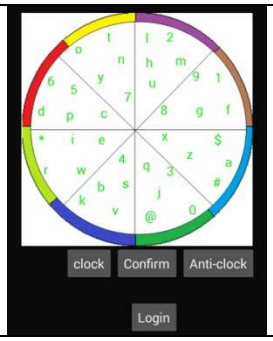

Fig. 6 Graphical Password

Fig. 7 CaRP Image

CAPTCHA Password

CAPTCHA scheme is used to remove the online guessing attacks, streaming, etc. To generate CAPTCHA image there is a CAPTCHA engine. That CAPTCHA engine will generate CaRP image that is CAPTCHA as a graphical Password [7]. There is an Authentication server at the server side, and that server stores user's original password. When user will click on his password letters/numbers/etc the co-ordinates of those clicked points will be sent to the server and server will match those co-ordinates with the original password saved. This scheme will remove the human guessing attacks, prevent user's phone from hacking.

CONCLUSION

This paper has presented a survey and some techniques for preventing different type of attacks .To prevent android user, first various types of attacks are identified and then different type of password schemes are introduced to resolve these attacks. This paper presented a new approach to protect user's password against spyware attack. Main contribution is that to introduce CAPTCHA into the realm of graphical passwords to resist spyware programs. From a security viewpoint, this exploration is expected to advance the development of passwords. Future evaluation work should focus on evaluating the different password schemes and practical implementation also. Practical approach can be extended by providing plug-ins.

Acknowledgements

The authors wish to thank University of Pune and also thank the participants of our lab study for their time and valuable feedback.

REFERENCES

[1] S Chiasson, P van Oorschot and R Biddle, Graphical Password Authentication Using Cued Click Points, *Computer Security, ESORICS*, **2007**, 359 374.

[2] R Lin, SY Huang, GB Bell, and YK Lee, A New CAPTCHA Interface Design for Mobile Devices, *12th Australasian User Interface Conference (AUIC 2011)*, Perth, Australia, **2011.**

[3] X Suo, Y Zhu and G Owen, *Graphical Passwords: A Survey*, **2005,** *www.acsac.org.*

[4] S Chiasson, A Forget, R Biddle and P van Oorschot, Influencing Users towards Better Passwords: Persuasive Cued Click Points, *Published by the British Computer Society*, **2008.**

[5] M Sreelatha, M Shashi, M Anirudh, MD Sultan Ahamer and V Manoj Kumar, Authentication Schemes for Session Passwords using Color and Images, *International Journal of Network Security & Applications*, **2011**,3(3).

[6] Yi Lun Chen, Wei Chi Ku, Yu Chang Yeh, and Dun Min Liao, A simple Text Based Shoulder Surfing Resistant Graphical Password Scheme, *IEEE 2nd International Symposium on Next Generation Electronics (ISNE)*, Kaohsiung, Taiwan, **2013.**

[7] BB Zhu, Jeff Yan, Guanbo Bao, Maowei Yang and Ning X, CAPTCHA as Graphical Passwords a New Security Primitive Based on Hard AI Problems, *IEEE Transactions on Information Forensics and Security*, **2014**, 9(6).