AN IMPROVED GRAPHICAL AUTHENTICATION SYSTEM TO RESIST THE SHOULDER SURFING ATTACK

M. Shanmuganathan[1], R. Sudha[2]
Dept. of Computer Science and Engineering.,
Adhiparasakthi Engineering College. Melmaruvathur, India

Abstract

The consumption of banking applications are more and popular on Android devices but it is not secure. To make secure on those confidential application such as banking, business application and personal data, password is provided to enhance privacy. Nowadays those passwords are easily usurped by hackers through shoulder side attacks or observing videos. To overcome from this inconveniences of accessing the account in public places, the proposed idea is to make smart way to authenticate the user bank account through the pictorial password and by injecting the indirect pin to the system. To predict the original password, temporary login indicator is used while accounting to login. The Existing paper does not safeguard the user's account from hackers, when the password is misused. The forget password module and banking service module is added which could be innovative and an effective idea to authenticate the proposed system. By implementing the above proposed idea, data and information on devices are maintained confidentially.

Index Terms— Shoulder Side attacks; Login Indicator; Hackers.

I. INTRODUCTION

Android is an open source and Linux-based operating system for mobile devices such as smartphones and tablet computers. Android was developed by the Open Handset Alliance, led by Google, and other companies. The code names of android ranges from A to N currently, such as Alpha, Beta, Cupcake, Donut, Eclair, Froyo, Gingerbread, Honeycomb, Ice Cream Sandwitch, Jelly Bean, KitKat, Lollipop and Marshmallow. Android applications are usually developed in the Java language using the Android SDK. Once developed, Android applications can be packaged easily and sold out either through a store such as Google Play, SlideME, Opera Mobile Store, Mobango, F-droid and the Amazon Appstore. The term Security means that something has been secured from unknown / third parties. The Password is Secert of word. The act of directly or indirectly attacking assets from users is called a "threat." Furthermore, the malicious person or applications that commit these acts are referred to as the source of the threats. Malicious attackers and malware are the sources of threats but are not the threats themselves.

This paper analyzes the password hacking methods and overcome by providing injecting indirect password method using OTP. It secures the system by using pictorial password scheme for banking application on smartphones. This scheme will enhance the privacy of the account. It protects the user's password from Shoulder side attacks by graphical authentication system. It also provides the forget password module and banking system services to users to recover the user's data.

II. EXISITING SYSTEM

In the Existing system, the users have to upload or select the pre-defined image that provided by the server as a password image. The user selects the image as password. Meanwhile, the server will splits the password image to 7x11 grids and

display the images to the user in grid view, and user select the single grid as a password grid for the particular image. Also, the user can upload with multiple images as per their need and select the passpoint on each uploaded image in registration phase. After the successful registration, the server will store those data on it.

While accounting to login, login indicator is provided. It is only visible by closing the proximity sensor of the user device and sees the LI in circular view by using hands. Your login indicator will be in the form of A→6. In vertical and horizontal bars, the alphabets and numeric values will be shuffled randomly. By moving, the user should place the value A vertically straight to the password grid, and move value 6 horizontal straight to the password grid then press OK, the grid will be authenticated and then user is provided with next image and new login indicator if needed. After completing all image authentications, if the entered LI is correct the services will be provided.

III. SYSTEM DESIGN

From the below system design, it clearly understood the process of password authentication. The user's password is authenticated using the Login indictor to hide the original password of the user. By this way the login indicator is useful for authentication.

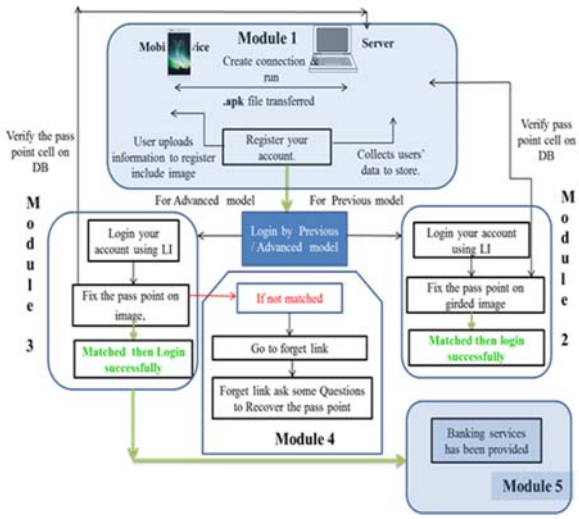

Fig. 1. System Archieture

IV. IMPLEMENTATION

A. *Account creation and registering your password:*

The users register the account with providing the user information, optional mobile number and the email to make alert about user account in some extreme cases. The users can upload the image by select the pre-defined image provided by the server as a password image. After user selects the image as password the server process with the image and split the password image to 7x11 grids and display all grid images to the user, and then user selects the single cell as a passpoint for the particular image. The user can upload with multiple images as per their needs and select one passpoint grid of each image. If you click submit button, the password will be stored and account will be registered.

B. *Authentication using graphical authentication:*

Authentication of the user's account by graphical authentication system. While logging in, the user is provided with the LI (temporary password). The login indicator is only visible while closing the proximity sensor of the user's device and the sees the LI by holding the 4 points in the screen using hands. Next the user is displayed with the gridded password image with movable horizontal alphabetic bar and movable vertical numeric bar.

The login indicator will be in the form of A , 6. In vertical and horizontal bar the alphabets and numeric values will be shuffled randomly. The user can move the bar values by using navigation keys provided below. By moving, the user should place the value A vertically straight to the password grid, and move value 6 horizontal straight to the password grid then press OK, the grid will be authenticated and then user is provided with next image and new login indicator if needed. After completing all image authentications, if the entered LI is correct the services will be provided.

C. *Authentication using Advanced Graphical system:*

This system has one time registration event i.e. registering the account on device is done only once for each IMEI number. On registration phase the user has to upload their datas including images either they can use single or multiple images that is user's choice to select from gallery. After the successful registration, server will collect all those data to store in the database.

During login phase, LI (login indicator) value is provided to user. It is only visible by closing

the proximity sensor and sees the LI by holding the 4 points displayed on screen. The LI value is in single numeric form 1 to 9. In this system the image is loaded and above the image the numeric numbers will scattered throughout the screen. The user can touch the single numeric value and drag it. The whole scattered numbers will be moved with respective to the numeric value that user is dragging. User has to drag any of the number and correspondingly place user's LI value on the image passpoint specified by the user during registration. If valid passpoint, Login Successful message will displayed.

D. Forget password and recovering phase:

1. The forget password and recovery module, to achieve this using an innovative idea of security questions about the user handset such as charging percentage in last 2 days.

    - Have you used camera in last two days?
    - Have you installed any of the application?
    - Have you registered any event for past and future 7 days?

2. The system can concentrate on the log files (camera, battery usage, calendar information, call log, installed applications) of the user mobile and frame the questions based on that.

E. Banking Services:

The banking services that are called virtual money concept, initially the user credited with rupees and if user is in need to transfer the money to some other account the user go to his withdrawal and enter the amount to transfer. The voucher id generated for the amount you entered. The user can share the voucher id to the particular user. User has to sends the deposit link and enter the voucher id given by user who is transferred the money.

The amount will be DEBITED from user's account and CREDITED to depositor account. If suppose hacker misusing the user's account by injecting the wrong password frequently then the server will track the location of the device and sends email or SMS to user and it blocks the account to secure the user's information on the device.

V. CONCLUSION

The improved graphical authentication application system resists the shoulder surfing attacks has been implemented. The user has to inject the account password to the server in the indirect manner using some temporary login indicator which is an interactive approach to the user. Secures the bank account from hackers by blocking, when the mobile was lost.

ACKNOWLEDGMENT

The preferred spelling of the word "acknowledgment" in America is without an "e" after the "g." Avoid the stilted expression "one of us (R. B. G.) thanks ...". Instead, try "R. B. G. thanks...". Put sponsor acknowledgments in the unnumbered footnote on the first page.

REFERENCES

[1] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon,"Passpoints: Design and longitudinal evaluation of a graphical password system," International Journal of Human-Computer Studies, vol. 63, no. 1-2, pp. 102–127, 2015.

[2] T. Takada, "Fakepointer: An authentication scheme for improving security against peeping attacks using video cameras," in Mobile Ubiquitous Computing, BT Technology journal vol. 44, no. 3, pp. 395–400. 2015.

[3] S. Gurav, L. Gawade, P. Rane, and N. Khochare, "Graphical password authentication: Cloud securing scheme," in Electronic Systems, Signal Processing and Computing Technologies (ICESC), 2014.

[4] Pas: Predicate-based authentication services against powerful passive adversaries," in 2014 Annual Computer Security Applications Conference. IEEE, 2014, pp. 433–442.ational Conference on, Jan 2014, pp. 479–483.

[5] H. Zhao and X. Li, "S3pas: A scalable shoulder-surfing resistant textual-graphical password authentication scheme," in Advanced Information Networking and Applications Workshops, 2012, 21st International Conference on, vol. 2IEEE, 2007, pp. 467–472..

[6] S. Chiasson, P. van Oorschot, and R. Biddle, "Graphical password authentication using cued click points," Computer Security–ESORICS 2007, pp. 359–374, 2007.

[7] J. Thorpe and P. van Oorschot, "Human-seeded attacks and exploiting hot-spots in graphical passwords," in Proceedings of 16th USENIX Security Symposium on USENIX Security Symposium.USENIX Association, 2007, p. 8.

[8] D. Hong, S. Man, B. Hawes, and M. Mathews, "A password scheme strongly resistant to spyware," in Proceedings of International conference on security and management, 2004.