Graphical Based Password for Android Phones using Keystroke Dynamics – A Survey

Madhuri Shinde[1] Dipali Sutar[2] Jasraj Mundada[3] Shalaka Deore[4]

Abstract— Technology has elevated to grab an important position in humans life, the best example is smartphones. They offer access to network as well as online banking transactions, where simplification of human labour affects security and user authentication, and passwords are first line of defense, it's crucial to pick a strong password. Online banking applications currently use alphanumerical usernames and passwords for authentication, which are exposed to eves dropping, attacks, and shoulder surfing. Users often choose either easy to remember passwords, which can be easily guessed or difficult ones, which tend to be forgotten. The paper revolves around the views, limitation of current system and offers a dynamic biometrics, as it can be easily integrated into the existing computer security systems with minimal alteration and user intervention. The main objective is to secure using cued click point (CCP), which is one click based graphical password scheme for sequence of images and measuring, assessing humans typing rhythm, it's based upon the human tendency to memorize graphical passwords more comfortably.

Key words: Smartphones, authentication, keystroke dynamics, cued click point, password

I. INTRODUCTION

Smartphones have an important role to play in lives of common man, the applications provided can access network to perform desirable operations. The applications such as online banking transactions provide alphanumeric for validation, users either choose a password easy to remember, or if difficult, they are prone to forget [10]. The textual passwords are exposed to attackers, by mere guessing.

An alternative proposed included images, graphical pictures to be used as passwords. Since human brain has the capability of remembering, and recollecting images better than texts, or numbers, the idea was made the basis of protection initially, many applications using this method can be found in market.

Biometrics, the physical traits and behavioral characteristics that make each of us unique, are a natural choice for identity verification [8]. But researchers realized the immature move had disadvantages, the common problem was any onlooker can peep in and illegally know the graphical password. Other problems were the processing time taken was long. The impatience frustrates user, thus reducing the popularity of the method. The behavioral biometric of Keystroke Dynamics is the manner and rhythm in which an individual types characters on a keyboard or keypad [13]. However, each person may have different styles to press the key because the typing style is based on user's experience and individual skill which is difficult to imitate [7].

This paper proposes to merge persuasive cued click points and password guessing resistant protocol. The rapid increasing interest in this field has made it innovative in ways to make it more efficient for security purposes. Keystroke dynamics was introduced to guard against the unauthorized access. This biometric technique doesn't require any special instrument or device to identify individual characteristics, like face scanner, iris, signature, or fingerprint scanner. It increments the level of security by adding biometrics as the main factor.

II. CLASSIFICATION OF AUTHENTICATION METHODS

Authentication by Vangie Bael is the process of identifying an individual, usually based on a username and password. In security systems, authentication is discrete from consent, which is the process of giving individuals access to system objects based on their identity.

The authentication methods can be divided into three major parts, such as Token based (two factor), Biometric based (three factor), and Knowledge based (single factor) authentication [1].

A. Token Based

It is a validation method to authenticate the user who attempt to log in to server. It allows users to input their username and password in order to retrieve a token which allow them to fetch a particular resource - without using their username and password. Once their token has been obtained, the user can offer the token - which offers access to a specific resource for a time period - to the remote site [6].

B. Biometric Based

Biometrics is the study of automated methods for recognizing individuals based upon one or more elemental physical or behavioral traits [6]. A biometric scanning device takes a user's biometric data, such as an iris pattern or fingerprint scan, and converts it into digital information a computer can interpret and verify.

C. Knowledge Based

Knowledge based approach are the most broadly used authentication techniques and include both text and image depend on passwords. It is an authentication scheme in which the user is asked to answer at least one "secret" question [6]. Knowledge is basically the fact of knowing, general understanding of particular subject, such as Personal Identification Number (PIN), password or pass phrase [11].

III. PASSWORD HISTORY

A password was originally a secret word used to identify friends from enemies. Blonder was the first person to describe graphical passwords. Since then, many other graphical password schemes have been proposed. Graphical password systems can be classified as either recognition-based which are usually are image based scheme, cued recall-based (image based scheme) or pure recall-based which are grid based scheme.

IV. RELATED WORK

1) Proposed a new hybrid graphical password based system for smart hand held devices (like smart phones i.e. PDAs, ipod, iphone, etc) which are easy to use and comfortable. The system is an association of recognition and pure recall based techniques and that avoids existing systems limitations and may be more convenient for the user. The approach is resistant to various attacks on graphical passwords. He proposed an authentication system which takes digits as password as selected for the images (objects) priori.
2) Paper uses a static keystroke dynamics in user authentication. The inputs given are the key down and up times and the key ASCII codes captured while the user is typing a string. This paper presents a scheme through typing biometrics features that improves the usual login-password authentication. This paper depicts the influence of practical aspects: the familiarity of the target string, the two-trial authentication, the adaptation mechanism, the timing accuracy, and the number of samples in enrollment, which were tested and observed.

V. PROBLEM DEFINATION

Smartphone nowadays access internet, and through applications the transactions can be performed, but validation of the user becomes the major problem. The current method to secure user authentication in online banking application includes textual passwords which are prone to eves dropping, shoulder surfing and dictionary attacks. Our project proposes a system where graphical passwords are chosen as an alternative to avoid above pitfalls. Text can be combined with images or colors to develop session passwords for authentication, these can be used only once as every time a new password is generated [14]. In this paper we propose simple yet elegant method called Cued Click Points (CCP) which is click based graphical password technique, to provide solution to the authentication problem in ubiquitous manner. The fundamental idea of CCP is based on premise that humans psychologically are better at identifying, remembering and recollecting graphical patterns than text patterns. Keystroke dynamics is measured with every CCP that user gives as an input, after authentication, the application can accesses for further operations.

A. Algorithms

Behavioral biometric, keystroke dynamics measures, calculates the typing rhythm of the user particularly while authentication. The aim of our work is to provide 3 levels in terms of security for transaction in banking applications.

1) AES Algorithm

Advanced Encryption Standard, a symmetric 128-bitblock data encryption technique developed by Belgian cryptographers Joan Daemen and Vincent Rijmen. The U.S government adopted the algorithm as its encryption technique in October 2000, replacing the DES encryption it used. AES works at multiple network layers simultaneously.

The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input, called the plaintext, into the final output, called the cipher text. Each round consists of several processing steps, each containing four similar but different stages, including one that depends on the encryption key itself. A set of reverse rounds are applied to transform cipher text back into the original plaintext using the same encryption key. Once the user is registered, the user is shown the next phase, graphical password screen.

2) Graphical Password Using CCP

Graphical passwords have been designed for more secure and that to make passwords more memorable and easy to use by the people. Pass Points, CCP, and PCCP use a grid-based discretization algorithm to determine whether login click-points are within tolerance. [5] Using this technique users click on the images rather than typing alphanumeric passwords. User is shown with sequence of images with 4x4 blocks; user has to select N blocks from each image [9],[12]. If user enters an incorrect click-point during login, the next image displayed will also be incorrect.

3) KDA (Keystroke Dynamic-Based Authentication)

A touch event includes the on touch down and up, producing five features DU, DD, UD, UU, DU2 defined as follows[15].

- Down-Up (DU) time: DU time is the interval between the same click being pressed and being released.
- Down-Down (DD) time: DD time is the interval between the click being pressed and the next click being pressed.
- Up-Down (UD) time: UD time is the interval between the click being released and the next click being pressed.
- Up-Up (UU) time: UU time is the interval between the click being released and the next click being released.
- Down-Up2 (DU2) time: DU2 time is the interval between the click being pressed and the next click being released.
- Internet Banking application Login, fund transfer and balance enquiry.

VI. COMPARISON WITH EXISTING SYSTEM

The proposed idea holds advantages over current system, the system adversely adding up to benefits presently in use. The alphanumeric system used in online applications are vulnerable to attacks namely shoulder, brute attacks, any person can guess the combination of words and numbers, leaving the authentication of a person weakly managed. Following psychological mindset on humans, they remember, recognize images better than passwords which contain combination of words, numbers and characters. Our idea offers graphical passwords which are set by users according to their own preferences.

[4] Ray's scheme holds limitations if compared, even if they chose objects which are symbols, characters, auto shapes, simple daily seen objects etc., still the user has to remember both the objects and string and the code. The user has to first give his username and textual password and then put digits pre-selected. These digits are then matched with the digits storedin the database. The error probability is from the power of user to remember the combination.

[2] The proposed system uses Painting Album Mechanism is an anti-shoulder surfing mechanism, which has characteristics of both recall and recognition graphical techniques. In this Swipe Scheme, Color Scheme, and Scot Scheme are the methods for password creation. Each input

scheme is non-identical, and it is user's options to choose the input scheme they prefer. The user has to remember three things every time authentication is to be done on online banking applications, the time consumed large, and its tedious to go through the whole process every time. Our project mainly focuses on biometrics, thus the user in our technique has to recognize only pictures, the database will store pictures and keystroke dynamics of the specific user.

VII. Conclusion and Future Work

We have studied keystroke biometrics variant with regard to the possible use of identification and a support for user authentication. With analysis of only two keystroke features and with the use of simple classifier the keystroke dynamics proved to be a promising and effective biometrics feature for authentication of individuals. It is necessary to stress that with the use of non-fixed text (various longer text parts) it is possible to effectively distinguish a vast majority of users with a relatively short keystrokes sequence. The proposed method improves the synergistic reinforcement of password mechanisms with rhythm click-based authentication on various devices perfectly. With this method, multiple level of security can be enforced to those systems where security is the major concern. In near future work will be extended for real time behavior using embedded system.

In future the customer's authentication is sound with their own biometric behavior, which is to be maintained. For any attacker it's not easy to adapt biometric behavior of particular individual, thus intensifying the level of reliability. The system can be practically installed in smart hand held devices without any intercession. The error probabilities can be reduced for improvised efficient working.

Acknowledgement

It gives us great pleasure in presenting a paper on `Graphical- based Password keystroke Authentication system for android phone'. We are really grateful to them for their kind support. Their valuable suggestions were very helpful. I am also grateful to Prof. Shalaka Deore, for guiding us through the work, Modern Education Society College of Engineering, Pune for her indispensable support, suggestions. In the end our special thanks to Other Professors for providing various resources.

References

[1] F. Monrose, M.K.R. "Graphical Password." //adrem.ua.ac.be/sites/adrem.ua.ac.be/files/chapter9-gp.pdf, (2011) July 19th.
[2] L. K. Seng, N. Ithnin and H. K. Mammi, "Identifying the Reusability of Triangle Scheme and Intersection Scheme on Mobile Device", International Journal of Computer and Information Science, vol. 4, no. 4, 2011.
[3] L. C. F. Araújo, L. H. R. Sucupira Jr., M. G. Lizárraga, L. L. Ling, and J. B. T. Yabu-Uti, User Authentication Through Typing Biometrics Features IEEE transactions on signal processing, vol. 53, no. 2, 2005.
[4] Partha Pratim Ray "Ray's Scheme: Graphical Password Based Hybrid Authentication System for Smart Hand Held Devices" Journal of Information Engineering and Applications, vol 2, no.2 2012.
[5] R. Biddle, S. Chiasson, and P. van Oorschot, Graphical Passwords:Learning from the First Twelve Years, to be published in ACM Computing Surveys, vol. 44, no. 4, 2012.
[6] Kailas I Patil, Jaiprakash Shimpi, A Graphical Password using Token, Biometric, Knowledge Based Authentication System for Mobile Devices, International Journal of Innovative Technology and Exploring Engineering (IJITEE) , vol.2, no.4, March 2013
[7] H. Saevanee, P. Bhatarakosol, User Authentication using Combination of Behavioral Biometrics over the Touchpad acting like Touch screen of Mobile Device, International Conference on Computer and Electrical Engineering, 2008 IEEE.
[8] F. Monrose and A. D. Rubin, Keystroke dynamics as a biometric for authentication, Future Generation Computer Systems, Volume 16, Issue 4, pp. 351-359, 2000.
[9] S. Chiasson, P. van Oorschot, and R. Biddle, Graphical Password Authentication Using Cued Click Points, Proc. European Symp. Research in Computer Security (ESORICS), pp. 359-374, Sept. 2007.
[10] Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, PassPoints: Design and Longitudinal Evaluation of a Graphical Password System, Intl J. Human Computer Studies, vol. 63, nos. 1/2, pp. 102-127, 2005.
[11] Campisi P., Maiorana E., Bosco M. L. and Neri A., "User authentication using keystroke dynamics for cellular phones," IET Signal Processing, Vol. 3, No. 4, pp. 333-341, 2009.
[12] S. B.Sahu, A.Singh, Secure User Authentication & Graphical Password using Cued Click-Points, IJCTT, Vol. 18 No. 4, Dec 2014.
[13] M. Kaur, R. S. Virk, Security System Based on User Authentication Using Keystroke Dynamics, International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 5, May 2013.
[14] M. Sreelatha, M. Shashi, M. Anirudh, M.D.S. Ahamer, V.M. Kumar, Authentication Schemes for Session Passwords using Color and Images, International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.3, May 2011.
[15] N. López, M. Rodríguez, C. Fellegi, D. Long, and T. Schwarz, Even or Odd: A Simple Graphical Authentication System, IEEE LATIN AMERICA TRANSACTIONS, VOL. 13, NO. 3, MARCH 2015
[16] Madhuri Shinde pursuing degree in Computer Engineering from Modern Education Society's College of Engineering, Pune, Maharashtra.
[17] Jasraj Mundada pursuing degree in Computer Engineering from Modern Education Society's College of Engineering, Pune, Maharashtra.
[18] Dipali Sutar pursuing degree in Computer Engineering from Modern Education Society's College of Engineering, Pune, Maharashtra.
[19] Shalaka P Deore has completed her Master of Engineering in Computer Science from Mumbai University. She is working as Assistant Professor at Modern Education Society's College of Engineering,

Pune. She has 9.5 years of experience in education field and has worked with reputed engineering institutes in Osmania University, Mumbai University and Pune University. Shalaka is member of IETE since 2010.

