IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

Graphical-Based Password Keystroke Dynamic Authentication System for Android Phone

Miss. Aarti Raman Sonawane [1], Prof. H. V. Kumbhar [2]

ICT Teacher, Kendriya Vidyalay No.1, Nasik, (Computer Engineering, PVPIT, Pune), India[1]

Assistant Professor, Computer Engineering, PVPIT, Pune, India[2]

Abstract: Most of the existing authentication system has certain drawbacks for that reason graphical passwords are most preferable authentication system where users click on images to authenticate themselves. An important usability goal of an authentication system is to support users for selecting the better password. User creates memorable password which is easy to guess by an attacker and strong system assigned passwords are difficult to memorize. So researchers of modern days gone through different alternative methods and conclude that graphical passwords are most preferable authentication system. The proposed system combines the existing cued click point technique with the persuasive feature to influence user choice, encouraging user to select more random click point which is difficult to guess.

Keywords: Reauthentication, usable security, Behavioural biometrics, graphical passwords, Smartphone.

I. INTRODUCTION

Keystroke Dynamics is behavioural biometric used to measure the typing rhythm of the user particularly for user authentication, when an individual types on the keyboard. It is assumed as a robust behavioural biometric. The functionality of this biometric is to measure the dwell time and flight time for changing keyboard actions.

The aim of this work is to provide 3 levels in terms of security for transaction in banking applications. First we are making use of encryption for sending user id and password on server from the user's mobile phone. Once the user is authenticated he will be shown with a graphical password screen. Secondly User is shown with sequence of images with 4x4 blocks; user has to select one block from each image. If user enters an incorrect click-point during login, the next image displayed will also be incorrect.

Legitimate users who see an unrecognized image know that they made an error with their previous click point. Conversely, this implicit feedback is not helpful to an attacker who does not know the expected sequence of images.

Third, We measure KDA (Keystroke Dynamic-based Authentication) for each images click. This project proposes a new graphical-based password KDA system for touch screen handheld mobile devices. The graphical password enlarges the password space size and promotes the KDA utility in touch screen handheld mobile devices. In addition, this paper explores a pressure feature, which is easy to use in touch screen handheld mobile devices, and applies it in the proposed system. This way we would improve security by using graphical authentication in mobile banking applications.

The most common approach to address this problem is the use of authentication mechanisms, e.g., PIN-based and pattern-based passcodes, which have been integrated into smartphone systems like Android and iOS. Unfortunately, most smartphone users tend to choose simple and weak passcodes for the sake of convenience and memorability, and some recent studies have shown how simple an attacker can derive the PIN passcodes from the oily residues left on the screen or the pattern passcodes from the shoulder surfing attack . An attacker could even infer the passcodes from the accelerometer and gyroscope readings. Therefore, it is highly desirable to enhance smartphone authentication with a passive and transparent authentication mechanism without active user involvement, to further detect whether the logged-in user is the true owner of a smartphone. An ongoing research project, the Active Authentication and Monitoring program initialized by DARPA (Defence Advanced Research Project Agency), aims to develop computational behavioural traits for validating the identity of the users in a meaningful and continual manner (without requiring the deployment of additional hardware sensors), through how users interact with the computing systems.

II. LITERATURE SURVEY

In paper [1], This work is the first to evaluate diverse types of touch-interaction behavior for active authentication across various application tasks and various application scenarios in smartphones. Experimental results show all types of touch operations exhibit considerable stability and discriminability among users for active smartphone authentication, and can achieve an EER around 1.8% in some cases. However, it is still less than ideal to reach the European standard for commercial biometric technology (FAR of 0.001% and FRR of 1% [1]). Thus, further progress is needed before we can depend solely on touch-interaction behavior as an authentication mechanism. One way to improve the

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

accuracy is to seek better representation of touch-interaction behavior, which is critical to accurately extract stable features. This study has shown promising performance using different types of touch operations for active smartphone authentication in some routine computing scenarios, but in more practice we are aware that such touch-behavior data may be affected by behavioral variability, in contrast with other physiological biometric characteristics, such as face or fingerprint patterns.

Real-world behavioral variability often comes from (1) hardware-level factors (e.g., smartphone type, touchscreen type); (2) software-level factors (e.g., operating system, screen resolution, sensitivity configuration, event sampling rate, perceptual delays caused by high CPU load); (3) environmental factors (e.g., distance between monitor and body, height of the chair, positions of the mouse pad); and (4) psychological and physiological state of the subject (e.g., the subject may be fatigued, distracted or distressed). Thus it is reasonable towonder whether these factors would change touch-behavior characteristics if the state of these factors is different at enrollment time than at authentication time, or even would have some impact on authentication performance. Given our results, it is hard to see which factors contribute more to the variability

In this paper [2], propose Safeguard, an efficient, transparent, and real-time reauthentication scheme for smartphones using the behavioral biometrics provided by sliding dynamics and the pressure intensity on touch screens. Our approach relies on angle and pressure-based metrics, and makes use of machine learning algorithms. By comprehensive experiments, we evaluate the system performance in terms of verification accuracy. The evaluation results demonstrate that the FAR and FRR are lower than 0.03% and 0.05%, respectively, in 10 to 20 sliding movements for reauthentication. We also show that the proposed system can effectively resist adversary imitation. Moreover, the system overhead in terms of storage and computation delay is very suitable to current smartphones. In practice, user's biometric metrics may vary with time. It means that the verification accuracy might degrade from time to time or with passage of time. To this end, we divide the biometric diversity under following two cases. 1) The biometric diversity parameters may vary particularly the threshold level. In resolution, we design and use a heuristic method to customize the threshold level for each distinct user. This solution is further assisted with other security mechanisms such as predefined security questions. 2) Our classifier should be able to deal with sudden and temporary changes in the sliding profile of a valid user. If the user's sliding pattern changes suddenly, e.g., due to unexpected accident such as a sprained finger, the difference in biometric metric can be too large to be recognized by the verification process.

In this paper [3], presented a novel approach of continuously validating the identity of a user in real time through the use of typing-based behavior biometrics. We investigated a number of methods to compute the similarity of two typing sequences. In particular, we proposed a novel BoMP approach to efficiently compute the high-order co-occurring phrases that are composed of words across both the temporal and feature spaces. We collected a multi-phase, multi-session, and multi-model (visual, audio, and keystroke timing) database of keyboard typing by 63 unique subjects. Through extensive experiments, we demonstrated excellent performance at operational points most relevant to authentication applications, as well as explained where and why BoMP improves upon the prior work. We also demonstrated superior performance over keystroke dynamics, with a much shorter probe sequence, which offers far less authentication delay.

Finally the success of our ultra-real-time demo system indicates again the promise of this novel biometric modality. As a novel exploration of TB, our approach focuses on the behavioral traits that can be observed through how an individual operates the keyboard. Similar to the fact that you leave a fingerprint when touching something with your finger, in behavior biometrics when you operate something you leave a pattern based on how your mind processes information, which is called a "cognitive fingerprint" by DARPA's Active Authentication program. Just like conventional fingerprints, the key challenge with cognitive fingerprints is whether the pattern is consistent within an individual and discriminative between individuals. Indeed typing behavior has demonstrated the potential to meet such challenge, with carefully designed data collection, extensive experiments, and a successful real-time demo system.

In this paper [4], The authors have tested a keystroke biometrics variant on a group of people 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.
Even more interesting is the use of a continuous user authentication whilst the user is performing normal interaction with the system, involving longer texts, alike what the authors experiments showed, a minimum of 200 keystrokes. Short user authentication consisting of several keystrokes seems to be too short for the practical use. It is also necessary to stress the advantages of keystroke dynamics: the possibility of using booming Internet as a natural transmission medium for the biometrics and no need for dedicated acquisition devices. That clearly shows the potential of keystroke biometrics for the authentication of individuals over the Internet.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

III. MOTIVATION AND PROBLEM STATEMENT

The underlying principle of Biometric-based user authentication focuses on "who you are" which differs from conventional user authentication approach that mainly relies on "what you have" or "what you know." Thus, a biometric-based approach is based on the inherent and unique characteristics of a human user being authenticated. Biometric-based reauthentication approaches have been widely studied for PCs [3]–[14]. However, we can find only few such implementations on smartphones, which are either limited by coarse accuracy or restrict application scenarios or gestures. Therefore, in this section, we focus on the state of the art on smartphones. We first present some smartphone applications that perform the one-time identification and reauthentication. We then highlight some applications that tend to abuse the smartphone resources to observe the user's biometric characteristics, which can be used for various purposes including the attacks.

A. Attacks With User Behaviours on Smartphone: Existing smartphones are equipped with sensors such as GPS, microphone, accelerometer, magnetic field, gravity, temperature, and gyroscope.

B. Behavioral Biometrics-Based Authentication on Smartphone.

1) One-Time Identification: This method enhances the security of sliding unlock pattern on smartphones by employing the intensity of pressure on touch screen.
2) Reauthentication: Some other approaches have been proposed [7]–[11] to exploit users' gestures as features for user classification. These approaches cannot provide highly accurate classification and suffer from drawbacks.

IV. PROPOSED SYSTEM

This research work focus on providing better security system by analysing the typing behaviour of individuals using keystroke dynamics.

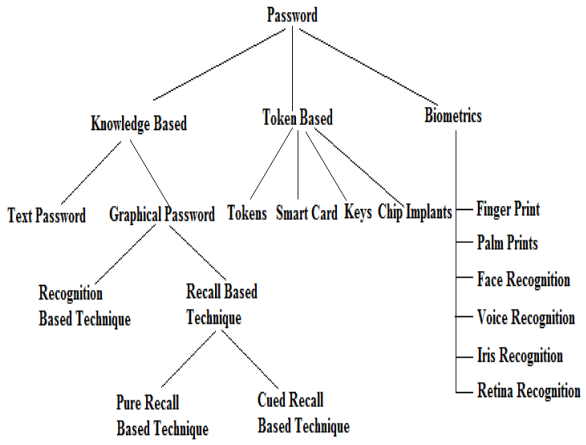

Fig: Classification of Password Authentication Methods

Main emphasis of this is to recognize typing behaviour of the users using FFNN with MLP to achieve more secure system. Keystroke Dynamics is becoming popular in real time security systems. The methods developed so far are less efficient than proposed technique. This paper deals with typing behaviour of individuals using MLP and it also validates the features of users using cross validation in order to give more secure and efficient system than previous system.

Product features are:

1. Encryption/decryption of data.
2. Graphical Authentication Using Cued Click- Points (CCP).
3. Measuring of KDA Parameters:

1. Down-Up (DU) time: DU time is the interval between the same click being pressed and being released.
2. Down-Down (DD) time: DD time is the interval between the click being pressed and the next click being pressed.
3. Up-Down (UD) time: UD time is the interval between the click being released and the next click being pressed.
4. Up-Up (UU) time: UU time is the interval between the click being released and the next click being released.
5. Down-Up2 (DU2) time: DU2 time is the interval between the click being pressed and the next click being released.

6. Authenticating User based on KDA parameter.
7. Internet Banking application Login, fund transfer and balance enquiry.

V. SYSTEM ARCHITECTURE

Keystroke dynamics or typing dynamics is the process of analyzing the way a user types at a terminal by monitoring the keyboard inputs thousands of times per second, and attempts to identify them based on habitual rhythm patterns in the way they type. It is the detailed timing information when each key was pressed and when it was released as a person is typing at a computer keyboard. The behavioral biometric of Keystroke Dynamics is the manner and rhythm in which an individual types characters on a keyboard or keypad. The keystroke rhythms of a user are measured to develop a unique biometric template of the users typing pattern for future authentication. Raw measurements available from every keyboard can be recorded to determine Dwell time (the time a key pressed) and Flight time (the time between "key up" and the next "key down"). Key hold time or dwell time is defined as the time for which each keystroke was pressed. The keystroke latency is the combination of the hold and flight times. In other words, the system verifies how a person types. Keystroke verification techniques can be categorized as either static or continuous.

Static verification system approaches study keystroke characteristics at a specific time. Continuous verification, on the other hand, examines the user's typing behavior throughout the interaction time.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

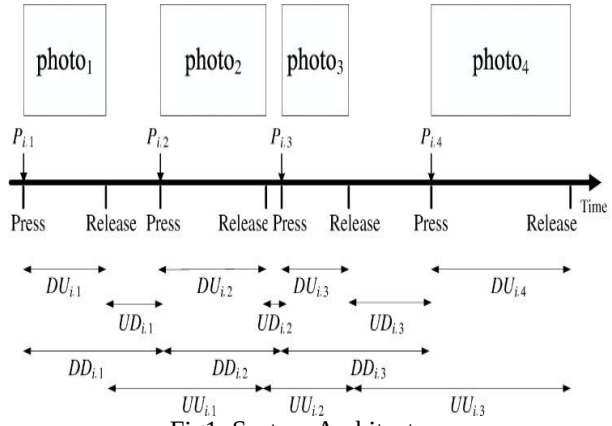

Fig1: System Architecture

Time-features can be extracted from keystroke data in many ways, such as studying keystroke latency, duration of key hold, pressure of keystroke, frequency of word errors, and typing rate. However, not all of these methods are widely used. Keystroke solutions are usually measured in three ways: dwell time – how long a key is pressed, flight time – how long it takes to move from one key to another, and key code. The recorded keystroke timing data is then processed through a unique neural algorithm, which determines a primary pattern for future comparison. Similarly, vibration information may be used to create a pattern for future use in both identification and authentication tasks. Data needed to analyze keystroke dynamics is obtained by keystroke logging.

VI. MATHEMATICAL MODEL

AES Algorithm:
AES is based on a design principle known as a substitution-permutation network, combination of both substitution and permutation, and is fast in both software and hardware.[10] Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. By contrast, the Rijndael specification per se is specified with block and key sizes that may be any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits.

AES operates on a 4 × 4 column-major order matrix of bytes, termed the state, although some versions of Rijndael have a larger block size and have additional columns in the state. Most AES calculations are done in a special finite field.
For instance, if there are 16 bytes, b0, b1, b2,……b15, these bytes are represented as this matrix:

$$\begin{bmatrix} b_0 & b_4 & b_8 & b_{12} \\ b_1 & b_5 & b_9 & b_{13} \\ b_2 & b_6 & b_{10} & b_{14} \\ b_3 & b_7 & b_{11} & b_{15} \end{bmatrix}$$

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 ciphertext. The number of cycles of repetition are as follows:

- 10 cycles of repetition for 128-bit keys.
- 12 cycles of repetition for 192-bit keys.
- 14 cycles of repetition for 256-bit keys.

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 ciphertext back into the original plaintext using the same encryption key.

VII. ALGORITHM

High-level description of the algorithm:
1. Key Expansions:- Round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.

2. Initial Round
1. Add Round Key:- Each byte of the state is combined with a block of the round key using bitwise xor.

3. Rounds
1. Sub Bytes:- A non-linear substitution step where each byte is replaced with another according to a lookup table.
2. Shift Rows:- A transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
3. Mix Columns:- A mixing operation which operates on the columns of the state, combining the four bytes in each column.

4. Add Round Key.
4. Final Round (no Mix Columns)
1. Sub Bytes
2. Shift Rows
3. Add Round Key.

VIII. FEATURES

1. Keystroke Dynamics Authentication (KDA).
2. Graphical Authentication Using CCP.
3. Internet banking application on android phone.

IX. CONCLUSION

For Graphical passwords there is a rising interest is that they are better than the Text based passwords, while the important argument for graphical passwords are that people are better at memorizing graphical passwords than text-based passwords. Also the proposed system removes the shoulder surfing attack. Also it removes the pattern formation and hotspot attack since it provides the system suggestion..

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

ACKNOWLEDGMENT

We take this golden opportunity to owe our deep sense of gratitude to our project guide **Prof. H. V. Kumbhar,** for her instinct help and valuable guidance with a lot of encouragement throughout this paper work, right from selection of topic work up to its completion. Our sincere thanks to Head of the Department of Computer Engineering **Dr. B, K. Sarkar** who continuously motivated and guided us for completion of this paper. I am also thankful to K. V. NO.1, Nasik staff members, for their valuable suggestions and valuable co-operation for partially completion of this work. We specially thank to those who helped us directly-indirectly in completion of this work successfully.

REFERENCES

[1] "Safeguard: User Reauthentication on Smartphones via Behavioral Biometrics", Li Lu, Member, IEEE, and Yongshuai Liu 2329-924X © 2016 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.

[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] F. Monrose, M.K.R. "Graphical Password." //adrem.ua.ac.be/ sites/adrem.ua.ac.be/files/chapter9-gp.pdf, (2011) July 19th.

[4] T. -Y. Chang, C. -J. Tsai and J. -H. Lin, "A Graphical-based Password keystroke Dynamic Authentication System for Touch Screen Handheld Mobile Devices", International Journal of Systems and Software, vol. 5, no. 85, (2012), pp. 1157-1165.

[5] C. J. T. T.Y. Chang and J. H. Lin, "A graphical-based password keystroke dynamic authentication system for touch screen handheld mobile devices, international journal of systems and software, vol.5, no. 85, (2012), pp. 1157-1165."

[6] C. F. D. L. F. M. I. N. Lpez, M. Rodrguez and T. Schwarz, "Even or odd: A simple graphical authentication system, ieee latin America transactions, vol. 13, no. 3, march 2015," 2015.

[7] R. S. V. Manpreet Kaur1, "Security system based on user authentication using keystroke dynamics," Feb. 2013.

[8] R. B. J. Ushir Kishori Narhar, "Highly secure authentication scheme 2015 international conference on computing communication control and automation."

[9] N. I. Lim Kah Seng and H. K. Mammi, "An anti-shoulder surfing mechanism and its memorability test international journal of security and its applications vol. 6, no. 4, october, 2012," 2012.

[10] R. Chippy.T, "Defenses against large scale online password guessing attacks by using persuasive click points international volume 03 no.3, issue: 01 march2012," 2012.

[11] User-Habit-Oriented Authentication Model: Toward Secure, User-Friendly Authentication for Mobile Devices jamie seto, ye wang, and xiaodong lin, (senior member, ieee) 2168-6750, 2014 IEEE. Translations and content mining are permitted for academic research only.

[12] Security System Based on User Authentication Using Keystroke Dynamics Manpreet Kaur, Rajinder Singh Virk Department of Computer Science and Engineering Guru Nanak Dev University, Amritsar (Punjab) India International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 5, May 2013.

[13] An approach for user authentication on non-keyboard devices using mouse click characteristics and statistical-based classification Cheng-Jung Tsai1;_, Ting-Yi Chang2, Yu-Ju Yang2 Meng-Sung Wu3 and Yu-Chiang Li4 International Journal of Innovative Computing, Information and Control Volume 8, Number 11, November 2012.

[14] Adding Persuasive features in Graphical Password to increase the capacity of KBAM Uma D. Yadav Computer Science & Engineering G. H. R. I. E. T. W. Nagpur, India Prakash S. Mohod Computer Science & Engineering 2013 IEEE International Conference on Emerging Trends in Computing, Communication and Nanotechnology (ICECCN 2013)