ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 11, March 2016

MOBILE USER AUTHENTICATION USING BEHAVIORAL HAND WAVING BIOMETRICS

Ms.R.Greena
PG Scholar, Dept of computer science
M. Kumarasamy College of Engineering, Karur
greenaraja666@gmail.com

Mr.U.Baveenther
Assistant Professor, Dept of Computer Science
M. Kumarasamy College of Engineering, Karur
baveentheru.cse@mkce.ac.in

***Abstract*—** Mobile devices, such as smart phones and tablets, offer a wide variety of important services to everyday users. Many of these services are highly sensitive and can be abused by malicious entities, without the knowledge of the device user, in the form of insider attacks (such as malware) and/or outsider attacks (such as unauthorized reading and relay attacks). In this paper, present a novel application authentication approach that can be used to protect mobile device from unauthorized access. It captures user's intent to access the service via a lightweight hand waving gesture. This gesture is very simple, quick and intuitive for the user, but would be very hard for the attacker to exhibit without user's knowledge. Then present the design and implementation of a hand waving gesture recognition mechanism using accelerometer and classify the patterns using neural network classifiers. We also report on experiments to analyze the performance of our approach both in benign and adversarial settings. This result indicates the approach to be quite effective in preventing the misuse of unlocking phones while imposing only minimal user burden.

Keywords— ***Adversary Settings, Behavioral biometrics, Classification, Gestures, Unlocking patterns.***

I. Introduction

Smart mobile devices have become essential tools in many people's daily lives. Not only are we using these devices as the means to communicate with others, as sources of entertainment and as ways of expressing ourselves, but we also use them to store sensitive personal information and access different online services. Despite all the information contained in a device and the transactions that can be performed with it, many users choose not to protect their devices and at the same time they tend to be perpetually logged into some of the services provided by mobile third party applications. Thus, an attack on the mobile device, or the loss of it, can have negative consequences such as the intrusion of privacy, the opportunity to impersonate users, and even severe financial loss. Currently, most of the solutions for authenticating users into their devices and other mobile services are based on the same solutions offered when using desktop computers, which usually involve the use of a PIN, a strong password, or some sort of extra external security token device. These techniques become cumbersome when applied to mobile devices and do not always provide a satisfactory user experience. Besides, they are not a sustainable approach for the future of mobile interactions, in which people would carry only one secure trustable device to perform most operations and would preferably use only one hand to operate such device.

A biometric-based re-authentication system involves an enrollment phase and a re-authentication phase. Behavioral biometrics assumes that people have distinct stable patterns on a certain behavior, such as waving patterns. Behavioral biometric-based re-authentication uses the behavior patterns to authenticate a user's identity. A user is enrolled by providing his hand waving patterns. The system learns patterns from the provided data and stores the learned patterns for future reference. During the re-authentication phase, the system compares the observed waving data against the stored data to re-authenticate a user.

II.RELATED WORK

A. Biometric-Rich Gestures: A Novel Approach to Authentication on Multi-Touch Devices:

[1] proposed a method based on multi-touch gestures and can be seen as an instance of a behavioral-biometric-based authentication technique. It is not susceptible to shoulder surfing or finger oil attacks and potentially provides significantly large entropy. The user performs the gesture with all five fingers at once, and biometrics is drawn from the hand's geometry as well as the dynamics of the gesture itself. Thus far, users have readily accepted multi-touch gestures in the interface, and much has been made of the accessibility of this mode of interaction to a broad user public.

B. Tapprints: your finger taps have fingerprints:

[2] found that sensor information from mobile devices specifically from the accelerometer and gyroscope can be adequate to infer the locations of touch-screen taps. Interpreted differently, a background process running on a mobile device may be able to silently monitor the accelerometer and gyroscope signals, and infer what the user is typing on the software keyboard.

C. Biometric gait authentication using accelerometer sensor

[3] implemented a system that contains identification mode, the system recognizes an individual by searching the enrolment samples of all users in the database for a match. The genuine attempt is a self verification attempt when a user's submitted sample is compared to his own enrolment sample in the database. The impostor attempt is a non self-verification attempt when user's verification sample is compared against another user's enrolment sample.

D. User evaluation of lightweight user authentication with a single tri-axis accelerometer:

[4] proposed a gesture-based authentication using uWave, a state-of-the art gesture recognition system based on a single tri-axis accelerometer and distinguish two different objectives of user authentication. For privacy-insensitive data, the objective of user authentication is to retrieve user-specific data instead of protecting them, e.g. personal profiles or personalized configurations on a TV remote shared by family members.

E. A Study on biometric authentication based on arm sweep action with acceleration sensor:

[5] implemented a system, just need to grasp and shake cellular phones. This advantage is especially important for cellular phones. This authentication is strong against injustice and right malicious imitation. It is well known that we can counterfeit fingerprint authentication or using someone's hair in DNA certification.

3 LOCKING PATTERNS IN ANDROID PHONES

In stock Android, every user has six different options to choose from lock screen, all of which offer their levels of security. If a user has a non-stock Android device like the Galaxy S3, then there are some differences in functionality but for the most part they all act in a similar fashion. First, to access the lock screen options, the universal location tends to be in Settings-Security. From there, one should see an option towards the top called "Screen lock," which then takes us to the lock screen options once tapped.

SLIDE TO UNLOCK

Slide is probably the most commonly used lock screen of all it's basically the default. This lock screen is not secure by any means, and only asks that the user of the phone grab the circle with a lock inside and slides it outside of a larger circle to unlock the phone. There are no passwords or patterns; it's simply a way to keep the phone from turning itself on and then accessing all sorts of info in the pocket or purse without your knowing. The nice thing about using Slide is that one can still access the notifications pull down without having to fully unlock the phone. None of the other lock screen options allow for this, as they are technically "secure"

FACE UNLOCK:

Face Unlock was introduced back in Ice Cream Sandwich as a fun way to unlock the phone using a face of the user. In order to set this option up, one has to place his face inside of a face shaped ring of dots using front facing camera until the device decides that the face is enough to be able to unlock with it. Once approved, a user will be asked to provide a backup option in case the device cannot recognize his face. The two backup options are PIN or pattern.

PIN PATTERN AND PASSWORD:

Pattern, PIN and Password unlocks are exactly as they sound. One should either create a pattern, a numeric PIN, or an alpha-numeric password that needs to be entered in order to unlock the phone. These are likely the most secure of them all. If a user forgets the pattern, PIN, or password, then he is not allowed to access the phone.

FINGERPRINT SCANNING

Fingerprint scanning technology is becoming increasingly important with everyday security measures and can provide an affordable, effective and reliable means of identification. Atrix smart phone, made by Motorola supplies a finger scanning system. Motorola Atrix 4G has a feature called Fingerprint Scanner. Overlapping processes on the screen and low speed are the main problems in this system.

3.5. CONTINUOUS TOUCH-BASED AUTHENTICATION

The main hypothesis of this study is that continuously recorded touch data from a touch screen is distinctive enough to serve as a behavioral biometric. The smart phone records times, finger pressures, and the screen areas covered by each finger. A continuous authentication application could run in the background and extract multiple features from all available raw input. This raw input is readily available through the phone's API. Based on various extracted features, the system can then learn a profile of the legitimate user and compare all screen interaction with this profile.

3.6 CIRCULAR SCREEN LOCK

The Lock Screen consists of six circles. Each circle changes its color maximum of seven times by retouching the circle. There is no specific order for touching the circles. Once retouching is done a password string is generated. This password string is then confirmed by clicking on ok button. If the string is matched then the phone is unlocked. The existing locking patterns are illustrated in fig 1.

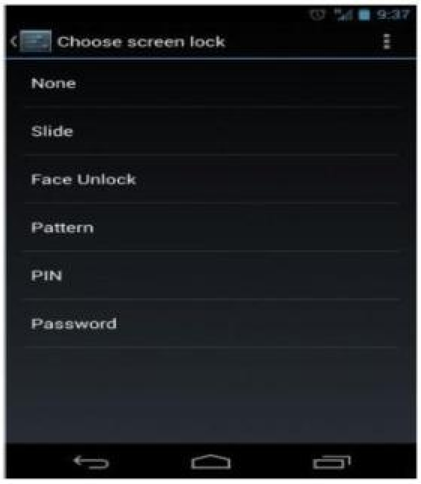

Fig 1. Existing locking patterns

4 PROPOSED SYSTEM

Smart phones are no longer the devices theater only used to call or text others. They become prevalent with much more powerful functions. Acting as pocket PCs, smart phones can be used to deal with complicated tasks such as sending/receiving e-mails, shopping, mobile payment, etc. Screen locker is a fundamental utility for smart phones to prevent the device from unauthorized use. For example, the Apple iPhones and Android phones can lock themselves automatically after being idle for a short time. It can protect the privacy of users as well as prevent unintentional operations. Classical screen lockers have been proposed long time back.

(1) The most widely used one is Slide-to-Unlock. The user can unlock his/her phone through sliding his finger across a defined trajectory. This method is too simple to protect user's privacy.

(2) PIN, the most common method used by traditional digital device, is always adopted on smart phones for unlocking smart phones. However, due to the relatively small screen and frequent unlocking request, it is inconvenient to set long and complex PIN on phones. For example, there are only four numbers allowed to be set as unlocking PIN in iPhones default setting. Such a short and simple PIN can often be easily guessed.

(3) The user can pre-define a graphical password, like connecting at least four circles shown in the screen. Being similar to the PIN, simple graphic passwords are easy to be peeked and guessed, while the complex pattern may confuse the user and make inconvenience. To enhance the security as well as the flexibility, many biometric authentication methods are introduced for screen lockers. The secrets of these methods cannot be easily spied and reproduced since they identify the user based on her natural features.

The biometric measures are grouped into two main categories: physiological biometrics and behavior biometrics. Physiological biometrics leverages the physiological features of human beings to identify the user, including recognitions of face, voice, fingerprint, ear, and so on. However, we find that

(i) performances of these solutions are heavily influenced external factors. For example, the face acquirement by the camera is severely affected by the illumination, resulting in the failure to identify user at night. Similarly, it is hard to distinguish the voice from the ambient interference in extremely noisy environments, like subway or restaurant. Any authentication method must be adapted to all kinds of conditions.

(ii) Unlocking operation is a very frequent operation, of which energy consumption should be carefully considered. It is well known that the camera is one of notorious energy killers in smart phones.

(iii) lack of required hardware on current mainstream smart phones, like fingerprint scanner. Christo Ananth et al. [6] proposed a system in which FASTRA downloads and data transfers can be carried over a high speed internet network. On enhancement of the algorithm, the new algorithm holds the key for many new frontiers to be explored in case of congestion control. The congestion control algorithm is currently running on Linux platform. The Windows platform is the widely used one. By proper Simulation applications, in Windows we can implement the same congestion control algorithm for Windows platform also. The Torrents application which we are currently using can achieve speeds similar to or better than ―Rapid share (premium user) application.

UNLOCKING PATTERNS USING HAND WAVING BIOMETRICS

A handshaking biometric-based approach, called OpenSesame is used to unlock the smart phone. For precisely characterizing user's shaking actions, selecting appropriate sensors is necessary. In this technique the 3-axis accelerometer is used for detecting the hand shaking motion. The accelerometer allows smart phones to detect the motion performed on them. The accelerometer in smart phones measures the acceleration of the phone relative to freefall. The accelerometer measures the acceleration of the phone in three different axes: X, Y, and Z. Based on these features, we propose a system with Open Sesame framework with neural network pattern classifiers. OpenSesame which consists of four components: sensing, filter, fetcher, classifier, and matcher.

Sensing: This component is straightforward used to record the user's hand waving action data.

Filter: In practice, we find that there always exist some silent periods when no waving or very low level sensing data is detected. For better feature extraction, we use filter component to wipe out the silent periods.

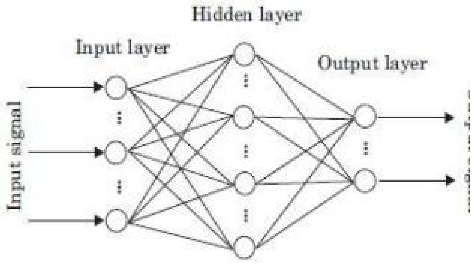

Fig 2. Waving pattern matching

Fetcher: The filtered raw tuples is fed into fetcher component in which four waving functions are applied to fetch the waving features.

Classifier: To discriminate the authorized users and unauthorized users, neural network classifier is employed in our system for classification.

Matcher: In the last component, the extracted feature is used to determine whether it matches the predefined one. The proposed framework is defined in fig 2.

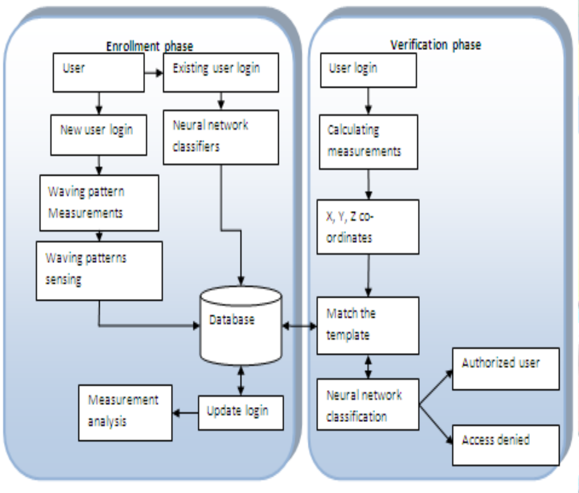

Fig 3. **System Architecture**

5 RESULTS AND DISCUSSION

We can analyze the proposed system using performance metrics such as sensitivity, specificity that contains true positive rate, false positive rate, true negative rate and false negative rate and these parameters are defined as follows:

- Sensitivity (also called the true positive rate or the recall in some fields) measures the proportion of positives that are correctly identified as such (e.g., the percentage of sick people who are correctly identified as having the condition).
- Specificity (also called the true negative rate) measures the proportion of negatives that are correctly identified as such (e.g., the percentage of healthy people who are correctly identified as not having the condition). Thus sensitivity quantifies the avoiding of false negatives, as specificity does for false positives.
- True positive rate (or sensitivity): TPR=TP/(TP+FN)
- False positive rate: FPR=FP/ (FP+TN)
- True negative rate (or specificity): TNR=TN/ (FP+TN)

Based on the above measurements, our proposed system provides increase TPR and reduces FPR and TNR. The proposed performance is analyzed in fig 3.

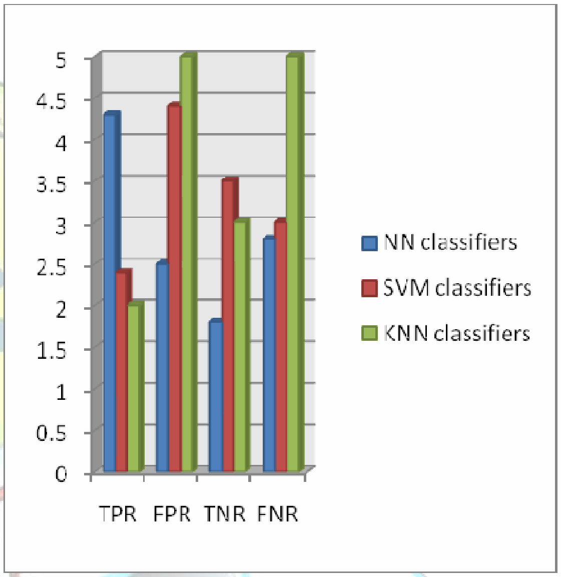

Fig 4. Performance evaluation

CONCLUSION

To prevent unauthorized usage of smart phones, a re-authentication system is more suitable than an authentication system. An authentication system authenticates a user for one time when he logs in, such as inputting a password to unlock a smart phone. The purpose of a re-authentication system is to continuously authenticate the current user during the whole system execution. In order to the system performs continuous re-authentication and does not need human assistance during re-authentication. We have discussed hand waving biometric feature design and selection for waving patterns. We have demonstrated the effectiveness and efficiency of our system in extensive experiments. In this project we propose a novel behavioral biometric-based authentication approach called OpenSesame for smart phone. We design four waving functions to fetch the unique pattern of user’s hand waving actions. By applying the neural network classifier, the smart phone can accurately verify the authorized user with the pattern of hand waving action.

REFERENCES

[1] N. Sae-Bae, K. Ahmed, K. Isbister, and N. Memon, “Biometric-rich gestures: A novel approach to authentication on multi-touch devices,” in Proc. SIGCHI Conf. Human Factors Comput. Syst., 2012, pp. 977–986.

[2] E. Miluzzo, A. Varshavsky, S. Balakrishnan, and R. R. Choudhury, “Tapprints: Your finger taps have fingerprints,” in Proc. 10th Int. Conf. Mobile Syst., Appl., Serv., 2012, pp. 323–336.

[3] D. Gafurov, K. Helkala, and T. Søndrol, “Biometric gait authentication using accelerometer sensor,” J. Comput., vol. 1, no. 7, pp. 51–59, 2006.

[4] J. Liu, L. Zhong, J. Wickramasuriya, and V. Vasudevan, “User evaluation of lightweight user authentication with a single tri-axis accelerometer,” in Proc. 11th Int. Conf. Human Comput. Interact. Mobile Devices Serv., 2009, p. 15.

[5] F. Okumura, A. Kubota, Y. Hatori, K. Matsuo, M. Hashimoto, and A. Koike, “A study on biometric authentication based on arm sweep action with acceleration sensor,” in Proc. IEEE Int. Symp. Intell. Signal Process. Commun., 2006, pp. 219–222.

[6] Christo Ananth, A. Ramalakshmi, S. Velammal,B. Rajalakshmi Chmizh, M. Esakki Deepana, “FASTRA –SAFE AND SECURE”, International Journal For Technological Research In Engineering (IJTRE), Volume 1, Issue 12, August-2014,pp: 1433-1438

[7] A. Jain, L. Hong, and Y. Kulkarni, “A multimodal biometric system using fingerprint, face and speech,” in Proc. 2nd Int. Conf. Audio Video-Based Biometric Person Authentication, 1999,
pp. 182–187.

[8] P. J. Phillips, A. Martin, C. L. Wilson, and M. Przybocki, “An introduction evaluating biometric systems,” Computer, vol. 33, no. 2, pp. 56–63, Feb. 2000.

[9] R. LiKamWa, B. Priyantha, M. Philipose, L. Zhong, and P. Bahl, “Energy characterization and optimization of image sensing toward continuous mobile vision,” in Proc. 11th Annu. Int. Conf. Mobile Syst., Appl., Serv., 2013, pp. 69–82.

[10] M. Conti, I. Zachia-Zlatea, and B. Crispo, “Mind how you answer me!: Transparently authenticating the user of a smartphone when answering or placing a call,” in Proc. 6th ACM Symp. Inf., Comput. Commun Security, 2011, pp. 249–259.