AUTHENTICATION AND UNCORKING SMART PHONES BY HAND-WAVE GESTURE

R.Pavithra,
B.E. Scholar,
Computer Science and Engineering,
Velammal Institute of Technology,
Chennai,India.

N.Sandhya,
B.E. Scholar,
Computer Science and Engineering,
Velammal Institute of Technology,
Chennai,India.

K.Balachander,
Assistant Professor,
Computer Science and Engineering,
Velammal Institute of Technology,
Chennai,India.

Abstract: Screen locking/unlocking is important for modern smart phones to avoid the unintentional operations and secure the personal stuff. Once the phone is locked, the user should take a specific action or provide some secret information to unlock the phone. The existing unlocking approaches can be categorized into four groups: motion, password, pattern, and fingerprint. Existing approaches do not support smart phones well due to the deficiency of security, high cost, and poor usability. We collect 200 users' hand-waving actions with their smart phones and discover an appealing observation: the waving pattern of a person is kind of unique, stable and distinguishable. In this paper, we propose OpenSesame, which employs the users' waving patterns for locking/unlocking. The key feature of our system lies in using four fine-grained and statistic features of hand-waving to verify users. Moreover, we utilize support vector machine (SVM) for accurate and fast classification. Our technique is robust compatible across different brands of smart phones, without the need of any specialized hardware. Results from comprehensive experiments show that the mean false positive rate of OpenSesame is around 15%, while the false negative rate is lower than 8%.

Keywords: Smart phone, Security, privacy, authentication, accelerometer.

I. INTRODUCTION

Smart phones are no longer the devices that are 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, Apple iPhones and Android phones can lock themselves automatically after being idle for 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 iPhone's default setting. Such a short and simple PIN can often be easily guessed [1], [2]. (3) The user can pre-define a graphical password, like connecting at least 4 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 leverage 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 influence 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 an 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 smartphones, like fingerprint scanner.

e-ISSN: 2395-5325

The behavior biometrics is the other classification of biometric measure, which identify the user based on their behavior features, such as gesture, typing behavior mouse movement tapping behavior or gait, However, these methods cannot either be adopted in smart phones or be suitable for unlocking smartphones. For example, in order to recognize the gait pattern, the user has to walk first or the smart phone to figure out whether he/she is valid. It appears odd and inconvenient for users to perform the behavior as answering a phone call for the purpose of checking his/her emails.

In this paper, we observe that different users wave their smart phones produce distinct features. For example, some persons used to wave their smart phones drastically while some others like to wave in a gentle way. This makes the waving speed and frequency totally different among users. Also, the waving range and the way of wrist twisting are also different from user to user. These patterns derive from user‟s physical features and habits. For example, the users with longer arms wave faster and wider than those with shorter arms. Some persons are accustomed to end their waving action with a wrist twisting while some others like to begin with a wrist twisting. Moreover, the gender, age, and occupation also greatly affect the feature of waving actions. On the other hand, we also observe that when a user waves his smart phone, he always shakes in a similar way. This is because, without intentional changes, a specific person tends to follow his habits once the habits are developed. Based on above observations, we propose a hand-waving biometric-based approach, called OpenSesame, to unlock the smart phone. Comparing with the existing methods, there are two major advantages of our approach. (i) It is difficult to forge. Using our approach, the authentication process is based on the features of the user's habits and motions.

II. RELATED WORK

A large scale study of password use and password re-use habits. The study involved half a million users over a three month period. A client component on users' machines recorded a variety of password strength, usage and frequency metrics. This allows us to measure or estimate such quantities as the average number of passwords and average number of accounts each user has, how many passwords she types per day, how often passwords are shared among sites, and how often they are forgotten. We get extremely detailed data on password strength, the types and lengths of passwords chosen, and how they vary by site. The data is the worst large scale study of its kind, and yields numerous other insights into the role the passwords play in users' online experience.

In current computing environments, collaborative computing has been a central concern in Ubiquitous, Convergent, and Social Computing. "MobiLife" and "MyLifeBits" are the leading projects for representing daily life services and their systems require complicate and collaborative network systems. The collaborative computing environments remain in high potential risks for users security and privacy because of diverse attack routes. In order to solve the problems, we design combined authentication and multilevel access control, which deals with cryptographic methods in a personal database of "MyLifeBits" system. We propose a scheme which is flexible in dynamic access authorization changes, secure against all the attacks from various routes, a minimum round of protocol, privacy preserving access control, and multifunctional.

Mobile phones are rapidly becoming small-size general purpose computers, so-called smartphones. However, applications and data stored on mobile phones are less protected from unauthorized access than on most desktop and mobile computers. This paper presents a survey on users' security needs, awareness and concerns in the context of mobile phones. It also evaluates acceptance and perceived protection of existing and novel authentication methods. The responses from 465 participants reveal that users are interested in increased security and data protection. The current protection by using PIN (Personal Identification Number) is perceived as neither adequate nor convenient in all cases. The sensitivity of data stored on the devices varies depending on the data type and the context of use, asking for the need for another level of protection. According to these findings, a two-level security model for mobile phones is proposed. The model provides differential data and service protection by utilizing existing capabilities of a mobile phone for authenticating users.

This study is a survey and classification of the state-of-the-art in behavioral biometrics which is based on skills, style, preference, knowledge, motor-skills or strategy used by people while accomplishing different everyday tasks such as driving an automobile, talking on the phone or using a computer. The authors examine current research in the field and analyze the types of features used to describe different types of behavior. After comparing accuracy rates for verification of users using different behavioral biometric approaches, researchers address privacy issues which arise or might arise in the future with the use of behavioral biometrics.

III. EXISTING SYSTEM

In the existing paper, the sensor is used for wave sensing, real trace collection and analysis on the data.

A.WAVING SENSING:

For precisely characterizing user's waving actions, selecting appropriate sensors is necessary. As the tremendous growth of MEMS technology, there are many powerful sensors equipped in our smart phone today, such as camera, microphone, proximity sensor, accelerometer, gyroscope, and magnetic sensor etc. In our system, the selected sensor should be able to depict the hand waving. In addition, it should be energy-efficient, stable, cheap, and compatible for wide deployment in most kinds of smart phones. Obviously, the first three sensors cannot capture the phone's motion. The gyroscope sensor is attractive because it is designed for measuring or maintaining purpose, based on the principles of angular momentum. Unfortunately, this kind of sensor is not a standard equipment in most smart phones due to its high price. The magnetic ensor is usually used for compass, but it tends to be interfered by the mental objects under special environment, like inside the car or subway.

B.DATA COLLECTION:

For investigating the uniqueness of hand waving, we collect the waving action data from 200 distinct smart phone users. For each specific user, he is asked to shake the smart phone for more than 10 seconds and repeat for three times. Note that there is no special restriction on user's waving actions. He can shake the smart phone arbitrarily in each trail .Indeed, we aim at taking insight into the hand-waving Action but not the motion pattern. The data is collected in two sampling modes: fast and normal modes. In the fast mode, the accelerometer samples every 10 to 20 milliseconds, corresponding to the acceleration value change rate. There are 100 users‟ traces collected using this mode. In the normal mode, the sampling interval is 200 milliseconds and 100 users‟ traces are sampled. Clearly, using normal sampling mode of accelerometer loses some data, but saves energy. We will compare these two modes in the evaluation section.

C.WAVING MEASUREMENT:

The For this purpose, we define the waving function to measure the global geometric properties of the waving shapes, which is formally given by: f=S(A) where, A={(xt0,yt0,zt0),(xt1,yt1,zt1),…(xtn, ytn, ztn)}. A is a set of raw waving tuples collected during t0 and tn. The waving function considers A as input and outputs a feature vector f. A good waving function should have the following properties: Efficiency. Since shape function will be performed in the smart phone, it should be simple enough to be fast and efficiently function. Invariance. In most time, the smart phone is working in mobile environments. The waving function should be insensitive to the position or direction change of smart phones.Robustness. Although the waving data generated by one person is similar, there always exist many noises and the sampling time is variable. Hence, the waving function should be robust to noise, blur, cracks, and dust in the waving.

IV. PROPOSED SYSTEM

This paper proposes a hand-waving biometric-based approach, called OpenSesame , to unlock the smart phone. Comparing with the existing methods, there are two major advantages of our approach. (1) It is difficult to forge. (2) It is the simplest and convenient. This approach can free users from remembering a large number of passwords or complicated patterns for unlocking their phones, preserved the security and All the user needs to do is just naturally wave the phone for 1 or 2 seconds.

A.SYSTEM OVERVIEW:

The figure below shows that the owner of the smartphone will first generate .apk file using eclipse. Then owner of the smartphone will install this .apk file in his smartphone. After installing this .apk file owner will proceed to set up the screen lock on his smartphone.

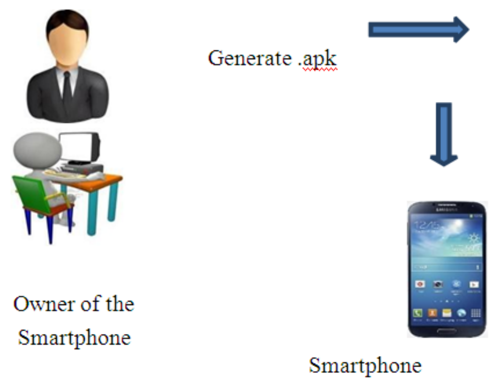

Figure 1: Pre-processing in smartphone

B. COMPONENTS:

OpenSesame consists of four components: sensing, filter, fetcher, classifier, and matcher. Sensing: This component is straightforward used to record the user's handwaving 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. Fetcher: The filtered raw tuples is feeded into fetcher component in which four waving functions are applied to fetch the waving features. Classifier: To discriminate the authorized users and unauthorized users, the support vector machine 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.

C. EXPERIMENT SETUP:

For investigating the uniqueness of handwaving, we collect the waving action data from 200 distinct smart phone users. The subjects producing these datasets are randomly selected in different public places, including railway station, university library, and stadtpark. When collecting the waving action data, three smart phones from different brands are used. For collecting each specific users handwaving data, he is asked to act with the following instruction: The user first randomly selects one of the three smart phones we provided, and holds this smart phone, which is running our data collection app, in his accustomed way. Then he pushes the button of „start‟ on the screen and begins to wave the smart phone until the hint sound is played by the smart phone. This waving process lasts for more than 10 seconds. The user repeats the above action for three times to terminatethe data collection. Note that there is no special restriction on users waving actions. He can wave the smart phone arbitrarily in each trail. Indeed, we aim at taking insight into the handshaking action but not the motion pattern.

V.CONCLUSION

In this paper, 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 handwaving actions. By applying the SVM classifier, the smart phone can accurately verify the authorized user with the pattern of handwaving action. Experiment results based on 200 distinct users' handwaving actions show that the OpenSesame reaches high level of security and robustness, and achieves good user's experience.

VI. REFERENCES

[1] D. Florencio and C. Herley, "A large-scale study of web password habits," in Proc. of ACM WWW, 2007.

[2] J. Bonneau, "The science of guessing: analyzing an anonymized corpus of 70 million passwords," in Proc. of IEEE Security and Privacy (SP), 2012.

[3] H.-A. Park, J. W. Hong, J. H. Park, J. Zhan, and D. H. Lee,"Combined authentication-based multilevel access control in mobile application for dailylifeservice," IEEE Transactions on Mobile Computing, 2010.

[4] N. Ben-Asher, N. Kirschnick, H. Sieger, J. Meyer, A. Ben-Oved, and S. M¨oller, "On the need for different security methods on mobile phones," in Proc. of ACM HCI, 2011.

[5] R. V. Yampolskiy and V. Govindaraju, "Behavioural biometrics: a survey and classification," International Journal of Biometrics, 2008.

[6] A. H. Akkermans, T. A. Kevenaar, and D. W. Schobben, "Acoustic ear recognition for person identification," in IEEE Workshop on Automatic Identification Advanced Technologies, 2005.

[7] A. Jain, L. Hong, and Y. Kulkarni, "A multimodal biometric system using fingerprint, face and speech," in Proc. of Audio-and Video-based Biometric Person Authentication, 1999.

[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, 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. of ACM MobiSys, 2013.

[10] N. Sae-Bae, K. Ahmed, K. Isbister, and N. Memon, "Biometric-rich gestures: a novel approach to authentication on multi-touch devices,"in Proc. of ACM CHI, 2012.

[11] 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. of ACM ASIACCS, 2011.

[12] F. Monrose, M. K. Reiter, and S. Wetzel, "Password hardening based on keystroke dynamics," International Journal of Information Security, 2002.