Protect Girls-Beast Car: User Behavior Pattern Analysis For Girls Protective Mechanism With Emergency Communication And Unlocking System

K.M.Sangeetha[1], M.Rekha[2]
Department of Computer Science and Engineering
[1, 2]Indira Institute of Engineering and Technology, Pandur, Thiruvallur

Abstract*-The increasing use of touchscreen smartphones to access sensitive and privacy data has given rise to the need of secure and usable authentication technique. Smartphone users have their own unique behavioral characteristics when perform-ing touch operations. These personal characteristics are reflected on different rhythm, strength, and angle preferences of touch-interaction behavior. This paper investigates the reliability and applicability on the usage of users' touch-interaction behavior for active authentication on smartphones. For each common type of touch operations, both static and dynamic features are extracted and analyzed for fine-grained characterization of users' touch behavior. Classification techniques (nearest neighbor, neural network, support vector machine, and random forest) are applied to the feature space for performing the task of active authentication. Analyses are conducted using data from around 134 900 touch operations of 71 participants in real-world scenarios, and the authentication performance is evaluated across various types of touch operations, varying operation lengths, different application tasks, and different application scenarios. The extensive experimental results are included to show that touch-interaction behavior exhibits sufficient discriminability and stability among smartphone users for active authentication, and achieves equal-error rates between 1.72% and 9.01% for different types of touch operations with the operation length of 11; the authentication accuracies improve when having long observation or small timespan between the training and testing phases, and express more reliably and stably in a specific task than in the free task. We also discuss a number of avenues for additional research that we believe are necessary to advance the state-of-the-art in this area.*

Keywords-Biometrics, touch interaction, active authentication, performance evaluation.

I. INTRODUCTION

SMARTPHONES have become omnipresent platforms ofpersonal computing for users to access the Internetand online services at anytime and anywhere. As moreand more privacy information and security information especially with the consideration that the smartphones are much easier to get lost or stolen in comparison with conven-tional computing platforms, according to a recent survey on US state of Cybercrime [1]. The most common approach to address this problem is the use of authentication mechanisms,

Unfortunately, most smartphone users tend to choose simple and weak passcodes for the sake of convenience and memorability [2], and some recent studies have shown how simple an attacker can derive the PIN passcodes from the oily residues left on the screen [3] or the pattern passcodes from the shoulder surfing attack [4]. An attacker could even infer the passcodes from the accelerometer and gyroscope readings [5], [6]. 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 [7] initialized by DARPA (Defense Advanced Research Project Agency), aims to develop computational behavioral traits for validating the identity of the users in a meaningful and continual manner through how users interact with the computing systems. Of various potential solutions to this problem, a particularly promising technique is the use of touch-interaction behavior. Compared with other biometric features on smartphones such as face and fingerprint, touch-interaction behavior does not require specialized sensors to collect data, and the detec-tion process can be integrated seamlessly into users' routine computing activities. Thus it can provide a non-intrusive and implicit solution for active authentication after entry-point based authentication by PIN-based or pattern-based passcodes, or could even substitute entry-point based authentication when reaching an acceptable level of performance.

Although there is a growing body of literature about touch-interaction behavior for entry-point based authentication, there is little work on the use of this behavior for active smartphone authentication. The major reasons may be the lack of in-depth analysis for various types of touch operations in terms of stability, discriminability, and usability for active authentication, and examination for its applicability across different application tasks and different application scenarios. Others might be the difficulty of extracting effective features or building reliable models from touch-interaction behavior. Of various potential solutions to this problem, a particularly promising technique is the use of touch-interaction behavior. Compared with other biometric features on smartphones such as face and fingerprint, touch-interaction behavior does not require specialized sensors to collect data, and the detection process can be integrated seamlessly into users' routine computing activities.

Firstly, we lay empirical work of relying ontouch-interaction behavior for active authentication on smartphones. We systematically investigate the reliability and applicability of continuously authenticating a user based on her touch- interaction behavior with a smart phone across different application tasks and scenarios, without dedicated and explicit actions that require attention from users.

Secondly, we propose a set of touch-behavior features by characterizing the touch operations based on various oper-ation properties, and make a systematic exploration on the discriminability and stability of the features across different touch types. Additionally, by ensuring the diversity in a set of classifiers to compare active authentication performances, we examine whether an observed effect is specific to one type of classifier or holds for a range of classifiers.

Thirdly, we present a repeatable and objective evaluation procedure to investigate the effectiveness of touch-interaction behavior for active authentication through a series of experiments. As far as we know, no earlier work made informed comparison between different touch types and application tasks, probably due to the lack of a standard test protocol. Here we provide comparative experiments to examine the validity of touch-interaction behavior for active authentication among various touch types, at varying operation lengths, and across different application tasks and different application scenarios.

Consequently, to our knowledge, this study is the firstto systematically evaluate diverse types of touch-interaction behavior for active authentication on smartphones across different application tasks and different application scenarios. Our results indicated that various types of touch operations exhibit sufficient discriminability and stability among users, and can lead to a better authentication performance when hav-ing long observation or small timespan between the training and testing phases, and express more reliably and stably in a specific task than in the free task. We also discuss a number of avenues for additional research that we believe are necessary to advance the state of the art in this area.

II. BACKGROUND AND RELATED WORK

A. Background of Touch-Interaction Behavior Analysis

Touch-interaction behavior, as a behavioral biometric for analysing behavior data from touching devices (e.g., touch-screen or touchpad), provides user authentication in an accessible and convenient manner [8], [9].

B. Active Authentication Based on Touch Behavior

Among the investigations of user authentication on smart phone through touch-interaction behavior, there are really two tasks of interest. The main strength of touch-interaction behavior is its ability to be constantly recorded and to monitor users' sessional usage without explicit attention from the users, thus to perform a nonintrusive active authentication. To our knowledge, few papers have targeted the use of touch-interaction behavior for active authentication on smartphones, which will be the central concern of this paper. Frank et al. [8] investigated the possibility of using touch behavior for continuous authentication on smartphones. They developed an application to capture simple touch movements in background, and extracted a set of 30 features from each stroke to characterize users' profiles. K-nearest neighbor (KNN) and support vector machine (SVM) were employed to perform the authentication tasks. Based on the data collected from 41 subjects, they achieved equal-error rates of approximately 13% with a single stroke (corresponding to an authentication time of 3.9 seconds), and the equal-error rates converged to a range between 2% and 3% with 11 to 12 strokes .These promising results suggest touch-behavior-based authentication could reach a practically useful level under laboratory conditions, but the reliability and applicability of this biometric in real-world scenarios need to be addressed for putting it into more practice.

These efforts confirm that touch-interaction behavior has a rich potential for active authentication on smartphones. But as compared with other biometric features such as face and fingerprints, touch-interaction behavior is less diagnostic. This study, differing from existing work, (1) focus on studying touch-sliding behaviors exclusively, and aim to provide in-depth analysis of each types of touch-sliding operations in terms of discriminability, stability, and applicability for active authentication in practice; (2) evaluated the authentication performance at varying operation lengths, across different application tasks, and under different application scenarios;(3) examined a set of classifiers to compare active authentication performance to explore whether an observed effect is specific to one type of classifier or holds for a range of classifiers.

III. TOUCH-INTERACTION BEHAVIOR ANALYSIS

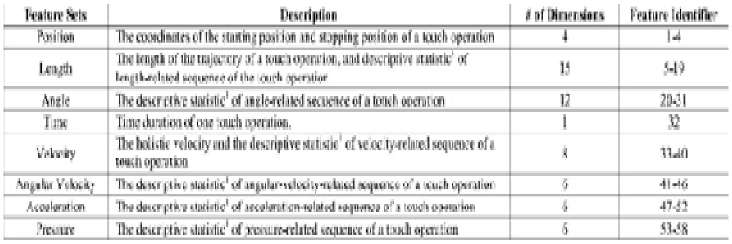
Touch-Interaction Operation

Touch-interaction behavior mainly consists of sliding operation and tapping operation, and the sliding operation is commonly divided into single-sliding and multi-sliding operations [13], [16]. Previous work has shown that in the continuous manner, tapping operations may contain less identity information than sliding operations for discriminating users [20]. Due to the simplicity and universality of these types of touch operations, users develop particular operational habits, which are based on different rhythm, strength, and angle preferences of their touch behavior.

Feature Extraction

Generally, not every touch operation is valid for feature extraction, because users cannot always avoid exceptional operations Preliminary observation on our raw data showed that there mainly exist two types of exceptional operations: very short sliding operation and back-and-fourth sliding operation.

In this study, one touch operation is a touch trajectory that is encoded as a sequence of touch points s_i=(x_i ,y_i , t_i , p_i , a_i), $i\in\{1,2, . . . , n\}$, with the location coordinates x_i,y_i, the timestamp t_i , the pressure on screen p_i , and the App name in which the event occurred a_i



Feature Sets	Description	# of Dimensions	Feature Identifier
Position	The coordinates of the starting position and stopping position of a touch operation	4	1-4
Length	The length of the trajectory of a touch operation, and descriptive statistic[1] of length-related sequence of the touch operation	15	5-19
Angle	The descriptive statistic[1] of angle-related sequence of a touch operation	12	20-31
Time	Time duration of one touch operation.	1	32
Velocity	The holistic velocity and the descriptive statistic[1] of velocity-related sequence of a touch operation	8	33-40
Angular Velocity	The descriptive statistic[1] of angular-velocity-related sequence of a touch operation	6	41-46
Acceleration	The descriptive statistic[1] of acceleration-related sequence of a touch operation	6	47-52
Pressure	The descriptive statistic[1] of pressure-related sequence of a touch operation	6	53-58

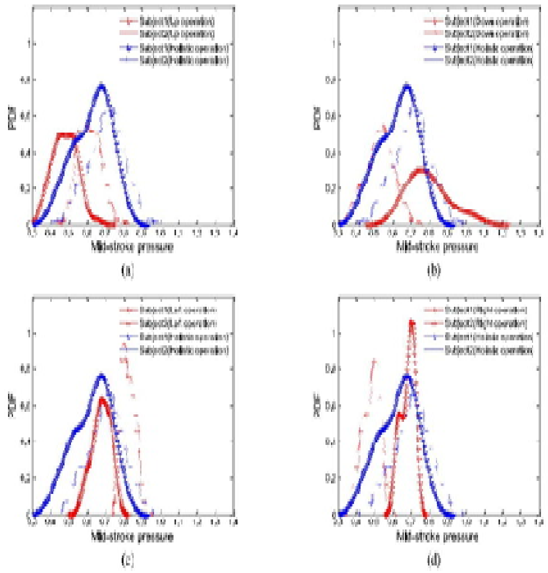


Fig. 1. Touch features extracted from each touch type and holistic operations. Panel (a), (b), (c), (d) show probability distribution function (PDF) curves of a typical touch feature used for two different subject

Figure 1 presents the comparison of some typical features for two different subjects across different touch types. We observe that the PDF curves of the features extracted from a single type of touch operations exhibit much more compact and concentrated than those from holistic touch operations, which indicates that the characteristics in a single type of touch operations may allow one to more accurately characterize touch behavior.. Additionally, we find that the PDF curves of “Left” and “Right” operations have smaller ranges compared with other two types. The reason might be that “Left” and “Right”operations have relatively-smaller active areas, and thus are easy to form stable behavior characteristics. Similar results can be observed for other subjects.

The Discriminability of Features Across Touch OperationsAnother essential trait of touch features is their discriminability, which is crucial in distinguishing users from one to another. Not only should the same subject have relatively stable features in her touch operations, but also different subjects should have distinct featuresAs Figure 1 shows, the PDF curves of features from holistic touch operations overlap each other in a relatively large region for two different subjects, which make it difficult to discriminate among subjects. Additionally, the PDF curves of “Left” and “Right” operations for two different subjects distinguish from each other obviously, which make it easier for a classifier to make a differentiation based on the features from those operations. Together with the stability of touch features discussed above, these results indicate different types of touch operations exhibiting inconsistent stability and discriminability for a same subject, and also make the features extracted from a single type of touch operations superior to those extracted from holistic touch operations. Note that for easy presentation, we only compare the difference between a pair of subjects. However, a similar observation holds for other subjects

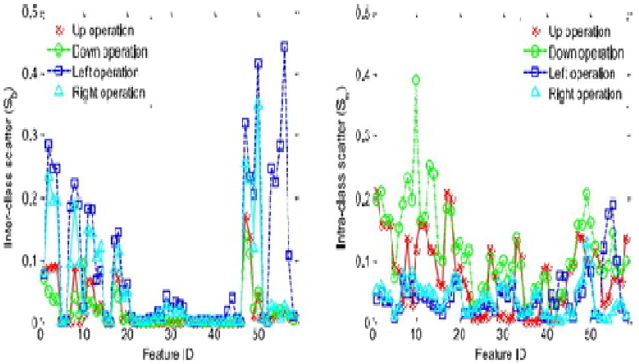


Fig. 2. The inter-class and intra-class scatter metrics of all the features extracted from each type of touch operations. The x-axis represents the identifier of the features defined in Table

Feature Selection for Different Types of Touch Operations

It is usually undesirable to use all components in the feature vector as input for a classifier, because some of data will not provide a significant degree of uniqueness or consistency

$$S_b(f_k)= \qquad P(i)(m^k_i - m^k)(m^k_i - m^k)^T,$$

$i=1$

$$P(i) \qquad {}_{x_i^k \in c_i} \qquad \frac{1}{n_i}(x_i^k - m_i^k)(x_i^k - m_i^k)^T.$$

For each feature, the measurement of Sb is zero if the feature has no discriminative power among users, and increases as the discriminability of the feature becomes better; the measure-ment of Sw is zero if the feature appears quite good stability for an individual users and increases as the stability of the feature becomes worse.Figure 2 presents inter-class and intra-class scatter metrics of all the features extracted from each type of touch operations. It is clear to see that both the inter-class and intra-class scatter values of the features exhibit obvious difference across different types of touch operations. This implied that the discriminability and stability of a feature may be different from one type of touch operations to another type of touch operations, and it may be better to select different features for different types of touch operations. Thus for each type of touch operations, the features were ranked in order of inter-class scatter values (in descending order) and intra-class scatter values (in ascending order). For the sake of providing the fea-tures to represent touch behavior in a low-dimensional space and for memory efficiency, the features which appeared in both top 40 results of the inter-class and intra-class scatter metrics were selected as the classifier input. Overall, we selected 22 features for “Up operations”, 22 features were selected for “Down operations”, 27 features for “Left operations”, and 24 features for “Right operations”. Table II summarizes the selected features for each

IV. CLASSIFIER IMPLEMENTATION AND EVALUATION

A. Classifier Implementation

User authentication is a challenging task from the pattern-classification perspective. In this evaluation, we considered the authentication task as a two-class classification problem (legitimate user vs. impostors), in which the classifiers are employed to analyze touch-behavior data and discriminate between a legitimate user and impostors.

The classifiers were implemented using the Matlabstatistical programming platform (version 7.13.0.564) [24]. Each classifier has a training phase where a set of feature vectors from training data is used to build a model of the user’s touch behavior, and a test phase where each new test vector is assigned a classification score.

Because some classifiers have certain parameters that may influence their performance, the issue of parameter tuning appears. Since there is no generally accepted method for tuning the parameters of classifiers on a data set without bringing bias to evaluation results, we tuned the parameters in order to result in the best performance of the classifiers, and illustrated what parameters we used.

1) K-Nearest-Neighbors: A K-Nearest-Neighbor classifier models a user’s touch-behavior data based on the assump-tion that new touch-behavior samples from the user will be similar to one or more of those in the training data [25]. During the

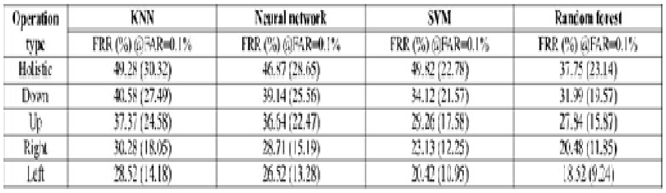
training stage, the classifier computed the covariance matrix of training feature samples, and chose the nearest-neighbor parameter k as 11, after multiple testswith k ranging from 2 to 20. During the testing stage, the classifier identified k training feature samples that are closest to the test sample and calculate the distance to these k points using Euclidean distance. The average distance from the new sample to the nearest samples was used as the classification score.

2) Support Vector Machine: Support vector machine (SVM) generalizes the ideas of finding an optimal hyper-plane in a high-dimensional space to perform a binary classifica-tion [26]. During the training stage, a SVM model was built on the training samples with a radial basis function (RBF) kernel, after comparative studies of linear, polynomial, RBF, and sigmoid kernels based on classification accuracy. The SVM parameter and kernel parameter were set to 0.03 and 0.006 respectively. During the testing stage, the testing samples were projected onto the same high-dimensional space, and the distance between the samples and the hyper-plane was computed as the classification score.

3) Backward-Propagation Neural Network:

Backwardpropagation neural network (BPNN) is a prevalent classification method of identifying patterns [25]. Here we used a double-hidden-layer network. During the training stage, we built the model with m input nodes, (2m + 1) first-hidden-layer nodes, 3 second-hidden-layer nodes, and 1 output node, where m is the number of the elements in the feature vector. The learning rate was set to 0.001. During the testing stage, testing samples were run through the network, and output of the network was recorded as the classification score.

TABLE V
Frrs For Four Types Of Touch Operations And Holistic Operations At Operation Length Of 11 (With Standard Deviation In Parentheses)



Operation type	KNN	Neural network	SVM	Random forest
	FRR (%) @FAR=0.1%	FRR (%) @FAR=0.1%	FRR (%) @FAR=0.1%	FRR (%) @FAR=0.1%
Holistic	49.28 (30.32)	46.87 (28.65)	49.82 (22.78)	37.75 (23.14)
Down	40.58 (27.49)	39.14 (25.56)	34.12 (21.57)	31.99 (19.57)
Up	37.37 (24.58)	36.54 (22.47)	29.26 (17.58)	27.94 (15.87)
Right	30.28 (18.05)	28.71 (15.19)	23.13 (12.25)	20.48 (11.85)
Left	28.52 (14.18)	26.52 (13.28)	20.42 (10.95)	18.52 (9.24)

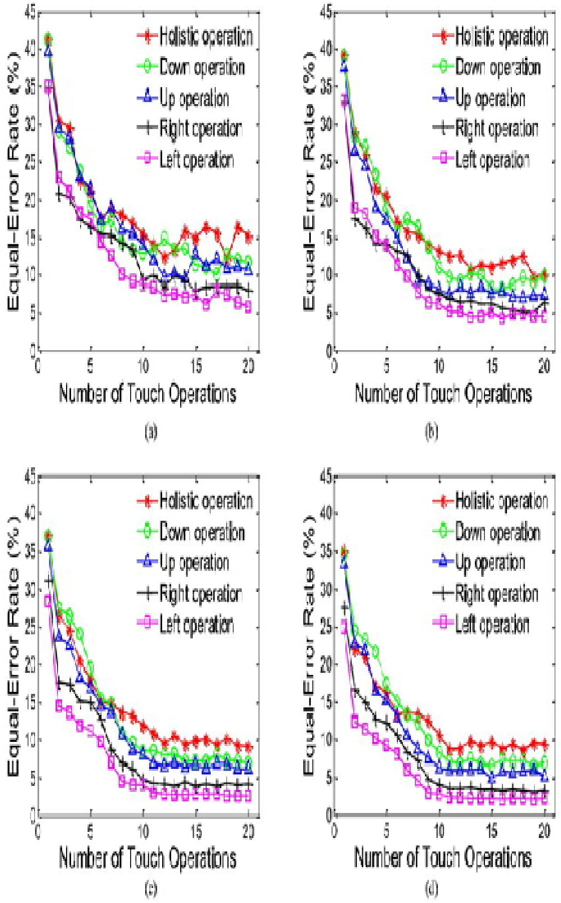


Fig. 3. EER curves for four types of touch operations and holistic operations at varying operating length, using four types of classifiers: (a) nearest neighbor, (b) neural network, (c) SVM, and (d) random forest. X-axis represents the number of touch operations that are used to verify a user's identity.

bootstrapping of data and random feature selection, may be also responsible for the performance boost.

b) Effect of operation length: When deciding with a single touch operation only, the EERs across various types of touch operations are relatively high (the best EER is approximately 25%), but the authentication decision only needs 0.77 seconds (on average). All the classifiers obtain smaller error rates when increasing the number of operations used to make an authentication decision. As the operation length increases to 5, the best EER drops to 8.87%, and the cor-responding time increase to 6.11 seconds. Therefore, this introduces a tradeoff between the authentication accuracy and the time required to make the authentication decision, and this time has a direct effect on the security since it says how long an attacker can interact with the devices. Also itshould be noted that all the EERs converges at a level of 10 to 11 operations which corresponds to an average time of 13.27 seconds for each decision, and stays there (with only small fluctuations) up to using 20 operations.

The results also show the same trend for all types of touch operations – that authentication accuracies will get better with an increase of operation length. Moreover, the performance of "Left" operations at varying operation lengths is better than those of "Right", "Up", and "Down" operations. This further indicates touch-interaction operations that occurred frequently and within a small active area could lead to more accurate and stable characterization of users' identity information.

c) Effect of feature selection: One may also wonder how much of the performance improvement is due to the use of our feature selection method. We employed random forest

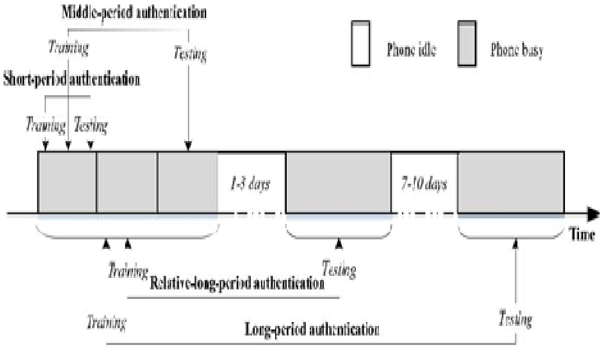

Middle-period authentication
Training
Testing
Short-period authentication
Training
Testing
Phone idle
Phone busy
1-3 days
7-10 days
Time
Training
Relative-long-period authentication
Testing
Training
Long-period authentication
Testing

Fig. 6.

Schematic diagram for our four authentication scenariosround of data collection, and chose the first quarter of the data as training data, and treated the second quarter of the data as testing data. The size of training data for each subject is around 160 touch operations (mean = 162, median = 151, min = 102, max = 183, s.d. = 31.3), in which the average proportions for different touch types are 31% for sliding up, 26% for sliding left, 24% for sliding down, and 19% for sliding right.

Middle-period authentication scenario:

In this sce-nario, a user operates the smartphone in routine usage for a while, and then puts the smartphone down. The smartphone starts to learn the user's touch behavior and build the clas-sification model. After a few minutes, the user picks up the smartphone, and the smartphone turns to detection mode of verifying the user's identity. This scenario allows users to use the phone for a longer time without locking or unlocking screen, and the usability would be increased. To explore the authentication performance of this scenario, we separated the data from first round of data collection into three parts evenly, and selected the first part as training data, and set the third part as testing data. The size of training data for each subject is around 210 touch operations (mean = 216, median = 203, min = 171, max = 265, s.d. = 48.2), in which the average proportions for different touch types are 30% for sliding up, 26% for sliding left, 24% for sliding down, and 20% for sliding right.

Relative-long-period authentication scenario

In this scenario, a user's profile and model are built on the observation of touch operations for a relatively long period of time (about 40 minutes in our evaluation). The model stays the same for a relative-long time up to few days, and then detects the legitimacy of users. For examining the authentication performance in this setting, we trained the classifier on the data that were recorded from first round of data collection, and test it on the data from second round of data collec-tion (in which the data are captured few days (1-3 days) later). The size of training data for each subject is around 640 touch operations (mean = 667, median = 627, min = 568, max = 693, s.d. = 122.5), in which the average proportions for different touch types are 29% for sliding up, 27% for sliding left, 24% for sliding down, and 20% for sliding right.

Long-period authentication scenario: In this sce-nario, we used the same methodology and training data in the relative-long-period authentication scenario to build the authentication model. The model stays the same for a longer time up to several days (8-13 days), and then detects the identity of users. We trained the classifier on the data that were recorded from first round of data collection, and test it on the data from third round of data collection (in which the data are captured several days (8-13 days) after first round).

We employed random forest classifier to conduct active authentication experiments with different timespans between enrollment and authentication in the free task, and specified the operation length of 11, to explore the performance of touch behavior across various application scenarios.

Results and Analysis: Figure 7 and Table VIII show the ROC curves and average FARs and FRRs across various application scenarios. Each panel displays the curves for each type of touch-interaction operations at the same scale.

The reason might be the fact that there has a longer observation of touch-interaction behavior in the training phase of middle-period scenario, leading to establishment of more stable and accurate user profiles. The FRRs in the relative-long-period and long-period scenarios are 3.97% and 7.56% respectively when the FARs remain to be 3%, which are worse than that in the short-period scenario. The similar results are observed for the standard deviations of these error rates. We conjecture these may be due to larger timespan between training and testing phases in the relative-long-period and long-period scenarios, which could introduce long period of behavior variability.

“Left” operation has lower error rates than other types of touch operations in every application scenario. This is another proof that touch operations occurred in a small active area can result in better authentication accuracy. “Left” operation also has the smallest standard deviation of error rates across different application scenarios, which indicates that the “Left” operation could produce more stable characteristics for touch behavior than other touch types. Besides, “Down” operation

V.DISCUSSION AND CONCLUSION

This work is the first to evaluate diverse types of touch-interaction behavior for active authentication across vari-ous 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% [31]). Thus, further progress is needed before we can depend solely on touch-interaction behavior as an authentication mechanism. Separately modeling different types of touch-interaction behavior and assembling them for authentication decision deserve more attention in future work.

We compared four typical types of touch operations to examine effectiveness of each touch type for active authentication on smart phones. The operations that occurred frequently and within a relatively small active area could produce more reliable and stable features, and thus lead to better authentication performance. Additionally, the operations produced by quick finger movements, which means less control information in the movements, would exhibit relatively large variability in the feature space. These would enable the research community gain insight into what characteristics of touch-interaction behavior can improve the performance, and identifying promising directions for further improvements of touch-interaction behavior for active authentication. Besides, by enriching the environment to include all kinds of touch operations (e.g., multi-touch operations), more information will be available as input to a detection module.

We analyzed the effect of touch-operation length on active authentication performance. Our results showed that authentication accuracies become better as the operation length increases. The error rates converge at the operation length around 11, corresponding to a detection time of around 13 seconds, and only small fluctuations within the accuracy range are apparent as the operation length increases even further. However, such detection time may limit the applicability in some real-world scenarios, thus a balance need to be made between authentication accuracy and authentication time. One possible way of improving this situation is to employ some newly developed tactics from “streaming classification” algorithms [34], [35], by which we may be able to use less data to make authentication decisions with acceptable levels of accuracy.

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. 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; (3) environmental factors (e.g., distance between monitor and body, height of the chair); and (4) psychological and physiological state of the subject

ACKNOWLEDGEMENT

The authors are grateful to T. Liu for his insightful comments and to Y. Song, X. Zuo, and Z. Yang for running the data collection. They would also like to thank several anonymous reviewers for their helpful comments.

REFERENCES

[1] PwC, CSO Magazine, The CERT Division of the Software Engineering Institute at Carnegie Mellon University, and The U.S. Secret Service. (May 2014). 2014 US State of Cybercrime Survey. [Online]. Available: http://www.pwc.com/us/en/increasing-it-effectiveness/ publications/2014-us-state-of-cybercrime.html

[2] J. Bonneau, “The science of guessing: Analyzing an anonymized corpus of 70 million passwords,” in Proc. IEEE Symp. Secur. Privacy, May 2012, pp. 538–552.

[3] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, “Smudge attacks on smartphone touch screens,” in Proc. 4th USENIX Conf. Offensive Technol., Washington, DC, USA, 2010, pp. 1–7.

[4] N. H. Zakaria, D. Griffiths, S. Brostoff, and J. Yan, “Shoulder surfing defence for recall-based graphical passwords,” in Proc. 7th Symp. Usable Privacy Secur., Pittsburgh, PA, USA, 2011, pp. 1–12.

[5] Z. Xu, K. Bai, and S.Zhu, “TapLogger: Inferring user inputson smartphone touchscreens using on-board motion sensors,” inProc. 5th ACMConf. Secur. Privacy Wireless Mobile Netw.,2012,113–124.

[6] E. Owusu, J. Han, S. Das, A. Perrig, and J. Zhang, “ACCessory: Password inference using accelerometers on smartphones,” in Proc. 12th Workshop Mobile Comput. Syst. Appl., 2012, pp. 9–14.

[7] Active Authentication, document DARPA-BAA-12-06, Defense Advanced Research Projects Agency, Arlington, VA, USA, 2012.

[8] M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song, “Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication,” IEEE Trans. Inf. Forensics Security, vol. 8, no. 1, pp. 136–148, Jan. 2013.

[9] F. E. Sandnes and X. Zhang, “User identification based on touch dynamics,” in Proc. 9th Int. Conf. Ubiquitous Intell. Comput. Autonomic Trusted Comput., Sep. 2012, pp. 256–263.

[10] D. Kim et al., “Multi-touch authentication on tabletops,” in Proc. SIGCHI Conf. Human Factors Comput. Syst., Atlanta, GA, USA, 2010,1093–1102.

[11] A. De Luca, A. Hang, F. Brudy, C. Lindner, and H. Hussmann, “Touch me once and i know it’s you! Implicit authentication based on touch screen patterns,” in Proc. SIGCHI Conf. Human Factors Comput. Syst., Austin, TX, USA, 2012, pp. 987–996.

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

[13] N. Zheng, K. Bai, H. Huang, and H. Wang, “You are how you touch: User verification on smartphones via tapping behaviors,” in Proc. IEEE 22nd Int. Conf. Netw. Protocols (ICNP), Oct. 2014, pp. 221–232.

[14] N. Zheng, K. Bai, H. Huang, and H. M. Wang, “You are how you touch: User verification on smartphones via tapping behaviors,” Dept. Comput. Sci., College William Mary, Williamsburg, VA, USA, Tech. Rep. WM-CS-201