Implicit Authentication for Mobile Device based on 3D Magnetic Finger Motion Pattern

Yaowen Liu, Ming Yang, Zhen Ling and Junzhou Luo
School of Computer Science and Engineering, Southeast University, Nanjing, China
{liuyaowen, yangming2002, zhenling, jluo}@seu.edu.cn

***Abstract*—Touch pattern based implicit authentication has been proposed to defend against diverse attacks against mobile devices that aim to obtain credentials, e.g., passwords, in the process of user authentication. However, this defense technique cannot obtain a complete user operation pattern by merely deriving user operation data via a touch-enabled screen, since user operations, including on-screen and in-air finger movements, are performed in a three-dimensional space. In this paper, we propose a novel three-dimensional magnetic finger motion pattern based implicit authentication technique, referred to as FingerAuth. To use FingerAuth, a user first wears a magnetic ring on her finger and uses this finger to operate her mobile device, e.g., typing messages and surfing websites. By using a built-in three-axis magnetometer on the mobile device, we can derive the three-dimension (3D) magnetic finger motion pattern that is used as a human behavioral feature to implicitly authenticate the user. We construct robust 3D magnetic finger motion pattern detection model using machine learning techniques. Real-world experiments were conducted to demonstrate that our approach achieves high accuracy of 96.38% as well as low false acceptance rate of 4.06% and low false rejection rate of 3.18%.**

Keywords—Behavioral Biometrics; Implicit Authentication; Mobile Device

I. INTRODUCTION

As computing power of mobile devices keeps growing, it plays an important role in collaborative environments, such as smart home and healthcare systems. Since various services can be accessed through mobile devices in these systems, extensive sensitive user information is stored on them. To keep the data from attackers, authentication techniques are pervasively adopted. However, most existing authentication techniques (e.g., password, fingerprint recognition, Android pattern lock) used on mobile devices today are usually invoked at the beginning of a session. Hence, attackers could pose a severe threat to security of the entire systems by retrieving the authentication credential through various side channels [1], [2], [3], [4], [5] and then perform impersonation attacks against mobile devices in these systems.

Although some secure input methods [6] were proposed to defend against side channel attacks, implicit authentication [7], [8] is widely accepted as a more promising technique to address the above issue. In contrast to explicit authentication that requires users to perform predefined authentication actions (e.g., enter the password or place the finger on top of certain sensor), implicit authentication commonly employs traits of the users that can be transparently sensed by using built-in sensors on a mobile device to implicitly authenticate the users. Since the majority of human-device interactions are performed using touchscreens, some researchers [8] use geometric patterns of users' interaction behavior on the touchscreens to implicitly authenticate users. However, the touchscreen could only record part of the finger interaction data, e.g., timestamp, touch pressure, touch position, and area of the finger touching the screen. It cannot completely model the finger motion pattern as user operations are performed in a three-dimensional space. Therefore, touch pattern based implicit authentication cannot provide accurate user identification.

In this paper, we propose a novel implicit authentication approach by exploiting three-dimensional magnetic finger motion pattern. A user is asked to wear a magnetic ring on her finger. When the user interacts with her mobile device, the finger motion could cause nearby magnetic field change and be sensed by a built-in magnetometer on the mobile device. The finger length and the angle between the finger and touchscreen vary among different people. Moreover, the in-air finger gestures are different as well. Thus, distinct user's finger motion could lead to various magnetic field changing pattern and this pattern can be used to distinguish different users. By excluding the influence of background magnetic field, the finger motion magnetometer data can be obtained during user-device interactions. Effective features are extracted and classification algorithms are then applied to detect the user finger pattern for implicit authentication. Our extensive empirical experiments are performed to show the effectiveness and efficiency of this approach.

The major contribution of this paper is summarized as follows.

- FingerAuth is the first of its kind for implicit authentication over mobile devices. Only a magnetic ring is required and a magnetometer is commonly an integral part of the mobile devices. Since users' finger and their motion pattern contains both physiological and behavioral characteristics, we make use of the magnetic ring to retrieve these biometric characteristics for implicit authentication purpose.
- We carefully choose effective features from the 3D magnetic finger motion pattern to accurately identify the users. We perform extensive real-world experiments to demonstrate the feasibility and effectiveness of our approach. The results show that the accuracy is 96.38%,

978-1-5090-6198-3/17/$31.00 ©2017 IEEE

while false acceptance rate and false rejection rate are of 4.06% and 3.18%, respectively.

The rest of this paper is organized as follows. We first discuss related work in Section II, then introduce the threat model and the basic idea of our proposed approach in Section III. In Section IV, we present the experimental results to verify the performance of the proposed implicit authentication approach. Finally, we conclude this paper in Section V.

II. Related Work

Implicit authentication is transparently performed to identify normal user activities without any explicit actions [9]. Implicit authentication technique could either be used at login or post-login phase. When adopted at login phase, it could serve as a secondary factor for authentication [7] to enhance the system to effectively defend against potential attackers who has already obtained a legitimate user's knowledge or possession factor for explicit authentication. To keep an attacker who can access a system authenticated by a legitimate user from obtaining the unauthorized information, implicit authentication techniques can be employed to re-authenticate the user at post-login phase.

The majority of implicit authentication techniques commonly exploit behavioral biometrics [10] for verifying the user's authenticity. Since most user-device interacting behaviors are achieved through a touchscreen, many researchers investigate various characteristics of touch behaviors for authentication purpose. The raw data a touchscreen could record usually are timestamp, touch pressure, touch position, and size (area of the finger touching the screen). Then, statistical and/or geometric features are extracted from the raw data. Algorithms and techniques such as Dynamic Time Warping and Machine Learning are finally utilized upon the raw data or extracted features [8], [11], [12], so as to authenticate the users. Among various touch interactions, typing has attracted much attention due to previous studies on keystroke dynamics in the past decades [13], [14], [15], which initially focus on physical keyboards for traditional systems. On a mobile device, typing is usually performed using an on-screen virtual keyboard. Consequently, touch features combining with traditional features such as latency, interval, dwell time, and flight time [16] can make this approach even more promising. Other built-in sensors are investigated as well, for example, accelerometer and/or gyroscope are used to extract biometric from gait [17], [18], typing [19], [20], or other user behaviors [21], and camera [22] is also used in some study.

There are also existing works exploring the built-in magnetometer in the field of human-computer interaction [23], [24], [25] and explicit authentication [26]. The study of [26] concentrates on explicit authentication by using a magnet to derive a user signature. However, we .1(n)-.8

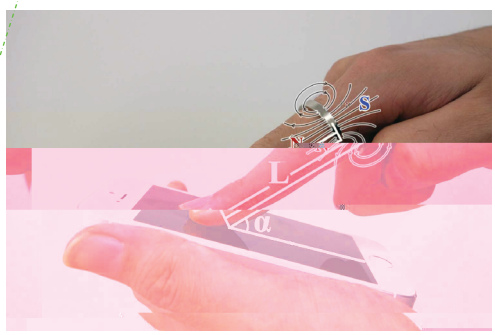

Fig. 1. A Magnetic Ring on the User's Index Finger

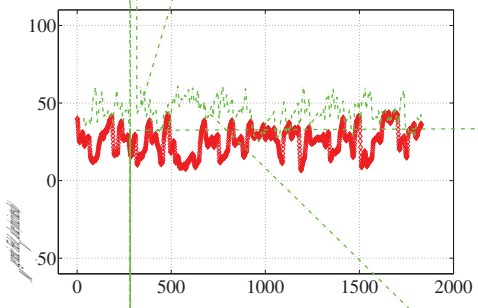

Fig. 2. Magnetometer Readings during Sentence Typing

Fig. 3. Workflow of the FingerAuth Approach

Fig. 4. Coordinate System of the Used Mobile Device

used on iOS devices is as depicted in Fig. 4, the field strength sensed by a magnetometer along each axis is in units of microteslas, while the direction of the field is represented by signs of sensor readings. As the finger moves around the device, strength and signs of magnetometer readings will change. Since the environment magnetic field can vary in distinct locations, we need to exclude the environment magnetic field to mitigate unexpected influence.

1) Background magnetic field cancellation: The overall magnetic field around a phone ($\mathbf{B_T}$) is the superposition of the magnetic field from the magnetic ring ($\mathbf{B_R}$) and the environment ($\mathbf{B_E}$, it is a superposition of magnetic field from Earth and nearby ferromagnetic materials). Thus, we have:

$$\mathbf{B_T} = \mathbf{B_R} + \mathbf{B_E} \tag{1}$$

Due to device rotations and the presence of hard iron and

where $\boldsymbol{M}$ denotes the rotation matrix of the smartphone, $\boldsymbol{W}$ and $\mathbf{V}$ represent soft-iron and hard-iron effects for simplicity. Hard-iron effect is caused by permanently magnetized ferromagnetic components of the sensor, while soft-iron effect is defined as "the interfering magnetic field induced by the geomagnetic field onto unmagnetized ferromagnetic components on the PCB" [27]. Most smartphone operating systems provide

calibration methods to mitigate these effects. We further eliminate potential side effects that can be brought out by environment magnetic field. After standard calibration process is performed, the magnetic field measured by a smartphone will be:

$$\mathbf{B_P} = \boldsymbol{M} \cdot (\mathbf{B_R} + \mathbf{B_E}) \tag{3}$$

The magnetic field strength of $\mathbf{B_E}$ in Equation (3) can be treated as a constant at a given location without significant environmental change, (e.g., increasing temperature). To cancel the background magnetic field, we first collect it using the built-in magnetometer without existence of the magnetic ring. Let $\mathbf{B_{E0}}$ be the recorded background magnetic field vector, and $\boldsymbol{M_0}$ be the rotation matrix corresponds to the attitude of the smartphone during environment magnetic field collection, since the inverse of a rotation matrix is its transpose,

ıetic field:

(4)

$$\mathbf{B_E} = (\boldsymbol{M_0})^{-1} \cdot \mathbf{B_{E0}} = (\boldsymbol{M_0})^{\mathrm{T}} \cdot \mathbf{B_{E0}} \tag{5}$$

For magnetic field vector $\mathbf{B_P}$ recorded with the presence of the magnetic finger ring, we have:

$$\mathbf{B_P} = \boldsymbol{M} \cdot (\mathbf{B_R} + \mathbf{B_E}) = \mathbf{B_R} + \boldsymbol{M} \cdot \mathbf{B_E}$$

$$= \mathbf{B_R} + \boldsymbol{M} \cdot (\boldsymbol{M_0})^{\mathrm{T}} \cdot \mathbf{B_{E0}} \tag{6}$$

In Equation (6), $\boldsymbol{M}$ is the rotation matrix corresponding to a new attitude of the smartphone, while $\mathbf{B_R}$ is the measured magnetic field introduced by the ring. Since the measured magnetic field of the magnetic ring is of our concern in this study, we have:

$$\mathbf{B_R} = \mathbf{B_P} \bar{\imath} \boldsymbol{M} \cdot (\boldsymbol{M_0})^{\mathrm{T}} \cdot \mathbf{B_{E0}} \quad (7)$$

While $\mathbf{B_{E0}}$ and $\mathbf{B_P}$ can be directly obtained from recorded data, the rotation matrix $\boldsymbol{M_0}$ and $\boldsymbol{M}$ could be easily calculated using the rotation angles of the mobile device. On the basis of equation (7), we may minimize potential side effects caused by environment magnetic field on later experiment. Then we can focus on analyzing the magnetic field changing pattern caused by the magnetic ring on the users' finger.

2) Sensor Data Segmentation: Three types of sensor data are collected, including magnetometer data, touchscreen sensor data, and device attitude data. The magnetometer readings we collected are series of timestamp and values of the magnetic field along each axis that can be denoted as T(i), Bx(i), By(i), and Bz(i), respectively. Touchscreen sensor data contains the touch information, e.g., timestamp, touch phase, etc. The device attitude data is used for background magnetic field cancellation purpose.

In the first step, we segment out magnetic field sensor data corresponding to user operations by using the timestamp of the first touch press and the last touch release. The second step is data alignment between magnetometer readings and device attitude values, this process is required because of the sampling rate difference between magnetometer and orientation sensor. On the iPhone used in our experiment, the sampling rate of the magnetometer is approximately around 50Hz, while the orientation sensor is about 100Hz. For each record from magnetometer readings, the timestamp T(i) is used to find the corresponding device attitude record with a minimum time difference. After data alignment is done, the background magnetic field cancellation process is conducted based on Equation (7). The last step is to further divide magnetometer data into smaller segments corresponding to on-screen and in-air finger movements for later data analysis purpose using touch information recorded from touch sensor.

D. Feature Extraction

After the data is properly preprocessed, a feature extraction process is performed. For each magnetic field data segment S_i obtained from data segmentation phase, a corresponding feature vector $\mathbf{F} = \{f_1(S_i), f_2(S_i), \ldots, f_n(S_i)\}$ is extracted for each axis data. Sixteen features are adopted: Mean, Median, Variance, Standard Deviation, Mode, Coefficient of Variation, Kurtosis, Skewness, Root Mean Square, Zero Crossing Rate, and the 1^{st}, 5^{th}, 25^{th}, 75^{th}, 95^{th}, 99^{th} Percentile.

IV. Experimental Evaluation

A. Data Collection

We design and conduct extensive experiments to test the applicability of using magnetometer to collect and extract motion pattern information of the finger with a magnetic ring on, and the effectiveness of utilizing this pattern to implicitly authenticate the user. The typical typing scenario is considered, which mainly involves tap gesture, as well as in-air gestures between taps. In order to collect sensor data in the scenario mentioned above, corresponding application for iOS devices is designed and implemented, it logs data from touch and magnetic field sensors, as well as device attitude data for preprocessing purpose while the user typing. Fifteen volunteers from our campus are recruited to participate in the data collection activity, and each one is asked to type the same ten predefined sentences for three times using the application we developed. To make data comparable among different participants, the same iPhone 5s smartphone is used, as well as the same magnetic ring, which is put on each participant's right index finger with identical direction, and all operations are performed using the index finger. Before each collection session, background magnetic field value without the presence of magnetic ring is also collected for background magnetic field cancellation purpose. Each extracted feature vector is first labeled with corresponding participant's name to make the data traceable. Then, each participant is assumed as a legitimate user in turn, corresponding data is copied and labeled with the string "legitimate", approximately the same amount of "illegitimate" data is produced by evenly copying data from other participants and the labels are changed to "illegitimate". The newly generated data (we may call it input instances) is stored in specific format that the machine learning software later used could utilize. Counting information of input instances for each participant is as TABLE I. shows.

TABLE I. Counting Information of Input Instances

Participant ID	Count of Instances with Different Labels		*Total Count*
	Legitimate	*Illegitimate*	
#1	1529	1526	3055
#2	1563	1554	3117
#3	1904	1904	3808
#4	1920	1918	3838
#5	1544	1540	3084
#6	1470	1470	2940
#7	1561	1554	3115
#8	1443	1442	2885
#9	1937	1932	3869
#10	1528	1526	3054
#11	1456	1456	2912
#12	1570	1568	3138
#13	1687	1680	3367
#14	1375	1372	2747
#15	1462	1456	2918

TABLE II. EVALUATION RESULTS

Participant ID	Naive Bayes			Random Forest			Support Vector Machine		
	Accuracy	*FAR*	*FRR*	*Accuracy*	*FAR*	*FRR*	*Accuracy*	*FAR*	*FRR*
#1	90.44%	18.02%	1.11%	97.68%	3.54%	1.11%	93.72%	7.27%	5.30%
#2	76.48%	44.66%	2.50%	97.34%	2.25%	3.07%	95.73%	4.89%	3.65%
#3	64.44%	65.97%	5.15%	95.06%	5.36%	4.52%	87.50%	11.08%	13.92%
#4	64.36%	69.24%	2.08%	95.44%	5.53%	3.59%	85.10%	19.34%	10.47%
#5	65.99%	60.91%	7.19%	99.42%	0.78%	0.39	98.80%	1.69%	0.71%
#6	83.57%	17.96%	14.90%	97.79%	1.43%	2.99%	94.80%	4.69%	5.71%
#7	67.67%	61.39%	3.40%	96.73%	4.25%	2.31%	86.04%	7.79%	20.12%
#8	68.77%	59.85%	2.63%	97.61%	1.32%	3.47%	95.42%	4.37%	4.78%
#9	72.09%	54.24%	1.65%	96.33%	1.97%	5.37%	87.34%	12.63%	12.70%
#10	73.12%	52.10%	1.70%	95.68%	6.29%	2.36%	89.95%	10.16%	9.95%
#11	66.41%	65.80%	1.37%	90.69%	12.84%	5.77%	77.30%	19.71%	25.69%
#12	71.03%	57.02%	0.96%	95.60%	4.34%	4.46%	87.09%	11.86%	13.95%
#13	92.16%	2.44%	13.22%	98.40%	0.48%	2.73%	96.35%	3.39%	3.91%
#14	88.75%	6.49%	16.00%	98.91%	0.66%	1.53%	97.67%	2.62%	2.04%
#15	68.71%	60.58%	2.12%	93.04%	9.82%	4.10%	75.91%	25.41%	22.78%
Average	74.27%	46.44%	5.06%	96.38%	4.06%	3.18%	89.91%	9.79%	10.38%

B. Security Evaluation

We use both classification and authentication metrics to evaluate the performance of the proposed approach, specifically, classification accuracy, false acceptance rate (FAR), and false rejection rate (FRR). In classification scenarios, accuracy is the proportion of correctly classified instances over a given instances set, while FAR and FRR are used in biometric systems to measure the probability of incorrectly accepting a malicious user and falsely rejecting a legitimate user respectively [9].

Recall that the goal is to study the feasibility of using the magnetic three-dimensional finger motion pattern to verify current user's authenticity, which could be abstracted as a classification problem in the domain of machine learning over feature vectors extracted from corresponding sensor data. Since the study itself is not targeting at machine learning issues, the widely used open-source machine learning software Weka [28] is used. Three classification algorithms are employed upon the same input data to learn which algorithm has the best potential performance. Specifically, the algorithms used are Naive Bayes [29], Random Forest [30] and Support Vector Machine [31], all are supported by Weka. Evaluation results using 10-fold cross-validation are shown in TABLE II. From the table we could see that although Naive Bayes could achieve high accuracy on some users' data, the FAR and FRR remain high comparing with other two algorithms, which could lead to security and usability issues. While SVM has considerable performance, it fails on some users' data. In general, Random Forest has the best performance among the three, with an average accuracy of 96.38%, an average FAR of 4.06%, and an average FRR of 3.18%. The promising results verified the applicability of the proposed approach for implicit authentication purpose.

V. CONCLUSION

In this paper, we proposed a novel three-dimensional magnetic finger motion pattern based implicit authentication technique to mitigate attacks that current explicit authentication techniques fail to defend against. We uncovered the hidden finger motion pattern by extracting effective features from magnetic field value introduced by the magnetic ring on user's finger, and constructed robust models using machine learning technique. Our extensive empirical experiments showed an encouraging result with accuracy above 90%, average FAR and FRR both below 5%, which verified that the proposed magnetic three-dimensional finger motion pattern is a promising trait that could be used to implicitly authenticate mobile device users. In further studies, we will delve into the causes and countermeasures of false acceptances and false rejections on a larger group of users to make the approach for real world application. The requirement of a magnetic ring maybe limits the wide range deployment, however, it won't be a problem when mobile devices are equipped with certain kind of sensor that could track the finger motion in a three-dimensional way.

ACKNOWLEDGEMENTS

This work was supported by National Natural Science Foundation of China under Grants No. 61572130, No.

61502100, No. 61532013, No. 61632008 and No. 61320106007, Jiangsu Provincial Natural Science Foundation of China under Grants No. BK20140648 and No. BK20150637, Jiangsu Provincial Key Technology R&D Program under Grant BE2014603, Qing Lan Project of Jiangsu Province, Jiangsu Provincial Key Laboratory of Network and Information Security under Grant No. BM2003201, and Key Laboratory of Computer Network and Information Integration of Ministry of Education of China under Grant No. 93K-9, in part by Collaborative Innovation Center of Novel Software Technology and Industrialization.

REFERENCES

[1] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, “Smudge attacks on smartphone touch screens,” in Proc. of the 4th USENIX Workshop on Offensive Technologies, Washington, DC, 2010.

[2] L. Cai and H. Chen, “TouchLogger: inferring keystrokes on touch screen from smartphone motion,” in Proc. of the 6th USENIX Workshop on Hot Topics in Security, San Francisco, CA, 2011.

[3] Q. Yue, Z. Ling, X. Fu, et al., “Blind recognition of touched keys on mobile devices,” in Proc. of the 2014 ACM SIGSAC Conference on Computer and Communications Security, Scottsdale, AZ, 2014, pp. 1403-1414.

[4] X. Pan, Z. Ling, A. Pingley, et al., “Password extraction via reconstructed wireless mouse trajectory,” IEEE Transactions on Dependable and Secure Computing, vol. 13, pp. 461-473, July-August 2016.

[5] Y. Zhang, P. Xia, J. Luo, et al., “Fingerprint attack against touch-enabled devices,” in Proc. of the 2nd Workshop on Security and Privacy a.949[sp]W2.26 -1.451 TD.0054 Tc([4])Tj]