Passcode Keystroke Biometric Performance on Smartphone Touchscreens is Superior to that on Hardware Keyboards

Lohit Jain[1], John V. Monaco[2], Michael J. Coakley[2], and Charles C. Tappert[2]

[1]Department of CSE, Indian Institute of Technology Kanpur, Kanpur, Uttar Pradesh, India
[2]Seidenberg School of CSIS, Pace University, White Plains, NY 10606, USA

International Journal of Research in Computer Applications & Information Technology
Volume 2, Issue 4, July-August, 2014, pp. 29-33
ISSN Online:2347-5099, Print:2348-0009, DOA : 11 August, 2014

ABSTRACT

This study determined the degree to which keystroke performance results obtainable on mobile devices exceed those obtainable on hardware keyboards. The biometric equal error rates on three sets of smartphone touchscreen data – the keystroke timing data similar to that available on hardware keyboards, the non-timing touchscreen data not available on hardware keyboards, and all the touchscreen data combined – were 10.5%, 3.5%, 2.8%, respectively. These results show that considerably greater biometric value is available from smartphone touchscreen data compared to that from hardware keyboards.

Keywords: *Biometrics, Keystroke Dynamics, Machine Learning, Mobile Devices, User Authentication.*

1. INTRODUCTION

Because passwords for computer and account access, and passcodes for building and ATM access, can be easily compromised, the addition of biometric user-identity information could help reduce these security threats. The touchscreen sensors of mobile devices provide considerably richer data than that available from personal computer hardware keyboards, and this study explores the keystroke biometric performance achievable from the richer touchscreen data compared to that available from hardware keyboards.

Keystroke biometric systems measure typing characteristics believed to be unique to an individual and difficult to duplicate. The keystroke biometric is one of the less-studied behavioral biometrics, usually relegated to conference sessions on "other biometrics" and described only briefly in books on biometrics. Nevertheless, the keystroke biometric has been reviewed in several recent articles [1, 2]. Most of the studies on keystroke dynamics have used data captured from hardware keyboards of personal computers, and there are currently a number of commercial products, primarily for password strengthening (also called password "hardening") [3].

Recent keystroke dynamic studies have focused on data captured on touchscreen virtual keyboards. Table 1 summarizes six keystroke studies on touchscreen data of mobile devices. The touchscreen sensor data typically includes:

- keystroke timing: key-down/key-up times also available on hardware keyboards
- pressure: the finger pressure used on a soft key
- location: x-y coordinates of the position of the finger touching a soft key
- size/orientation: length and orientation of major and minor axes of finger-press area

When references undertook several studies, only the most relevant ones are listed in the table. The most common performance metric used when comparing biometric systems is the Equal Error Rate (EER) where the False Accept Rate (FAR) is equal to the False Reject Rate (FRR).

Table 1. Summary of Previous Mobile-Device, Touch Screen Studies.

Ref	Sensors Used	Input	# Users	Performance
[4]	Keystroke timing	4-digit PIN	20	FAR=57%/FRR=15%
[5]	Keystroke timing	Fixed/free text	10	70% identification
[6]	Keystroke timing	Short sentences	300	TPR=92% FPR=1%
[7]	Keystroke timing Speed & distance	10-char passphrase	20	EER=26% EER=13.6%
[8]	Keystroke timing Pressure/size orientation	7-digit number	35	FAR=9.0%/FRR=6.7%
[9]	Keystroke timing Pressure/size orientation Acceleration	4-digit PIN 8-digit PIN	53 25	EER = 3.65% EER = 4.45%

Buchoux and Clarke [4] obtained a FRR of 15% and a FAR of 57.5% on 20 users entering a 4-digit PIN. Fleming [5] successfully identified users entering long (about 200 words) fixed and free-form text 70% of the time on 10 users. Gascon et al. [6] tasked over 300 participants to enter short text sentences into a mobile phone, obtaining a True Positive Rate (TPR) of 92% with a corresponding False Positive Rate (FPR) of only 1%. Kambourakis et al. [7] augmented traditional keystroke biometric data with the additional features of distance covered (in pixels) between two successively pressed keys, and speed calculated as the distance divided by the time between successive key presses. The incorporation of these additional features led them to achieve an EER of 26% on a ten-digit passcode and an EER of 13.6 on short passphrase input. Trojahn and Ortmeier [8] used key-press pressure and key-press area size in addition to keystroke timing to achieve FAR=9.0 and FRR=6.7% on a 12-key layout. Zheng et al. [9] focused their research on exploiting four features easily extracted from today's smartphones – keystroke timing, pressure of key-press, size/orientation of finger-press area, and acceleration – to achieve the Table's best EER's of 3.65% on data from 53 users.

Other recent studies focused primarily on data captured from the accelerometer and gyroscope sensors. For example, Giuffrida et al. [10] employed text passwords (the words "internet" and "satellite") with data captured from the accelerometer and gyroscope sensors to achieve high performance using research staff members as participants in a highly-controlled environment. This research suggests that data captured from the accelerometer and gyroscope sensors on mobile devices can essentially replace the traditional keystroke-timing data to authenticate users with considerably higher accuracy than that obtainable using traditional keystroke analytics.

The current study employed a common-to-all-user, 10-digit passcode input on the keypad of a mobile phone. The passcode was similar to that used in two earlier studies on hardware keyboards [11, 12]

and references to related keystroke studies on numeric data can be found in those papers. This study differed from the earlier studies on touchscreen data (Table 1) because it directly compared the performance obtained from the richer touchscreen data to that obtainable from hardware keyboards. This was achieved by measuring system performance on three sets of features derived from the following data:

1. Keystroke timing data also available from hardware keyboards
2. Non-timing touchscreen data not available from hardware keyboards
3. All the touchscreen data (sets 1 and 2 combined)

In addition to touchscreen sensors, smartphones usually have other sensors, such as accelerometers and gyroscopes that typically capture data periodically along the x, y, and z axes. These non-touchscreen sensors were not used in this study.

The remaining sections of the paper present the methodology, the experimental results, the discussion, and the conclusions.

2. METHODOLOGY

This section describes the methodologies employed in this study: choice of passcode, data capture, feature extraction, and authentication classification.

2.1 Choice of Passcode

A single 10-digit passcode was employed in the study. Although longer than the average passcode, this length was chosen to provide reasonable discrimination among the participants while not being too tedious to type repetitively, as in earlier studies [11, 12]. The same passcode was used by all the participants primarily for experimental purposes to allow each participant to be treated as a "zero-effort" imposter for the other participants. The passcode number chosen was **914 193 7761** because 914 is the local area telephone code and because the sequence spans the keypad.

2.2 Data Capture

A soft keyboard application was developed for the Android platform to collect data from participants. The custom input method editor (IME) replaces the system keyboard, and can capture keystrokes in any application that uses a keyboard. Key press and release events were stored in a SQLite database and transmitted to a server to centralize all of the data collected.

Events are generated when a user presses are releases a button on the soft keyboard. Each event contains the action (press or release), timestamp, screen coordinates, and pressure. Additional sensors on the devices such as gyroscopic and rotational sensors, are ignored in this study, as many touchscreen devices (e.g. ATM or self-checkout registers) do not contain these types of sensors. Captured events strictly alternate between press and release actions, since the software used to capture data did not support multiple-touch gestures. Timestamps were captured in millisecond precision, although the actual precision of the device depends on the hardware clock and is not known. The pressure is usually in the range from 0 to 1, where 1 indicates a "normal" pressure and also depends on the calibration of the device [13]. Screen coordinates are in the range of the screen resolution, and need not be normalized since data collection was performed using identical devices.

The numeric keypad data were collected from 30 subjects over several days with 15-30 samples collected per subject per day. Each participant first practiced keying the input string several times

before the samples were recorded. Each sample consisted of the numeric sequence **914 193 7761** (shown here in telephone number format) followed by the **Enter** key to provide a total of 11 keystrokes per sample. The samples were entered on the phone's numeric keypad as if entering a phone number or entering an ATM pin. Data collection was performed on 5 identical LG-D820 Nexus 5 devices, which have 4.95 inch touch screens with a resolution of 1080x1920 pixels. Only samples that were entered correctly, i.e. exactly 11 keystrokes in the correct order, are considered. Samples that include deletions or incorrect entries are omitted.

2.3 Feature Extraction

Three sets of features are defined in order to determine the effect of touchscreen biometrics in addition to the well studied keystroke biometrics. The three feature sets include: timing features, touchscreen features, and both timing and touchscreen features combined. Timing feature extraction is performed similarly to that described in [11]. The duration of each soft keystroke, and transitions between press-release and release-press events are taken, for a total of 31 features.

The non-timing touchscreen features are calculated similarly to the timing features. The pressure and the position of screen-touch x-y coordinates are defined as touchscreen measurements, for a total of three measurements. Accurate size/position data were not available on the device used in this study. The three measurements are sampled at each press and release event. The complete touchscreen feature set is composed of touchscreen measurements at each press and release event (3x22=66), the difference of each measurement between press and release events for each key (3x11=33), and the difference of each measurement between press-release and release-press transitions (3x10x2=60). Thus, there are a total of 159 touch features.

All features were normalized into the range 0-1 by clamping each feature at +/- 2 standard deviations.

2.4 Authentication Classification

Authentication classification was performed by a "one-class" Support Vector Machine (SVM) as described by Yu and Cho [14] and employed in a study by Killourhy and Maxion [15]. This algorithm creates a one-class SVM linear separator in a high-dimensional space from the training vectors. During testing, a test vector is projected into the same high-dimensional space, the signed distance from the linear separator calculated, and this distance with the sign inverted is used as the classification score.

3 EXPERIMENTAL RESULTS

The SVM classification system was used to measure system performance on three sets of features derived from:

1. Keystroke timing data also available from hardware keyboards
2. Non-timing touchscreen data not available from hardware keyboards
3. All the touchscreen data (sets 1 and 2 combined)

The results are shown in Table 2.

Table 2. EER for the Three Experimental Conditions

Keystroke Timing Data	Non-timing Touchscreen Data	All Touchscreen Data
10.5%	3.5%	2.8%

4 CONCLUSIONS

The main contributions of this study were to quantify the degree to which the keystroke performance results obtainable on mobile devices exceed those obtainable on hardware keyboards. The EER of 10.5% obtained here on the keystroke timing data from the smartphone touchscreen is comparable to that obtained on hardware keyboard studies [11, 12] as was anticipated. The EER of 3.5% on the non-timing touchscreen data indicates that the touchscreen data not available on hardware keyboards has greater biometric value than that available on hardware keyboards. Finally, the EER of 2.8% on all the touchscreen data employed in the study demonstrates that touchscreen data has considerably greater biometric value than that available on hardware keyboards. Future work could incorporate the additional data available from the accelerometer and gyroscope sensors which should further separate the biometric performances of systems based on data available on smartphone touchscreens relative to that available on hardware keyboards.

REFERENCES

[1] M. Karnan, M. Akila, and N. Krishnaraj, "Biometric personal authentication using keystroke dynamics: A review," *Applied Soft Computing J.*, vol. 11, 2011.

[2] K. Revett, "Chapter 4: Keystroke dynamics," in *Behavioral biometrics: A remote access approach* (Wiley, 2008), pp. 73-136.

[3] Wikipedia, Keystroke dynamics, commercial products. http://en.wikipedia.org/wiki/ Keystroke_dynamics#Commercial_products , accessed July 2014.

[4] A. Buchouox and N. Clarke, "Deployment of Keystroke Analysis on a Smartphone," *Australian Information Management Conference*, 2008.

[5] S. Fleming, "Identification of a Smartphone User via Keystroke Analysis," *Thesis, Naval Postgraduate School*, Monterey, CA, March 2014.

[6] H. Gascon, S. Uellenbeck, C. Wolf, K. Rieck, "Continuous Authentication on Mobile Devices by Analysis of Typing Motion Behavior," *Proc. of GI Conference "Sicherheit" (Sicherheit, Schutz und Verlässlichkeit)*, March 2014.

[7] G. Kambourakis, D. Damopoulos, D. Papamartzivanos, E. Pavlidakis, "Introducing Touchstroke: Keystroke-based Authentication System for Smartphones", *John Wiley & Sons, Ltd.*, 2013

[8] M. Trojahn and F. Ortmeier, "Biometric authentication through a virtual keyboard for smartphones." Int. J. Computer Science & Info. Technology (IJCSIT), Vol. 4, No. 5, 2012.

[9] N. Zheng, K. Bai, H. Huang, H. Wang, "You Are How You Touch: User Verification on Smartphones via Tapping Behaviors", *College of William & Mary Department of Computer Science*, WM-CS-2012-06, December 2012.

[10] C. Giuffrida, K. Majdanik, M. Conti, H. Bos, "I Sensed It Was You: Authenticating Mobile Users With Sesnsor-Enhanced Keystroke Dynamics", *DIMVA 2014*, Springer International Publishing, 2014, pp. 92-111.

[11] R.A. Maxion, and K.S. Killourhy, "Keystroke biometrics with number-pad input." *Proc. IEEE/IFIP Int. Conf. Dependable Sys. & Netw. (DSN-10)*, pp. 201-210, 2010. IEEE Comp. Soc. Press, 2010.

[12] N. Bakelman, J.V. Monaco, S. Cha, and C.C. Tappert, "Keystroke Biometric Studies on Password and Numeric Keypad Input," *Proc. 2013 European Intelligence and Security Informatics Conf.*, Sweden, 2013.

[13] Android docs, http://developer.android.com/reference/android/view/MotionEvent. html#getPressure(int) , accessed July 2014.

[14] E. Yu and S. Cho, "GA-SVM wrapper approach for feature subset selection in keystroke dynamics identity verification," *Proc. Int. Joint Conf. Neural Networks (IJCNN)*, IEEE Press, 2003, pp. 2253–2257.

[15] K. Killourhy and R. Maxion, "Comparing anomaly-detection algorithms for keystroke dynamics," *Int. Conf. Dependable Systems & Networks*, Lisbon, 2009, pp. 125-134.