# Accepted Manuscript


TouchWB: Touch behavioral user authentication based on web browsing on smartphones

Weizhi Meng, Yu Wang, Duncan S. Wong, Sheng Wen, Yang Xiang

PII: S1084-8045(18)30172-3

DOI: 10.1016/j.jnca.2018.05.010

Reference: YJNCA 2142

To appear in: *Journal of Network and Computer Applications*

Received Date: 12 February 2018

Revised Date: 3 May 2018

Accepted Date: 9 May 2018

Please cite this article as: Meng, W., Wang, Y., Wong, D.S., Wen, S., Xiang, Y., TouchWB: Touch behavioral user authentication based on web browsing on smartphones, *Journal of Network and Computer Applications* (2018), doi: 10.1016/j.jnca.2018.05.010.

# TouchWB: Touch Behavioral User Authentication Based on Web Browsing on Smartphones

Weizhi Meng[a,b], Yu Wang[a,2], Duncan S. Wong[c], Sheng Wen[d], Yang Xiang[d]

[a]*School of Computer Science, Guangzhou University*
[b]*Department of Applied Mathematics and Computer Science, Technical University of Denmark, Denmark*
[c]*Hong Kong Applied Science and Technology Research Institute, Hong Kong*
[d]*Swinburne University of Technology, Australia*
[e]*E-mail address: {weme@dtu.dk, yuwang@gzhu.edu.cn}*

**Abstract**

Modern mobile devices specially smartphones have rapidly evolved and are widely adopted by people of different ages. Smartphones can assist users in a variety of activities, i.e., from social networking to online shopping, but also have become an attractive target for cyber-criminals due to the stored personal data and sensitive information. The traditional authentication mechanisms like PIN suffer from well-known limitations and drawbacks in the security community; thus, touch behavioral authentication has recently received much attention. Intuitively, authentication based on free touches would be hard to build a stand-alone system. In this work, we advocate that such authentication can consider users' actions under certain phone applications like web browser, and then propose a touch gesture-based authentication scheme, called *TouchWB*, with 21 features that can be extracted from web browsing gestures. For evaluation, we implemented the scheme on Android phones and conducted a user study involving 48 participants. Experimental results demonstrated that our approach could reduce the touch behavioral deviation by nearly half and achieve an average error rate of about 2.4% by using a combined classifier of PSO-RBFN.

*Keywords:*
Behavioral Authentication, Touch Gesture, Smartphone Security, Access Control, Touchscreen, Machine Learning.

## 1. Introduction

Nowadays, smartphones have undoubtedly dominated the phone market. A report from International Data Corporation has shown that a total of 344.3 million smartphones have been shipped around the world only in the first quarter of 2017 (1Q17), achieving a 3.4% increase over the last year [7]. Due to the increasingly enhanced capabilities of smartphones, users often store their personal data and even sensitive information on the phones for convenience, such as personal photos, credit card numbers, online transaction credentials and so on [12]. The use of smartphones are beneficial to people's daily life, but the stored data is an attractive target for cyber-criminals, who are always keen on breaking into the phones and making profits [11, 13]. As a result, there is a significant need to deploy proper user authentication schemes to protect these devices.

Current authentication on smartphones is still provided by conventional password-based mechanisms like Personal Identification Numbers (PIN) and graphical passwords [2]. However, password-based authentication has well-known drawbacks. For instance, passwords are easily to be stolen through direct observations like "shoulder surfing" [34], smudge attacks [1] and smartphone charging attacks [19, 22], where an attacker can take advantage of observation techniques, the smudges left by a finger and recording phone screen information to refer users' privacy, respectively. In addition, due to the long-term memory limitation of remembering a strong password, users are found more likely to choose a simple and memorable password instead, which would degrade the whole authentication security level.

[1]A preliminary version of this paper appears in Proceedings of the 8th China International Conference on Information Security and Cryptology (INSCRYPT), pp. 331-350, LNCS, Springer, 2012. The first author finalized the work during the visit at School of Computer Science, Guangzhou University.

[2]Corresponding author, yuwang@gzhu.edu.cn