available at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Keystroke dynamics-based authentication for mobile devices

Seong-seob Hwang, Sungzoon Cho, Sunghoon Park*

Seoul National University, 599 Gwanangno, Gwanak-gu, Seoul 151-742, Republic of Korea

ARTICLE INFO

Article history:
Received 26 November 2007
Received in revised form
2 June 2008
Accepted 29 October 2008

Keywords:
Mobile device
Keystroke dynamics
Artificial rhythms
Tempo cues
Biometrics
User authentication

ABSTRACT

Recently, mobile devices are used in financial applications such as banking and stock trading. However, unlike desktops and notebook computers, a 4-digit personal identification number (PIN) is often adopted as the only security mechanism for mobile devices. Because of their limited length, PINs are vulnerable to shoulder surfing and systematic trial-and-error attacks. This paper reports the effectiveness of user authentication using keystroke dynamics-based authentication (KDA) on mobile devices. We found that a KDA system can be effective for mobile devices in terms of authentication accuracy. Use of artificial rhythms leads to even better authentication performance.

1. Introduction

Use of mobile devices is diversified more and more (Chen et al., 2008). Cell phones and personal digital assistants (PDA) are used for banking and stock trading nowadays. However, there are three reasons why security of mobile devices has a lot to be desired. First a PIN comprises only four digits, thus, the number of candidate passwords is limited to only 10,000 (from 0000 to 9999). It is much easier for a potential impostor to acquire the password by shoulder surfing and systematic trial-and-error attacks. Second, mobile devices may be easily lost or stolen because of their small sizes. For example, more than one million mobile phones are stolen in Europe for a typical year (Kowalski and Goldstein, 2006). Third, we tend to lend mobile phones easily to other people, thus they are exposed to a higher risk of surreptitious use.

Recently, biometrics has been proposed to improve the security of mobile devices. The term ''biometrics'' is defined by International Biometric Group as ''the automated use of physiological or behavioral characteristics to determine or verify identity.'' Physiological biometrics relies upon a physical attribute such as a fingerprint, a face and an iris, whereas behavioral approaches utilize some characteristic behavior, such as the way we speak or sign our name (Clarke and Furnell, 2005). Clarke and Furnell (2007a) concluded that the two-factor authentication, combining PIN code and biometrics, improves the overall reliability of authentication.

Keystroke dynamics-based authentication (KDA) is one of biometrics-based authentication methods, motivated by the observation that a user's keystroke patterns are consistent and distinct from those of other users. When implemented for mobile devices, KDA has the following advantages over other biometrics-based methods. First, most biometrics-based methods require an extra device, e.g. a finger-scanner or an iris-scanner (Clarke and Furnell, 2005), which restricts mobility as well as increases cost. On the other hand, KDA

* *Corresponding author*. Tel.: +82 2 880 6275; fax: +82 2 889 8560.
E-mail addresses: hss9414@snu.ac.kr (S.-s. Hwang), zoon@snu.ac.kr (S. Cho), shpark82@snu.ac.kr (S. Park).
0167-4048/$ – see front matter © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2008.10.002

requires no additional device. Second, users tend to be reluctant to provide their fingerprints or irises. On the other hand, a user always has to type his or her password to log in, so collecting keystroke patterns can be done without causing any extra inconvenience to the user. Third, a scanned fingerprint or iris requires a large volume of memory, a higher computing power and communication bandwidth than keystroke timing vectors. The efficiency of KDA is particularly important in mobile environment which tends to have a smaller memory, a lower computing power and slower wireless Internet than a PC on the wired Internet.

Behavioral attributes are more subject to deviation from norms than physical ones. A high variability leads to a high authentication error. The variability is a measure of data quality. Another measure of data quality is how unique the typing patterns are. The more unique, the less likely the patterns are similarly replicated by impostors. Recently, artificial rhythms and tempo cues were proposed to improve the quality of typing patterns: uniqueness and consistency in particular (Cho and Hwang, 2006). Improving the data quality by decreasing variability and increasing uniqueness helps us alleviate the weakness of a short PIN.

In this paper, we propose KDA with artificial rhythms and tempo cues for mobile user authentication. To compare between ''Natural Rhythm without Cue'' and ''Artificial Rhythms with Cues,'' we completed the following tasks. First, we implemented KDA system on a mobile phone which is connected to a remote server through a wireless network. The novelty detector classifier was built since only valid users' patterns are available in practice. Second, subjects were asked to perform enrollment, login, and even intrusion to other subjects' accounts. Whenever a subject types his or her password, the typing pattern is collected, sent to a server and stored. Third, a comparative analysis was conducted to verify the superiority of artificial rhythms and cues over natural rhythms without cues. We also tested hypotheses to compare the performance involving different typing strategies.

The organization of this paper is as follows. The following section introduces keystroke dynamics-based authentication for mobile devices and describes our methods to improve the quality of typing patterns. Section 3 presents the data collected and experimental results. Finally, conclusions and a list of future work are discussed in Section 4.

2. Keystroke dynamics-based authentication for mobile devices

2.1. *Keystroke dynamics-based authentication (KDA)*

The password-based authentication is the most commonly used in identity verification. However, it becomes vulnerable when the password is stolen. Keystroke dynamics-based authentication was proposed to provide additional security (Gaines et al., 1980; Umphress and Williams, 1985). Keystroke dynamics-based authentication (KDA) is to verify a user's identity using not only the password but also keystroke dynamics. For example, a keystroke pattern is transformed into a timing vector when a user types a string ''5805'' as illustrated in Fig. 1. The duration and interval times are measured by milliseconds. A user can get access only if his timing vector is similar enough to those already registered in the server. Thus, he or she can only get access if the password is typed with the correct rhythm.

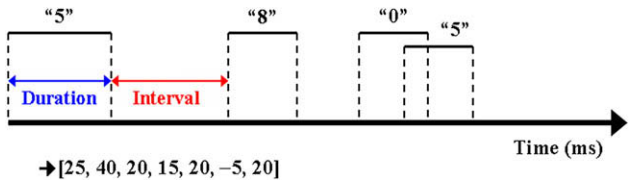

Fig. 1 – A keystroke pattern is transformed into a timing vector when a user types a string "5805." The duration and interval times are measured by milliseconds.

Three steps are involved in KDA as illustrated in Fig. 2. First, a user enrolls his/her keystroke patterns. A keystroke pattern is defined as depicted in Fig. 1. A password of m characters is transformed into a $(2m-1)$-dimensional timing vector. A ''duration'' denotes a time period during which a key is pressed while an ''interval'' is a time period between releasing a key and stroking the next key. Second, a classifier is built using the keystroke patterns. The classifier, in a sense, is a prototype of the valid user patterns. Third, when a new keystroke pattern is given, one will reject it as an impostor pattern if the distance between the prototype and the pattern is greater than some threshold, or accept it as the valid user's pattern otherwise.

KDA can help us improve security for various services involving mobile devices (Hwang et al., 2007). Even when an impostor obtains both PIN and the mobile device, KDA can still prevent him from logging in through the strengthened authentication process. Recently, Clarke and Furnell (2005, 2007a,b) studied user identification using KDA on mobile devices. They utilized the keystroke of 11-digit telephone numbers and text messages as well as 4-digit PINs to classify users. Their identification models were based on feed forward multi-layer perceptron (FF-MLP), radial basis function (RBF) networks, and generalized regression neural networks (GRNNs).

Our approach is different from that of Clarke and Furnell (2005, 2007a,b) in the following aspects. First, they built a classifier using impostors' patterns as well as the valid user's patterns. In reality, however, impostors' patterns are not available unless the password be disclosed to potential impostors and their patterns are collected. Rather, we employed novelty detection framework where only the valid user's patterns are used for training. Second, each user in their experiments enrolled 30 typing patterns. In practice, users would not endure such a long enrollment procedure. Moreover, the typing speed on mobile devices is much slower than that on a local PC. In our study, we collected only five patterns from each user for enrollment. We compensated the reduced data quantity with improved data quality through use of artificial rhythms and cues strategy. Third, they utilized various patterns such as 4-digit PINs, 11-digit telephone numbers, and text messages while we focused only on 4-digit PIN since PIN has been fixed to four digits for decades. Fourth, their subjects used an SW interface developed on a laptop while our subjects used a real mobile phone, which is a third