Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

Continuous user authentication using multi-modal biometrics

Hataichanok Saevanee [a,*], Nathan Clarke [a,c], Steven Furnell [a,c], Valerio Biscione [b]

[a] Centre for Security, Communications and Network Research, Plymouth University, Plymouth, United Kingdom
[b] Centre for Robotics and Neural Systems, Plymouth University, Plymouth, United Kingdom
[c] Security Research Institute, Edith Cowan University, Perth, Western Australia, Australia

ARTICLE INFO

Article history:
Received 15 December 2014
Received in revised form
2 June 2015
Accepted 3 June 2015
Available online 12 June 2015

Keywords:
Biometrics
Transparent authentication
Multimodal biometrics
Linguistic profiling
Keystroke dynamics
Behavioural profiling
Mobile device

ABSTRACT

As modern mobile devices increase in their capability and accessibility, they introduce additional demands in terms of security – particularly authentication. With the widely documented poor use of PINs, Active Authentication is designed to overcome the fundamental issue of usable and secure authentication through utilizing biometric-based techniques to continuously verify user identity. This paper proposes a novel text-based multimodal biometric approach utilizing linguistic analysis, keystroke dynamics and behavioural profiling. Experimental investigations show that users can be discriminated via their text-based entry, with an average Equal Error Rate (EER) of 3.3%. Based on these findings, a framework that is able to provide robust, continuous and transparent authentication is proposed. The framework is evaluated to examine the effectiveness of providing security and user convenience. The result showed that the framework is able to provide a 91% reduction in the number of intrusive authentication requests required for high security applications.

1. Introduction

It is commonly acknowledged that mobile devices have become part of an individual's everyday life. Mobile devices are widespread with over 7 billion subscribers around the world (ITU, 2014). With the rapid development of mobile network technology and the increasing popularity of mobile devices, modern mobile devices are capable of providing a wide range of services and applications over multiple networks. The plethora of functionalities offered by mobile devices enables user to store increasing volumes of business and personal information, both of which could be sensitive. A series of studies have highlighted the potential risk of mobile device misuse if personal information (e.g. home address), credentials (e.g. PIN codes, user name and password) and business data (e.g. customer data) are stored upon them (Kaspersky Lab, 2011; Dimensional Research, 2013).

The most commonly used authentication method for protecting mobile devices from being misused is the use of Personal Identification Number (PINs) or passwords. Unfortunately, the weaknesses of passwords and PINs have been widely documented (McAfee, 2013; Clarke and Furnell, 2005). In addition, the fundamental flaw of the PINs or

[*] *Corresponding author.*
E-mail address: info@cscan.org (H. Saevanee).

http://dx.doi.org/10.1016/j.cose.2015.06.001
0167-4048/© 2015 Elsevier Ltd. All rights reserved.

passwords is that as a point-of-entry technique, once the user has been authenticated successfully, they have access to the system without having to be re-authenticate again. This can lead to high risk environment when an intruder targets a post authenticated session. Although many authentication mechanisms such as fingerprint or face recognition have been developed for mobile devices with the aim of increasing the level of security and convenience for the end user, these advanced techniques remain point of entry and intrusive to the user. Several studies have proposed advanced authentication mechanisms that can provide transparent and continuous authentication to the user by using behavioural biometrics (Karatzouni et al., 2007; Li et al., 2011; Sim et al., 2007). According to these studies a number of biometrics could have the potential to be used for transparent authentication on mobile devices including keystroke dynamics, behavioural profiling and gait recognition. Since texting is one of the most popular applications that a mobile user uses on a daily basis (Ofcom, 2012), this paper focuses upon the use of three behavioural biometric techniques: linguistic profiling, keystroke dynamics and behaviour profiling for developing an authentication mechanism that can provide a cost-effective, non-intrusive and continuous solution to the problem of user authentication.

There are a large number of studies in the area of transparent and continuous user authentication and they all seek to develop new and more efficient modalities to support the underlying biometric performance or focus upon the management processes (Clarke and Furnell, 2007; Crawford et al., 2013). The paper aim at contributing to a wider field of research in the area of transparent authentication and makes a number of additional contributions over the existing work. This paper begins by introducing the study and presenting the state of the art in behavioural biometrics that has been applied within the mobile domain. This will then be followed by describing a comprehensive experimental study of multimodal biometrics. Based upon the results, Section 4 presents a novel text-based multimodal framework that will provide the verification of a mobile user's identify in a continuous and transparent manner. Section 5 presents an evaluated of the aforementioned framework through simulation. The paper concludes by highlighting the future direction of the research.

2. An overview of behavioural biometrics for mobile devices

In recent years, many mobile devices have come equipped with a variety of hardware components that are able to capture biometric traits. This enables several biometric approaches to be deployed on them. For example, Apple has now incorporated TouchID, a finger-print-based approach, and Google has Face Unlock for its Android Operating System (ComputerWeekly; MIT Technology Review). To date, however, these physiological biometric techniques are mainly deployed to offer point-of-entry solutions that. In comparison, behavioural biometric methods have the ability to provide continuous and transparent verification of a user's identity. However, behavioural biometric features tend to change over time and under different external circumstances that can affect the sample collection and classification. Therefore, care is required when considering their implementation in an authentication system where less control over the user and the environment exists.

A number of studies have been carried out on the use of behavioural techniques such as gait, hand writing and voice recognition for authentication on mobile devices (Clarke and Mekala, 2007; Hoang et al., 2013; Kim et al., 2010). Of interest in this research is the use of three behavioural biometric techniques: linguistic profiling, keystroke dynamics and behavioural profiling. It is hypothesized that the integration of these three techniques together could offer the opportunity to improve upon the usability through transparent capture and improved overall recognition performance.

Linguistic profiling is a behavioural biometric that identifies people based upon linguistic morphology (Halteren, 2004). A number of researchers have investigated the feasibility of linguistic profiling for several purposes such as text categorization, authorship identification and authorship verification (Halteren, 2004; Zhang and Lee, 2006; Stamatatos, 2007). In the authorship verification domain, examples of writing from a single author are given to the system, which is then asked to confirm if the given texts were written by this author. Over 1000 writing styles have been proposed and both statistical and machine learning methods were used in the analytical process (Rudman, 1998). Many studies have confirmed the good discriminative capability of linguistic features. By using a machine learning method, the performance accuracies were in the range of 80%–100% (Halteren, 2004; Zheng et al., 2006). However, there is no agreement on a best set of features for authorship verification and historically large volumes of text are required for the training dataset. The performance of linguistic profiling technique is highly dependent upon the number of candidate authors, the size of texts, the combination of the selected features and classification models utilized. Although the majority of previous studies tend to focus on long texts per author – 10,000 words per author are regarded to be a reliable minimum for an authorial set (Burrows, 2007), some studies have shown promising results with short texts (e.g. student essay and email) but the minimum requirements for a text have not been determined (Sanderson and Guenter, 2006; Hirst and Feiguina, 2007). The effectiveness of linguistic profiling have been examined in various languages. The study (Hirst and Feiguina, 2007) examined the n-gram language model on Greek newspaper articles, English documents and Chinese novels using Bayesian classification techniques. The researchers concluded that to identify unique linguistic characteristics of Chinese, character-based features n-grams should be used to avoid word-segmentation problems. They also noted that the Chinese vocabulary is much larger than the English, which may give rise to sparse data problems. The results showed that the best accuracy achieved was 90% in all three language. However, the performance on Chinese was not as good as that for English.

Behavioural profiling aims to identify users based upon the way in which they interact with the services on their mobile device. Previous behaviour-based studies have mainly focused upon the area of fraud detection and intrusion detection (Boukerche and Nitare, 2002; Damopoulos et al.,