Journal of Information Security and Applications 37 (2017) 28–37

Contents lists available at ScienceDirect

Journal of Information Security and Applications

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

A survey on behavioral biometric authentication on smartphones

Ahmed Mahfouz [a,*], Tarek M. Mahmoud [a,b], Ahmed Sharaf Eldin [c,d]

[a] Computer Science Department, Minia University, El-Minia, Egypt
[b] Canadian International College (CIC), Cairo, Egypt
[c] Information Systems Department, Helwan University, Egypt
[d] Faculty of Information Technology and Computer Science, Sinai University, Egypt

ARTICLE INFO

Article history:

Keywords:
Behavioral biometric authentication
Touch dynamics
Keystroke dynamics
Behavioral profiling
Gait recognition

ABSTRACT

Recent research has shown the possibility of using smartphones' sensors and accessories to extract some behavioral attributes such as touch dynamics, keystroke dynamics and gait recognition. These attributes are known as behavioral biometrics and could be used to verify or identify users implicitly and continuously on smartphones. The authentication systems that have been built based on these behavioral biometric traits are known as active or continuous authentication systems.

This paper provides a review of the active authentication systems. We present the components and the operating process of the active authentication systems in general, followed by an overview of the state-of-the-art behavioral biometric traits that used to develop an active authentication systems and their evaluation on smartphones. We discuss the issues, strengths and limitations that associated with each behavioral biometric trait. Also, we introduce a comparative summary between them. Finally, challenges and open research problems are presented in this research field.

1. Introduction

With the diversity of sensors and services on smartphone as shown in Fig. 1, the smartphone became more smarter and attracts both (1) users who enjoy using it to facilitate their daily life more than ever before, consequently they store more sensitive and private information on it, and (2) attackers who pay more attention to access or steal these sensitive data. These attacks could be done by either **insider attacker**, someone who know the user such as friend or family member or **stranger attacker**, someone who does not know the user [2].

Due to the weaknesses of the traditional authentication mechanisms such as PIN, Pattern and Password, and the biometric based mechanisms such as fingerprint, face and voice recognition on smartphones, the research community have developed authentication mechanisms based on behavioral biometric traits such as gesture, keystroke and gait. These mechanisms are known as active or continuous authentication mechanisms.

In this paper we present the components and the operating process of the active authentication mechanisms in general, followed by some different metrics that used to evaluate the performance of an active authentication mechanisms. We also conducted an extensive survey of the state-of-the-art active authentication systems and their evaluation on smartphones. We discuss the issues, strengths and limitations that associated with each behavioral biometric trait, and introduce a comparative analysis between them. Finally, we identify challenges, open research problems and provide a set of recommendations in this research field.

The rest of the paper is organized as follows: Section 3 provides an overview of active authentication systems in general. Section 4 presents a set of factors that facilitate the selection of a behavioral biometric trait. Section 5 presents another set of factors that help in the designing process of the biometric authentication system. Section 6 surveys the common behavioral biometric traits. Section 8 presents some limitations and followed by set of challenges and future trends.

2. Adversary attacks

The main goal of attackers is to gain physical access to the victim's device for snooping or data destruction. These attacks could be done by either **insider attacker** or **stranger attacker** [2].

Insider attacker, someone who know the user such as friend or family member. The insider attacker has opportunity to have unauthorized access to the victim's device due to the proximity between them. Based on a previous research done by Usmani et al. [3] where they characterized the social insider attacks and found that the existing devices (i.e., which use the traditional authenti-

* Corresponding author.
E-mail addresses: e.ahmedmahfouz@mu.edu.eg (A. Mahfouz), d.tarek@mu.edu.eg (T.M. Mahmoud).

https://doi.org/10.1016/j.jisa.2017.10.002
2214-2126/

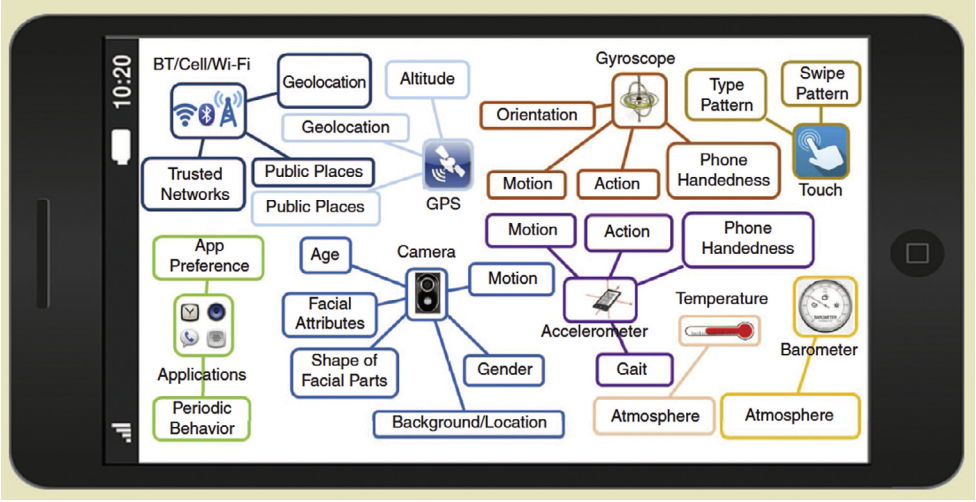

Fig. 1. Sensors, services and devices in smartphones that could be used to make a person recognition based on physiological and behavioral traits [1].

cation methods such as Pattern or Password) and the Facebook account security measures are ineffective to resist social insider attacks.

Stranger attacker, someone who does not know the user. The stranger attacker has no prior knowledge about the victim, who may steal the legitimate user's device or found a lost device.

3. The active authentication

In this section we define what is an active authentication and show an overview on how does the active authentication system work, followed by its modes of operation. Finally, we present different metrics that have been used to evaluate the performance of active authentication systems.

3.1. What is an active authentication system?

Active authentication system is an automated recognition process that verifies or identify individuals based on detailed information about their body such as face or their behaviors such as how they type or interact with some sensors on smartphone. Fig. 1 shows some sensors and services that can be used to acquire behavioral biometric data. The main goal of the recognition process is to prevent the unauthorized access from imposters and grant access only for legitimate user. The idea behind the recognition process in active authentication system is to establish an identity based on **who you are?** concept. The details of how recognition process work based on a specific biometric trait will be described in the next section.

There are two important characteristics that should be achieved by any active authentication system which are as follows:

- **Continuity**: A smartphone verifying user in a continuous manner, where the authentication system keep authenticating users as long as the user uses the smartphone. In other words, it is a re-authentication process that conducts periodically.
- **Transparency**: All authentication processes should be carried out in the background without interrupting the user (i.e., user will be implicitly authenticated without any intervention).

The two aforementioned characteristics are representing the cornerstone of any active authentication system, which make it different than the traditional authentication system. There are different biometric techniques could be used to achieve these characteristics. These techniques are categorized into two groups, physiological biometric mechanisms such as face and voice recognition, and behavioral biometric mechanisms such as touch and keystroke dynamics. In this paper we concentrate on surveying the behavioral biometric ones.

3.2. How does the active authentication system work?

The active authentication system works similarly like the biometric recognition system, which contains two main phases, enrolment phase and recognition phase as shown in Fig. 2. In the enrolment phase, the system acquires the biometric data, analyzes this data and extracts a distinctive features set, then it builds the feature templates (e.g., like the training process for a classifier). In the recognition phase, the system, similarly, acquires biometric data and extracts features, but instead of storing these features in the feature templates, it compares it with the stored one to verify the user identity.

There is a set of basic modules should be included in any active authentication system in general which are as follows:

1. **Data acquisition module**: it is the first step in the system where the raw biometric data is collected by one of the sensors in the smartphone such as camera or touchscreen sensor (see Fig. 1). The quality of the collected data is very important because it will affect on the successor modules of the recognition process. The quality of data is impacted by the used sensors and the environment in which the data was collected [4].
2. **Feature extraction module**: before extracting the distinctive features, the raw data has to be preprocessed, detect and remove outliers, improve the data quality, especially if the data collected in an uncontrolled environment with uncooperative users. Then, once the data is cleaned and processed, set of discriminative features are extracted. The extracted features depend on the type of raw data, for example if the collected data contains timestamps, temporal feature could be extracted.
3. **Feature templates**: it is a repository database that contains a concatenation of the extracted feature vectors for a specific user (i.e., device owner). It is built during the enrollment phase and used during the recognition phase to be compared with the captured feature sample to verify the claimed identity.
4. **Matching and decision-making module**: it used only during the recognition process, where it compares the extracted features against the stored feature templates to generate a matching score to make a decision. The decision validates the claimed identity to see it is done by legitimate user or imposter.