Journal of Information Security and Applications 40 (2018) 63–77

Contents lists available at ScienceDirect

Journal of Information Security and Applications

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

A continuous combination of security & forensics for mobile devices

Soumik Mondal*, Patrick Bours

Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Norway

ARTICLE INFO

Article history:

Keywords:
Continuous authentication
Continuous identification
Pairwise user coupling
Behavioral biometrics
Mobile devices
Security and forensics

ABSTRACT

In this research, we introduce the concept of adversary identification in combination with continuous authentication. To protect the system from session hijacking, it is important to not only use the traditional access control at the beginning of a session but also continuously monitor the entire session whether the present user is still the legitimate user or not. In case an impostor is detected, the system should lock to avoid loss or disclosure of personal or confidential information. In many cases, it will be important to not only secure the system but also establish the identity of the impostor which could be seen as a deterrence measure or could be used as a shred of evidence in the court. This concept has not been introduced in this manner before, and it combines security and forensics continuously.

We have performed a closed-set and an open-set experiment to validate our proof of concept with two different publicly available mobile biometrics datasets. Depending upon the dataset and used settings, we show that the adversary can be correctly identified with 82.2% to 97.9% of the attack cases for closed-set experiment and for the open-set experiment this performance ranges from 73.8% to 77.6%.

1. Introduction

Technological advances in mobile devices make people dependent on such devices day by day. Nowadays mobile devices (*i.e.* smart-phone or tablet) can be treated as a pocket computing device, and people are using it for financial transactions, email, health monitoring and social networking. Therefore these devices contain highly sensitive and private information. Securing these devices from illegitimate access to such information is one of the primary concerns for the security research community.

State of the art access control on mobile devices is implemented as a one-time proof of identity (*i.e.* password, pattern lock, face or fingerprint) during the initial login procedure, where the legitimacy of the user is assumed to be the same during the full session [7,8,10,19,28]. Unfortunately, if the device is left unlocked and unattended, any person can have access to the same information as the legitimate user. This type of access control is referred to as static authentication or static login. On the other hand, we have continuous authentication where the genuineness of a user is continuously monitored based on the biometric signature present on the device to protect the device from session hijacking. When doubt arises about the authenticity of the current user, the system can lock, and the user has to revert to the static authentication access control mechanism to be allowed to continue working. Continuous authentication is not an alternative security solution for static authentication; it provides an added security measure alongside static access control.

In most cases, it is important to detect if the current user is the legitimate user or an impostor user, but in some cases, it could also be interesting to establish the identity of the impostor user when detected. An example where identification can be useful is in an online user forum. Here it could be used to identify a person posting anonymous yet offensive or criminal comments, or posting comments under the name of someone else, *e.g.* after getting access to the account of the other person. In our research, we are not only looking at the *Continuous Authentication (CA)* where the system checks if the current user is the genuine user or not, but also at *Continuous Identification (CI)* where the system tries to establish the identity of the current user if he or she is known to the system. During our research we address two questions:

- CA: Is an impostor currently using the system?
- CI: If an impostor is currently using the system (detected by the CA system), then who is this impostor?

The primary motivation of this research is to unveil the identity of an impostor once the system has detected that an impostor is using the system. Fig. 1, shows the system pipeline of our proposed architecture. It is divided into two major subsystems (see Fig. 1 with the dotted lines), *i.e.* the *Continuous Authentication System (CAS)* and the *Continuous Identification System (CIS)*. In Fig. 1, after successfully providing the credentials for the static login the user is accepted as genuine and obtains the permission to use the

* Corresponding author at:
E-mail addresses: mondal_soumik@sutd.edu.sg (S. Mondal), patrick.bours@ntnu.no (P. Bours).

https://doi.org/10.1016/j.jisa.2018.03.001
2214-2126/

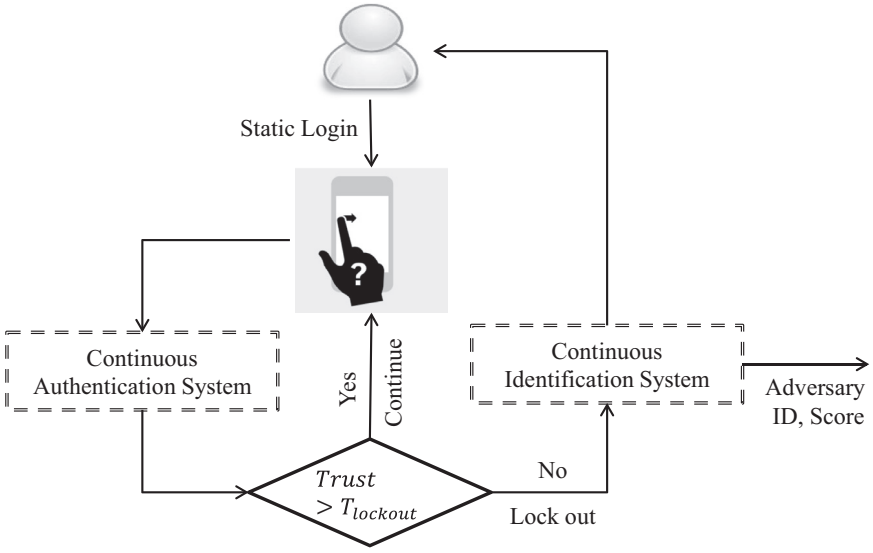

Fig. 1. Block diagram representation of our proposed system.

device. During the usage of the device, the behavioral dynamics of the each and every activity (*i.e.* swipe action or key tapping) performed by the user is compared with the stored profile by the CAS and returns the current system *Trust* on the genuineness of the user. The *Trust* values are used in the decision module where it is compared with a predefined threshold ($T_{lockout}$) to determine whether the user can continue to use the device or, if the trust is too low (*i.e.* our system feels that the device is operated by an impostor user), the device will be locked. After detecting that the present user is an impostor (*i.e.* $Trust < T_{lockout}$), all the performed actions done by the current user are used by the CIS to try to establish the identity of the impostor from a known/semi-known user database and return to the static login part of the system.

The remainder of this paper is organized as follows. In Section 2, we will discuss some background details related to this research. The description of the CAS and CIS can be found in Sections 3 and 4. The experimental protocols followed in this research, and the system performance measure are described in Section 5. In Section 6, we discuss the results obtained from our research. In Section 7, we discuss some of the significant findings from this research and present a comparison with previous research. Finally, we conclude our paper in Section 8.

2. Background knowledge

2.1. Related research on CA

Research on CA started in 1995 when Shepherd [30] and later Monrose et al. [23] showed some impressive results on CA using *Keystroke Dynamics (KD)* on a computer. Later on, researchers have introduced *Mouse Dynamics (MD)* [11,24] and also the combination of KD and MD for CA on computers [1,3,22,32]. Researchers also tried to mitigate the lower performance of behavioral biometrics (*i.e.* KD and MD) based CA by using biological biometrics like face or fingerprint but were confronted with other challenges, *e.g.* environmental constraint, user-friendliness, computational overhead, and the extra hardware required [25,31].

Nowadays CA systems for mobile devices are also studied and show some encouraging results that could be used as a motivation for further studies in this domain [16,26]. Table 1 shows the state-of-the-art research in the CA domain on mobile devices. Some of these papers have used KD based CA (*i.e.* tapping behavior) [13,27] but most of them have used swipe gesture behavior for CA [5,12,14,15,28,29,36]. We can also find the combination of tapping and the swipe gesture for CA [18]. Except for [12], all the other experiments were conducted in a controlled setting. We can also find the use of face biometrics for CA on mobile devices [9,35].

All of the above research was implemented as a periodic authentication, where the system will re-authenticate the user after a block of a predefined fixed number of activities or a pre-set fixed time interval. Therefore, even if the system can achieve 0% EER, the impostor user always gets a specific amount of activity or time to cause damage on the device. In our research, we will focus on actual CA where each action is immediately taken into consideration to determine if the current user is genuine or not. Our contribution in this paper is not so much in CA but instead in CI, where we are more interested in identifying the current user after he/she is locked out by the CA system. Since CI has been introduced first time in the research, we are unable to find related research in this domain.

2.2. Classifier(s)

We have used a machine learning based approach during the analysis. More precisely, we have used *Artificial Neural Network (ANN), Counter-Propagation ANN (CPANN)* and *Support Vector Machine (SVM)* classifiers in our research. We have also used *Multi-Classifier Fusion (MCF)* with a score fusion technique to obtain the better performance than for a single classifier [17].

2.3. Data description

In our research, we have used two publicly available datasets for the analysis [2,14]. The detail description of these datasets is given below.

2.3.1. Dataset - 1

A client-server application was deployed to eight different Android mobile devices (screen resolutions ranging from 320×480 to 1080×1205) for data collection, and the swipe gesture data was collected from 71 volunteers (56 male and 15 female with ages ranging from 19 to 47). Each volunteer has provided an average of 202 swipe actions. To the best of our knowledge, this dataset contains the largest number of users compared to other publicly