A Transparent and Continuous Biometric Authentication Framework for User-Friendly Secure Mobile Environments

Muhammad Muaaz
University of Applied Sciences
Softwarepark 11
A-4232, Hagenberg, Austria
muhammad.muaaz@usmile.at

Abstract

Personal mobile devices (PMDs) have become ubiquitous technology. Their, steadily increasing computational and storage capabilities have enabled them to offer an increasingly large set of services. Considering their significance, it's necessary to ensure that they aren't misused. Unfortunately, a less effective and inconvenient PIN based authentication system is used to protect them against their misuse. Therefore, we propose a continuous and transparent multi-modal biometric authentication system for PMDs. This authentication system is based on gait, 3D-face and voice recognition. It requires minimal to no interaction from users for identity verification to maintain a transparent confidence level of identity throughout its period of use. Further, one of the more stable biometric traits will be used for extracting fuzzy crypto keys to encrypt and decrypt sensitive information stored on the internal or external memory of the PMD.

Author Keywords

Biometric, authentication, machine learning, gait recognition, fuzzy crypto

ACM Classification Keywords

D.4.6 [Security and Protection]: Authentication, Cryptographic controls; H.1.2 [User/Machine Systems]: Human factors.

UbiComp '13 Adjunct, Sept 8-12, 2013, Zurich, Switzerland.
ACM 978-1-4503-2139-6/13/09...$15.00.

An Overview of the User-Friendly Secure Mobile Environments Project

Rapidly increasing computational and storage capabilities of Personal Mobile Devices (PMDs) are widening their use on the personal and business front as they are offering a large array of services. The *'Bring your own device' (BYOD)* trend demands enhanced security of PMDs as consumers are not only using them for making calls and text messages, but also for accessing wireless local area networks to corporate data network services, and from social, entertainment applications to financial and mobile payment applications. However, many of these services either offer low security in terms of standard requirements of confidentiality, integrity, availability, auditability and privacy for end users, or are too complicated to set up by typical end users. The vision of the *User-friendly Secure Mobile Environments (u'smile)* project [2] is to overcome these challenges in security and usability to offer a potential future applications towards even better mobility and convergence of devices and end-user services.

Introduction

Identification and verification is considered as first line of defence of every secure system. The ubiquitous nature of PMDs has not only opened doors to access multitude of services but also greater mobility. Unfortunately, mobility has an associated risk that PMDs can easily be left unattended, lost or become facile target of theft. To offer enhanced end user security, it is important to ensure that PMDs are secured with more intuitive authentication system. If illegitimate persons get their hands on someone's PMD, they should not be able to access private and business related information.

Most of current PMDs are secured with a Personal Identification Number (PIN) based authentication system with different complexity levels or graphical ways of entering the PIN. Studies have shown that a PIN based authentication system is less effective and indeed inconvenient too [6]. Therefore, a majority of PMD users don't use this authentication system. With no or little authentication effort required, an attacker can analyze data and use stored passwords to access emails and private information.

Therefore, it is absolutely necessary to ensure that a PMD is under continuous control of a legitimate person. This imposes a strong need of developing such authentication mechanisms which provide efficient identity verification, beyond the point of entry. With the key objective of not only providing robust security with minimal effort, a continuous and non intrusive authentication system also maintains a continuous confidence level of an identity. Identity with a high confidence level is provided with automatic access to the sensitive information. If the confidence level is low then access to sensitive services is denied [6]. Continuous authentication may solve privacy risks associated with lending PMD to someone else.

Various authentication systems have been developed for PMDs to enhance end user security such as, locimetric, drawmetric, cognometric, fingerprints, speaker, and face recognition [5]. Biometric authentication is acknowledged as more intuitive authentication system over PIN or token based authentication systems. Biometric characteristics are unique, can't be transferred to others, unforgettable and difficult to reproduce and hide. This makes them more suitable for PMDs [6]. Its difficult steal biometric characteristics at first place, but once stolen its really difficult for the owner to change it. Multi-modal biometric system could be an approach against such attacks on biometrics. Also, a single biometric technique can't be adapted for all users and scenarios [6]. Considering the trade-off between usability and security, we therefore, propose a multi-modal biometric authentication framework, which utilizes three biometric techniques for identity verification of individuals in a continuous and transparent fashion. The scope of this research is to analyze the possibilities of and develop a generic transparent and continuous user-friendly framework for user authentication on PMDs using the following biometric techniques:

- Implicit gait recognition using built-in phone sensors of PMDs such as, accelerometer, gyroscope, and magnetometer
- 3D-face recognition using the built-in camera
- Voice recognition using built-in microphones

The secondary goal of this research is to extract fuzzy cryptographic keys from one of the more stable biometric templates in order to encrypt and decrypt highly sensitive data stored on the devices.

Research Questions

In the prospect of this research topic, we are responsible for evaluating biometric gait authentication and developing a generic continuous and transparent authentication framework for PMDs. The work on 3D-face and speaker recognition is being carried out by other colleagues involved in this project. In order to achieve our research goals following research questions will be answered:

- How it is possible to achieve a fully transparent and continuous authentication framework for PMDs using gait, 3D-face, and voice as biometric techniques?
- What are the possible ways of combining different available (gait, 3D-face and voice) authentication mechanisms depending on user and application context (activity, spatial, temporal, and social)?
- What are the possible ways of assigning different confidence levels to different applications?
- Which authentication mechanism (gait, 3D-face, and speaker) is effective and suitable for extracting fuzzy crypto keys towards transparent on-device encryption?
- What are the hardware requirements in order to deploy such a framework? (most importantly, battery runtime)
- What are the constraints for gait authentication to be continuous and transparent considering the factors influencing gait recognition mentioned in the literature?
- How many models are necessary to perform gait authentication for a large percentage of the population, considering different activities(e.g. walking speeds and surfaces) and factors (e.g. position and orientation of the phone, shoes, and clothing) affecting gait?
- Are there any circumstances under which gait of two different persons become somehow identical?

Current Status and Outlook

We have conducted an extensive literature study on various approaches to gait recognition. Since, the idea of using biometric authentication for mobile devices is not new. C.Nickel [5] and M.O.Derawi [4] have studied the feasibility of gait recognition as an alternative authentication mechanism for mobile devices. Crawford [3] has studied keystroke dynamics and speaker recognition to achieve continuous and transparent authentication framework. The MOBIO project [1] team has evaluated different face and speaker recognition systems on a database collected using camera and microphone of PMDs. In order to answer research questions raised for this research work, we have developed a data recording application for the Android platform to record gait data and PMD orientation using accelerometer, gyroscope, and magnetometer. Currently, we are in the process of extracting various features from gait data and evaluating different machine learning options. Later, we will be implementing a demonstrator using the best-performing classifiers in terms of accuracy and time taken by classifiers to learn. Then we will start integrating gait and 3D-face with a more abstract user authentication framework.

Objectives

My main objective of attending UBICOMP doctoral school is to establish contacts with other researchers working in and around this research domain. This would give me an opportunity to learn from experts and fellow researchers. Feedback on research goals, research methodology and technical details from domain experts will definitely help me to better frame this research work.

Acknowledgements

We gratefully acknowledge funding and support by the Christian Doppler Gesellschaft, A1 Telekom Austria AG, Drei-Banken-EDV GmbH, LG Nexera Business Solutions AG, and NXP Semiconductors Austria GmbH.

References

[1] Welcome to mobio (mobile biometry). http://www.mobioproject.org/.

[2] Welcome to the u'smile project. http://www.usmile.at/.

[3] Crawford, H. A. *A Framework for Continuous, Transparent Authentication on Mobile Devices*. PhD thesis, University of Glasgow, December 2012.

[4] Derawi, M. O. *Smartphones and Biometrics: Gait and Activity Recognition*. PhD thesis, Gjøvik University College, November 2012.

[5] Nickel, C. *Accelerometer-based Biometric Gait Recognition for Authentication on Smartphones*. PhD thesis, TU Darmstadt, June 2012.

[6] Saevanee, H., Clarke, N., and Furnell, S. Multi-modal behavioural biometric authentication for mobile devices. In *Information Security and Privacy Research*, D. Gritzalis, S. Furnell, and M. Theoharidou, Eds., vol. 376 of *IFIP Advances in Information and Communication Technology*. Springer Berlin Heidelberg, 2012, 465–474.

Muhammad Muaaz received his Master of Science in Information and Communication Systems Security from KTH University, Sweden in 2012. Since March 2013, he is enrolled in the PhD program at Johannes Kepler University, Austria. His main research interests are authentication systems, biometrics and machine learning. His dissertation supervisors are: **René Mayrhofer**, professor at University of Applied Sciences Upper Austria, and **Josef Scharinger**, professor at Johannes Kepler University Linz. Expected date of completion is by the end of 2016.