Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 127 (2018) 379–387

Procedia Computer Science

www.elsevier.com/locate/procedia

The First International Conference On Intelligent Computing in Data Sciences

A Context-Aware Authentication System for Mobile Cloud Computing

Kamal Benzekki[a,*], Abdeslam El Fergougui[a], Abdelbaki ElBelrhiti ElAlaoui[a]

[a] *Laboratory of Computer Networks and Systems, Faculty of sciences, Moulay Ismail University, Meknes, Morocco*

Abstract

Context-aware authentication systems are becoming more and more interesting, as mobile devices are using pervasive computing environments. They can be implemented in different ways and ensure secure authentication by analyzing the user behavior from his device. Context-aware authentication systems add an additional security layer when implemented in conjunction with the password-based authentication methods. Also, they can replace, in some scenarios, the conventional authentication methods. In this paper, we propose a practical context-aware authentication system which is cost-effective and easy to implement. The environmental information is only sent when the user makes an authentication request which renders our system more practical and lightweight. However, the authentication request goes through different steps in order to make a decision regarding the access.

Keywords: Authentication; Mobile Cloud Computing; Context-Awareness; Pervasive Computing

1. Introduction

Smartphones and tablets have become ubiquitous in our daily lives and quickly gained in usage and popularity, more consumers are relying on these devices, as their primary source of internet access. Smartphone devices are characterized by convenient features, such as operating systems that can enable users not only to navigate, but also to interact with applications (e.g., playing games, chatting, recording videos and taking pictures). At the same time, continued and rapid increase of online applications and secure cloud services [1] results in an increase in demand for authentication.

Authentication plays an important role [2] in how we interact with computers, mobile devices, the web, etc. For example, in recent years, more corporate information and applications have been accessible via the Internet and Intranet. Several employees are working from different distant spots and require entry to protected corporate files. In the meantime, it is possible for malicious/unauthorized users to get access to the system. For this particular cause, it is rational to possess some mechanism in place to discover whether the particular logged-in user is the exact same user in control

[*] Corresponding author. Tel.: +212-625-13-13-70
E-mail address: benzekki@gmail.com

10.1016/j.procs.2018.01.135

of the session.

Conventional authentication via password input [3] in addition to strong authentication by means of usage of a second factor (e. g., a SecureID token) both fall short in the particular case of authentication on mobile gadgets (e.g.,Smartphones), exactly where devices constraints and consumer perspective need even more integrated, hassle-free, but secure experience. Password-based authentication may withstand brute force plus dictionary attacks when users pick strong passwords with sufficient entropy[4]. Nevertheless, password-based user authentication suffers from a significant issue that human beings are not really specialists in memorizing textual content.

Typically the context-aware authentication is usually a good approach that makes use of findings of user habits with regard to authentication. Considering that individuals are usually creatures of routines, a person would go to work in the early morning, possibly having a stop at a particular coffee shop, yet practically usually using exact same path and connect from these places. Once at work, he may remain inside the common vicinity of his office building right up until lunch break. Within the mid-day, maybe he phone calls home and picks up his kid coming from school. Later in the day, this individual moves home besides making interactions by way of multimedia application such as Facebook, Whatsapp, Snapchat, Instagram, Viber,etc.. Throughout the day time, he checks his different e-mail accounts. Possibly he also uses online banking service and frequently relies on mobile phone to access away from home. Weekly visits to the grocery store and connecting from different places, etc.. are almost all rich details that might be obtained and noted almost completely using smartphones.

With the migration of users into pervasive computing, mobile devices begin to interact with the cloud through multimedia applications and producing additional data. This set of data and information that is collected daily defines a profile that works as a reliable criterion for authenticating users.

The remainder of this paper is organized as follows. In section II we present the related works. Section III suggests our proposed context-aware authentication system and details the components of the system. An evaluation of our system is given in Section IV. Finally, Section V concludes this paper.

2. Related Works

Several context-aware authentication systems have been presented in the large body of literature which propose to verify the authenticity of a user authentication request by considering contextual information characterizing the user behavior and environment.

Shi et al. [5] present an implicit authentication system which records user's routine tasks and habits such as making phone calls or visiting places in similar periods of time, then builds a profile for each user characterizing his behavior. For the first time, the system goes through a learning phase where past user's behavior that characterizes the behavioral patterns is collected and then learned as a user model. Based on this user model and some recent perceived user behaviors we can make a comparison to decide whether the authentication is allowed or not. The comparison is depending on a probability value that reflects an authentication score which increases or decreases according to new observed behaviors. Habitual events and usual tasks are judged as positive events that augment the score. When the score decreases and falls below a predefined threshold the user is prompted to authenticate explicitly.

Sathish and Venkataram [6] propose an authentication scheme based on mobile transaction called TBAS (Transaction-Based Authentication Scheme), which operates on the application level to classify the user behavior and transactions' sensitivity with the help of intelligent agents for perceiving information in the environment and reasoning about these perceptions. The TBAS uses Mobile Cognitive Agents (MCA) to collect information about the user behaviors, and static agents (SCA) for identifying transactions' sensitivity and for determining the adequate authentication process depending on the security level needed.

Witte et al. [7] propose a context-aware mobile biometric system based on Support Vector Machine (SVM) for learning and evaluating the collected contextual information which is captured by observing behavioral biometric features (e.g. speech patterns, online signatures, keystroke dynamics, face recognition, etc.) from a range of active and passive sensors. Furthermore, environmental conditions are also considered in order to construct a subject-specific context model, as they can directly affect the biometric features. For instance, a rather dark environment may reduce the reliability of face recognition; a human injury may disable functionality or feature. The system gathers a large size of contextual information and processes it in order to build an accurate user model. A training phase follows the processing where the data set describing the current context is classified according to a probabilistic model.