Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 85 (2016) 293 – 300

Procedia Computer Science

International Conference on Computational Modeling and Security (CMS 2016)

A Novel Strong Password Generator for Improving Cloud Authentication

Abderrahim Abdellaoui[a,*], Younes Idrissi Khamlichi[b], Habiba Chaoui[a]

[a]*Systems Engineering Laboratory, ADSI Team, ENSA Kénitra, Ibn Tofail University, Morocco*
[b]*Systems Engineering Laboratory, UMBA University, ENSA Fes, Morocco*

Abstract

In recent years, there has been a growing interest in the cloud computing paradigm thanks to its benefits, such as multi-tenancy, scalability, cost efficiency and its unlimited storage. However, like any new technology, there are still a number of challenges relevant to this paradigm and most notably user authentication. In order to achieve better security than the alphanumerical password, this paper describes a scheme which allows strengthening the authentication process in the cloud environment using the password generator module by means of a combination of different techniques such as multi-factor authentication, One-time password and SHA1.

Keywords: Security Cloud Computing; One-time password; Multi-factor Authentication;

1. Introduction

As Cloud computing is gaining more popularity in the recent years, more and more organizations are attracted by its characteristics (On-demand self-service, Broad network access, Resource pooling, Rapid elasticity, Measured service(1)) and advantages such as business ease and financial saving. Thus, these organizations attempt to shift to

* Corresponding author. Tel.: +212-6-53287057;
E-mail address: abderrahim90@gmail.com.

doi:10.1016/j.procs.2016.05.236

the cloud infrastructure in order to exploit its advantages. Cloud computing is an automated technology service, which deliver in addition to networking and storage, customer relationship management. It is an economic model based on a hugely scalable IT platform (Data Center) to reduce the cost of provisioning, operating and de-operating its resources. This concept is very cost efficient and it provides access to almost unlimited storage. However, some recent developments in cloud computing have heightened the need for promoting the security in this environment from a different security perspective (authentication, confidentiality, integrity, non-repudiation, availability), particularly cloud authentication. In fact, the safety and security of sensitive user data and applications in the cloud environment relies primarily on user authentication. As a matter of fact, the authentication feature is one of the most important security characteristics of whatever system, particularly, the cloud system. It enables verifying the legitimacy of the users before accessing to cloud resources. There are many authentication schemes that have been proposed in recent years following different approaches, specifically, we can distinguish, text password, multi-factor authentication, 3D password, third party authentication, biometric scans and graphical password. Furthermore, it has been recently shown that text-based password is the most used method among the previously cited methods. However, according to many research studies (4-10, 12, 15, 20, 21), due to its vulnerabilities such as dictionary and brute-force attacks, key-loggers, shoulder surfing and social engineering, the text-based password scheme remains a quite weak authentication method for the cloud environment even if its ease of use.

This paper introduces a new authentication scheme based on the one-time password and two-factor authentication. The aim of this scheme is to strengthen the authentication process in the cloud environment, using the password generator module. The second section presents some works related to the authentication techniques that enhance the process of authentication in the cloud. Section 3, describes the key concepts and introduces a prototype of our scheme. Section 4 provides the security analysis details about PassGen scheme. Finally, a conclusion is given with, eventually, some perspectives for further works.

2. Related works

A variety of methods have been proposed in the literature to overcome the problem of weak user authentication. Each one has its advantages and drawbacks. In 1981, Leslie Lamport (2) introduced his first remote user authentication method based on one-way hash encryption function and a password table. However, despite its ease of use, the scheme suffers from some weaknesses such as high hash overhead and the necessity to store the password table (3). Other researchers emphasize on the concept of smart card to overcome the weak user authentication problem. Hwang et al (4), presented a scheme in which they combine smart card and third party authentication to achieve a single sign-on authentication in an inter-cloud service. Several smart-card methods have been proposed in the literature, particularly, Tsaur et al.(5), Hwang et al.(6), Choudhury et al. (7), Jaidhar (8), however, these approaches require special tools such as a smart card reader for the authentication process. The second category of approaches is multifactor authentication, Yassin et al (9), proposed a scheme that combines two-factor authentication (2FA), RSA digital signature and One-Time Password (OTP) in the cloud computing using asymmetric scalar-product preserving encryption (ASPE) and RSA digital signature as two-factors. The scheme introduced three main steps: setup, registration and the authentication phase. The user performs the Setup and Registration phase only once, whereas the authentication phase is done whenever the user access to the cloud. This scheme does not require extra devices such as token device, a card reader in a smart card system and scanner in physiological biometrics. However, they have not treated password update in much detail. Another concept of enhancing authentication is biometric scans, by way of illustration, Jivanadham et al (10), proposes a two levels of authentication called the Cloud Cognitive Authenticator (CCA). It is an API, integrating bio-signals and one round Zero Knowledge Protocol (ZKP) for authentication. It uses Electro Dermal Responses (EDR) for the first level authentication. The main weakness of this scheme is the requirement of an extra device for the authentication. CCA uses data captured from an EDR biometric scanner when the users want to access the cloud services. One of the most important alternatives of the login/password scheme is graphical passwords, this technique consists of clicking on a set of images instead of using an alphanumeric password. By means of example, Shi et al. (11), introduced a scheme in which users choose and memorize the locations of passwords for each n × n squares, then, they enter the numbers corresponding to the locations in each randomly generated square. One major drawback of this scheme is, it cannot resist strong shoulder-surfing attack. In this section we have introduced some significant approaches