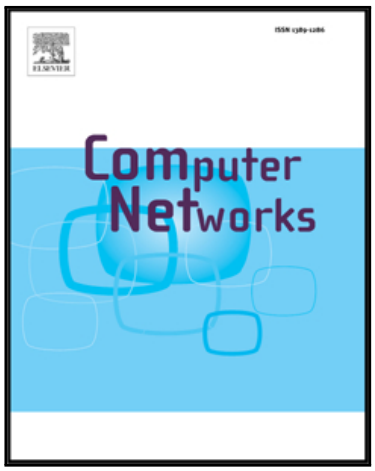
Accepted Manuscript



A new two-server authentication and key agreement protocol for accessing secure cloud services

Durbadal Chattaraj, Monalisa Sarma, Ashok Kumar Das

PII: S1389-1286(17)30425-5
DOI: 10.1016/j.comnet.2017.12.007
Reference: COMPNW 6341

To appear in: *Computer Networks*

Received date: 30 April 2017
Revised date: 27 October 2017
Accepted date: 19 December 2017

Please cite this article as: Durbadal Chattaraj, Monalisa Sarma, Ashok Kumar Das, A new two-server authentication and key agreement protocol for accessing secure cloud services, *Computer Networks* (2017), doi: 10.1016/j.comnet.2017.12.007

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

ACCEPTED MANUSCRIPT

A new two-server authentication and key agreement protocol for accessing secure cloud services

Durbadal Chattaraj[a,*], Monalisa Sarma[a], Ashok Kumar Das[b]

[a]Subir Chowdhury School of Quality and Reliability, Indian Institute of Technology, Kharagpur 721 302, India

[b]Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500 032, India

Abstract

Emerging Cloud computing paradigm came up with the on-demand ubiquitous service sharing facility via the Internet. In this synergy, the cloud service providers provide various services, namely, Infrastructure as a Service (*IaaS*), Platform as a Service (*PaaS*) and Software as a Service (*SaaS*) to their clients. In such a provision, both the end parties demand proper auditing so that the resources can be legitimately utilized, and meanwhile the privacy is also preserved. In order to achieve this goal, there is a need for designing an efficient and robust authentication mechanism. Though other existing authentication protocols, such as Kerberos, Open Authorization (OAuth) and OpenID are proposed in the literature, they are vulnerable to various security threats such as replay, online dictionary, offline dictionary, stolen-verifier, impersonation, denial-of-service, privileged-insider and man-in-the-middle attacks. In this paper, we aim to propose an authentication protocol which overcomes these security loopholes in the existing protocols. In the proposed protocol, a new dynamic password-based two-server authentication and key exchange mechanism is proposed with the help of both public and private key cryptography. Moreover, to achieve strong user anonymity property, a new multi-factor authentication scheme with identity preservation has been also introduced. The security analysis using both the formal security using the broadly-accepted Real-Or-Random (ROR) model and the informal security show that the proposed protocol protects several well-known attacks. In addition, the formal security verification using the widely-used Automated Validation of Internet Security Protocols and Applications (AVISPA) ensures that the scheme is resilient against replay as well as man-in-the-middle attacks. Finally, the performance study contemplates that the overheads incurred in the protocol is reasonable and comparable to that of other existing state-of-art authentication protocols. High security along with comparable overheads make the proposed protocol to be robust and practical for a secure access to the cloud services.

Keywords: Cloud computing, Authentication, Key agreement, Cloud data security, Security, AVISPA

1. Introduction

With the growing trend of Cloud services (e.g., SaaS, IaaS, PaaS), it has been predicted that the annual global data traffic will reach to 10.4 zettabytes per annum by the end of 2019, which is three times faster than 3.4 zettabytes yearly in 2014[1]. The report also indicates a huge success of the cloud technology, but there is a challenge too. In the cloud, a client remotely accesses his service provided by a service provider [1], [2], [3]. This leads to opening up a security problem as the communication takes place over insecure channel for accessing services. Towards this solution, a number of authentication protocols have been proposed in the literature, such as Kerberos[2], OAuth[3] and OpenID[4].

The existing state-of-the-art authentication protocols [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14] provide security in a distributed environment, and they follow a single server-based authentication mechanism. In order to achieve mutual authentication, all clients must interact with a particular authentication server. The single authentication server stores the credentials of all the principals in its database. Thus, this server is fully reachable for public access, and is also vulnerable to a number of attacks including dictionary attacks, password guessing attacks and stolen-verifier attacks [15], [16]. To mitigate these attacks, several schemes have been proposed [17], [18], [19], [20], [21], [22], [23], [24], [25], [26], [27], which are based on either smart card or PKI (Public-Key Infrastructure) based approach or even both. However, these approaches are less computationally intensive and expensive. Furthermore, the single server authentication model is susceptible to a single point of failure, that is, if the authentication server fails for any reason, the entire system will jeopardize. However, some approaches support replication and distribution of the authentication database to ensure the integrity of authentication server failure. Nevertheless, it results in an internal security breach and it has a costly solution[28]. To verify a user, the existing authentication mechanisms [4], [6], [29],

*Corresponding author

Email addresses: dchattaraj@iitkgp.ac.in (Durbadal Chattaraj[a,*]), monalisa@iitkgp.ac.in (Monalisa Sarma[a]), iitkgp.akdas@gmail.com, ashok.das@iiit.ac.in (Ashok Kumar Das[b])

[1]"Cisco Global Cloud Index: Forecast and Methodology 2014 to 2019 White Paper (http://www.cisco.com)"

[2]http://web.mit.edu/kerberos/

[3]http://www.oauth.net/

[4]http://openid.net/

Download English Version:

https://daneshyari.com/en/article/6882805

Download Persian Version:

https://daneshyari.com/article/6882805

Daneshyari.com