Accepted Manuscript

Anonymous biometrics-based authentication scheme with key distribution for mobile multi-server environment

Qi Feng, Debiao He, Sherali Zeadally, Huaqun Wang

PII: S0167-739X(17)30902-0
DOI: http://dx.doi.org/10.1016/j.future.2017.07.040
Reference: FUTURE 3570

To appear in: *Future Generation Computer Systems*

Received date : 4 May 2017
Revised date : 8 June 2017
Accepted date : 16 July 2017

Please cite this article as: Q. Feng, D. He, S. Zeadally, H. Wang, Anonymous biometrics-based authentication scheme with key distribution for mobile multi-server environment, *Future Generation Computer Systems* (2017), http://dx.doi.org/10.1016/j.future.2017.07.040

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

Anonymous Biometrics-based Authentication Scheme with Key Distribution for Mobile Multi-server Environment

Qi Feng

State Key Lab of Software Engineering, Computer School, Wuhan University, Wuhan,China

Debiao He*

State Key Lab of Software Engineering, Computer School, Wuhan University, Wuhan,China

Sherali Zeadally

College of Communication and Information, University of Kentucky, USA

Huaqun Wang

Jiangsu Key Laboratory of Big Data Security and Intelligent Processing, School of Computer School, Nangjing University of Posts and Telecommunications, Nanjing, China

Abstract

Significant advances in wireless communication technologies have led to the emergence and proliferation of a wide range of mobile devices and mobile services. However, the use of various cloud servers has made the traditional single-server architecture, where we have one server and many users, inefficient in terms of its performance. To address this drawback, multi-server architectures have been proposed. Password or smart card-based authentication schemes suffer from poor security in the multi-server environment and as a result biometrics have become a preferred choice for secure and robust authentication because of its close link with the physical characteristics of an individual. Recently Kumari and Li et al. proposed a biometrics-based authentication scheme for multi-server environment. However, we found that their scheme fails to meet user anonymity requirement and is vulnerable to several attacks. First, we describe

*Corresponding author
Email address: hedebiao@163.com (Debiao He*)

Download English Version:

https://daneshyari.com/en/article/6873123

Download Persian Version:

https://daneshyari.com/article/6873123

Daneshyari.com