International Journal of Innovative Computing, Information and Control
Volume **7**, Number **3**, March **2011**

ICIC International ©2011 ISSN 1349-4198
pp. 1443–1456

AN ID-BASED ACCESS CONTROL IN A HIERARCHICAL KEY MANAGEMENT FOR MOBILE AGENT

Chia-Hui Liu[1], Yu-Fang Chung[2], Tzer-Shyong Chen[3] and Sheng-De Wang[1]

[1]Electrical Engineering Department
National Taiwan University
No. 1, Sec. 4, Roosevelt Road, Taipei 10617, Taiwan
{ d96921027; sdwang }@ntu.edu.tw

[2]Electrical Engineering Department
[3]Information Management Department
Tunghai University
No. 181, Sec. 3, Zhonggang Road, Xitun District, Taichung 407, Taiwan
{ yfchung; arden }@thu.edu.tw

Received October 2009; revised March 2010

Abstract. *The related techniques and applications on e-commerce have been concerned by a great number of researchers. The use of a mobile agent, in particular, is an important breakthrough on the e-commerce applications. With the abilities of higher autonomy and mobility, a mobile agent can move freely among different execution environments, can automatically detect its resided environment, and can react itself accordingly. Besides, a mobile agent itself can complete the tasks assigned by the users. Because of these characteristics, a mobile agent becomes the most suitable application for e-commerce. However, it is always a risk to transfer confidential information over an open Internet environment. When a mobile agent roams itself among the servers over Internet or the mobile agents exchange information with each other, the users would concern whether the mobile agent was attacked by some manipulated servers or the carried confidential information is stolen or tampered by the others. All these worries make the safety of a mobile agent on the Internet be an important issue. Thus, this paper will propose a suitable and secure scheme for the mobile agent. The scheme, based on the bilinear pairing over elliptic curves, takes the concept of identity-based access control on a hierarchical key management. This paper also aims to increase improvements on the scheme presented by Volker and Mehrdad to resolve the problem of storage waste in their scheme because of storing the overlapping decryption keys of a mobile agent. From the results of the security and performance analysis in this paper, the proposed scheme is proven to protect the mobile agent in an efficient and secure way.*

Keywords: Mobile agent, Access control, Key management, Information security, Bilinear pairings

1. Introduction.

With the speedy development of the Internet, there is a growing demand on information sharing, information management, improvement of network efficiency and secure transmission. Therefore, more complex technologies for distribution systems are required because bulk information and data are transmitted forward and backward among numerous servers, which were spread out in an open network. Due to the great deal of data transferring in such an open distributed system, the problem of overloading transmission occurs. However, the present information management on facing toward a large and distributed network framework meets the problems such as dependability, expandability, interactivity and inelasticity. The development of mobile agents is the answer to these problems.