International Journal of Innovative Computing, Information and Control
Volume **6**, Number **5**, May **2010**

ICIC International ©2010 ISSN 1349-4198
pp. 2159–2170

A SECURE TIME-BOUND HIERARCHICAL KEY MANAGEMENT SCHEME BASED ON ECC FOR MOBILE AGENTS

Jen-Yan Huang[1], Yu-Fang Chung[2], Tzer-Shyong Chen[3] and I-En Liao[1]

[1]Department of Computer Science and Engineering
National Chung-Hsing University, Taiwan
matt@thu.edu.tw

[2]Department of Electrical Engineering
Tunghai University, Taiwan
yfchung@thu.edu.tw

[3]Department of Information Management
Tunghai University, Taiwan
arden@thu.edu.tw

Received October 2008; revised May 2009

Abstract. *The core competencies of a mobile agent include free-roaming between different environment and autonomous environment detection and simultaneous adaptation to environment. Because of these competencies, the concept of mobile agent is widely used in many different fields, such as the Internet business, wireless communication and information security technologies, etc. In 1983, Akl and Taylor [1] suggested the concept of superkey to resolve the key management issues faced by the mobile agent. Later in 1998, Volker and Mehrdad [2] proposed a hierarchical mobile agent model for access control. Our proposed paper would be based upon the studies of superkey and a hierarchical mobile agent model with Elliptic Curve Cryptosystem (ECC). ECC, with its shorter key length and better efficiency at encryption/decryption, enhances the mobile agent model. All related works are presented in Section 2 of this paper. Following the explanation of the background of our proposal, we present our proposal, which aims to resolve the key management issue found in Volker and Mehrdad's model. Time-bound key management is considered to be a good solution, because it can make the key management in the existing mobile agent model more convenient by distributing keys that has a validity period.*

Keywords: Mobile agent, Key management, Access control, Elliptic curve cryptosystem, Time-bound key management

1. **Introduction.** With the Internet and usage of personal computers being part of our daily lives, the general public are also now more aware of security issues regarding data transmission over the Internet, and looks for a secure way to transmit data. In this paper, the mobile agent, which possesses autonomous environment detection and adaptation, is integrated with hierarchical structure. With this hierarchical structure, each user will hold a different encryption key depending on their access rights. The encryption key will ensure that data is securely transmitted upon request. But when a user in the hierarchy logs out of the system, or changes the authority level for access, the system must cancel the previously assigned key so as to prevent illegal access of data. However, the above action of managing encryption keys require delegation of huge amount of resources and could slow down operations.

To resolve the issue above, this study attempts to apply time-bound key management scheme, whose concept in association with mobile agent is to prescribe a validity period