International Journal of Innovative Computing, Information and Control
Volume **4**, Number **9**, September **2008**

ICIC International ©2008 ISSN 1349-4198
pp. 2375–2389

EFFICIENT HIERARCHICAL KEY MANAGEMENT SCHEME FOR ACCESS CONTROL IN THE MOBILE AGENT

Yufang Chung[1], Tzershyong Chen[2] and Chiahui Liu[3]

[1]Department of Electrical Engineering
Department of Information Management
Tunghai University, Taichung, Taiwan
yfchung@thu.edu.tw

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

[3]Department of Electrical Engineering
National Taiwan University, Taiwan

Received August 2007; revised December 2007

Abstract. *The technologies applied to e-commerce have always been a widely discussed subject among researchers; mobile agent is one such technology and is considered to have great potential. It has high autonomy and mobility, that is, it can move unbridled in different execution environments and automatically detect its current environment and respond accordingly. The above qualities make the mobile agent very suitable for use in e-commerce. Transfer of confidential information over the Internet is always risky. A mobile agent may be tampered with by a malicious host, or confidential information carried by the mobile agent could be stolen by other agents. Thus, it is essential that a mobile agent is equipped with security measures to guard against these attacks. This paper proposes a security scheme for mobile agents. The scheme includes access control and key management to ensure the security and confidentiality of information and the system. After examining the access control and key management scheme for mobile agents proposed by Volker and Mehrdad, the proposed scheme applies the concepts of polynomial interpolation formula, hierarchy structure, and the superkey to improve Volker and Mehrdad's schemes which needed a large amount of space for the mobile agent. A security and performance analysis proves the proposed scheme can effectively protect the mobile agents.*

Keywords: Mobile agent, Access control, Key management, Information security, Polynomial interpolation formula

1. **Introduction.** The mobile agent, with its convenience, makes it a popular subject of research. Its technology is a subject widely discussed by academics. As a result, many mobile agent related products have been developed. For example, the mobile agent product developed by IBM and General Magic [16], which hopes to create a perfect mobile agent system. The mobile agent is an agent that is autonomous and migrates from host to host in diverse network environments. It can transmit messages, distribute resources, and interact with other mobile agents or distributed resource systems. The mobile agent accepts tasks assigned by the users, and move on to the Internet to platforms that provide related services to search or process information. When the mobile agent completes its task, it reports back to its user.