International Journal of Innovative
Computing, Information and Control
Volume **5**, Number **10(A)**, October **2009**

 ISSN 1349-4198
pp. 3241–3247

A PRACTICAL TIME BOUND HIERARCHICAL KEY SCHEME

Jiqiang Liu[1,2] and Sheng Zhong[2]

[1]Computer and Information Technology Department
Beijing Jiaotong University
Beijing 100044, P. R. China
jqliu@bjtu.edu.cn

[2]Computer Science and Engineering Department
State University of New York at Buffalo
Amherst NY 14260, USA
szhong@cse.buffalo.edu

Received April 2008; revised November 2008

Abstract. *In a complex information system, users and data are usually organized in a hierarchy structure for access control. Users in superior classes should be allowed to derive the secret keys belonging to subordinate classes. In this paper, we propose a new time bound hierarchy key assignment scheme to achieve this goal. Compared with the existing similar schemes, our scheme is more secure and needs less computational time. Furthermore, our scheme does not need tamper-resistant device, which makes our scheme much more practical.*
Keywords: Hierarchical key assignment, Time bound, Cryptography, Access control

1. **Introduction.** Just like the problems of quantum key distribution [15], multi-key exchange [6] and secure session initialization [26], the problem of key management in a hierarchy structure for access control has attracted much attention.

In a complex information system, users and data are usually organized in a hierarchy structure for access control. Different classes in the hierarchy structure are assigned different secret keys. At any point of time, users in superior classes should be allowed to derive the secret keys of subordinate classes. Furthermore, they should have no idea of the secret keys of any class that is not subordinate to their own.

This problem is first studied by Akl and Taylor [1, 2]. After that, a number of improved schemes have been proposed, e.g., [3]-[5], [8], [10], [12]-[14], [16]-[20], [22]-[23], [27]-[29]. Most of these results focus on saving time or storage space, while some of them target at achieving flexibility. In particular, the scheme of Sandhu [16] is very efficient although it only applies to tree hierarchy. Zhong [28] and Atallah et al. [3] extend Sandhu's scheme to a general hierarchy to achieve more flexibility. These traditional schemes assume that once a user is assigned to a security class, she always belongs to that security class.

More recently, researchers have taken into consideration that a user may not always belong to the same security class. In other words, a user may belong to a security class only during a specific time interval. A hierarchical key management scheme is *time bound* if it considers this issue. Tzeng' scheme [21] is the first time bound scheme, but it lacks efficiency and is proved to be insecure by Yi and Ye [24]. A more efficient time bound scheme is proposed by Chien [7], which uses tamper-resistant device to protect the assigned information. Unfortunately, it is still insecure as pointed out by Yi [25]. Consequently, these schemes are not suitable for use in practice.