International Journal of Innovative
Computing, Information and Control
Volume **6**, Number **2**, February **2010**

ICIC International ©2010 ISSN 1349-4198
pp. 439–447

SECURE AND EFFICIENT TIME-BOUND KEY ASSIGNMENT SCHEME FOR ACCESS CONTROL IN HIERARCHICAL STRUCTURE

Yu-Li Lin[1], Tzong-Chen Wu[1] and Chien-Lung Hsu[2,*]

[1]Department of Information Management
National Taiwan University of Science and Technology
Taipei 106, Taiwan
andrina_lin@yahoo.com.tw; tcwu@cs.ntust.edu.tw

[2]Department of Information Management
Chang Gung University
Tao-Yuan 333, Taiwan
*Corresponding author: clhsu@mail.cgu.edu.tw

Received August 2008; revised December 2008

Abstract. *Cryptographic key assignment schemes in the partially ordered hierarchy allow a higher security class to derive the cryptographic key of a lower security class for key management, supervising, and etc. A "time-bound" cryptographic key assignment scheme can allow each security class to own distinct secret keys for different time periods and the higher security class to perform key derivation only within the predetermined valid time period(s). Several previously proposed time-bound hierarchical key assignment schemes have been shown to be insecure against some potential collusive attacks. This paper will propose a new and secure time-bound key assignment scheme for access control in hierarchical structure. Advantages of the proposed scheme are given below. (i) The proposed scheme is flexible and practical since each security class can be given some discrete time periods for key derivation instead of a continuous one. (ii) We propose practical and efficient solutions to dynamic key management problems, including adding/deleting a security class and changing a derivation key without regenerating or updating all cryptographic keys owned by the classes. (iii) It can achieve confidentiality of encryption/derivation keys, forward secrecy, backward secrecy, access control, and time-bound security. (iv) Performance of the proposed scheme is more efficient than that of previously proposed schemes in terms of the computational complexities, the storage, and the key management efforts.*

Keywords: Access control, Key assignment, Secure broadcasting, Time-bound

1. **Introduction.** Access control problem in an arbitrary POSET hierarchy was first introduced by Akl and Taylor [2] (referred to as Akl-Taylor scheme for short). In such a scheme, users and their information items are classified into a number of disjoint sets of security classes, say $SC = \{SC_1, SC_2, \ldots, SC_n\}$, which are partially ordered by a binary relation "$\leq$". $SC_i \leq SC_j$ is referred to a user in security class, where SC_i is higher than or equal to the security class SC_j. The users in the security class SC_i can have access the information items held by those in the security class SC_j, while the opposite is not allowed. Each security class is assigned a distinct secret key which can be used to derive the successor's one according to the access control policy. In 1988, Sandhu [4] proposed a cryptographic key assignment scheme for a tree hierarchy which is a special case for a hierarchy. His scheme is based on the one-way functions which are easy to compute but computationally difficult to invert. The above schemes are based on symmetric cryptosystems and use the top-down approach.