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

ICIC International ©2011 ISSN 1349-4198
pp. 1087–1095

A SUPERVISING AUTHENTICATED ENCRYPTION SCHEME FOR MULTILEVEL SECURITY

Chien-Lung Hsu[2], Liang-Peng Chang[1] and Tzong-Chen Wu[1]

[1]Department of Information Management
Chang-Gung University
259 Wen-Hwa 1st Road, Kwei-Shan, Tao-Yuan, Taiwan
clhsu@mail.cgu.edu.tw

[2]Department of Information Management
National Taiwan University of Science and Technology
43 Section 4, Keelung Road, Taipei, Taiwan
kevinchang@ntu.edu.tw; tcwu@cs.ntust.edu.tw

Received October 2009; revised February 2010

Abstract. *Access to secret data should be managed to allow authorized people only. An authenticated encryption scheme can be used to protect valuable information or secret data for data confidentiality, authentication, non-repudiation and integrity. In this paper, the authors propose a new supervising authenticated encryption scheme for multilevel security which deals with the monitor and access control problems found in hierarchical organization, for protecting valuable authenticated encryption messages from being disclosed by malicious adversary. The proposed scheme provides two effective access control mechanisms, one is the partial access control and the other is the complete access control, which allows management superiors to monitor or access authenticated encryption messages received by inferiors within a hierarchical organization. Considering user privacy, the partial access control mechanism allows only a superior to access the "intended" authenticated encrypted information. In case of some special scenario (e.g., the monitored inferior is dead or dismissed), the complete access control mechanism allows the superior to access "all" authenticated encrypted messages received by the monitored inferior.*

Keywords: Multilevel security, Authenticated encryption, Access control, Monitor

1. Introduction.

A cryptographic scheme for enforcing multilevel security systems, where the hierarchy is represented by a partially ordered set, was introduced by Akl and Taylor [1]. Many cryptography techniques could be used to solve hierarchical access control problems, which mainly include access control [1-6], key escrow [7-9], and key recovery/key backup [10-12]. Although established methods could achieve the goal of multilevel security [13-17], these methods allow superiors access with the user's private key, or it requires additional operating costs to guarantee superiors only access to all user's specific information. Considering the balance between the user's privacy and superior's access rights, the system must be able to restrict each superior access to information, and prevent them from exceeding their level of authority access to information. However, under certain situations, some superiors must be authorized to access all user's information, for example, a user leaves the job.

An authenticated encryption scheme integrates encryption, decryption and digital signature techniques, and can be regarded as a combination of a data encryption scheme and a digital signature scheme for achieving privacy, integrity, and authentication [18-26]. However, the digital signature must be verified by a specified recipient, while the message remains completely confidential.