International Journal of Innovative Computing, Information and Control
Volume **5**, Number **5**, May **2009**

ICIC International ©2009 ISSN 1349-4198
pp. **1243–1251**

GROUP-BASED AUTHENTICATION TO PROTECT DIGITAL CONTENT FOR BUSINESS APPLICATIONS

Chin-Ling Chen[1], Yu-Yi Chen[2] and Yi-Hwa Chen[3]

[1]Department of Computer Science and Information Engineering
Chaoyang University of Technology
Taichung, Taiwan 413
clc@mail.cyut.edu.tw

[2]Department of Management Information Systems
National Chung Hsing University
Taichung, Taiwan 402
chenyuyi@nchu.edu.tw

[3]Institute of Applied Mathematics
National Chung Hsing University
Taichung, Taiwan 402
t132@nkc.edu.tw

Received December 2007; revised April 2008

Abstract. *Over the past several years, several high profile cases involving intellectual property copyright violations have brought the issue of digital content protection to the forefront of public attention. In most business enterprises, teamwork project members are dynamically organized into a group from which they can then retrieve relevant documents by participating in discussion. In this paper, we propose an efficient group-based authorized DRM system to solve this problem.*

We present efficient digital content protection and practical management architecture for use in business applications. Public key cryptosystems, symmetric cryptosystems, secret sharing mechanisms, one-way hash functions, and digital signatures are integrated into our scheme. Any business enterprise can thus use our system to limit access to only those with proper authorization. Moreover, persistent protection, integrity, authentication, tracking usage of DRM work, portability, and practicability are assured. Our scheme lends itself to the goals of many businesses by effectively protecting digital content.

Keywords: DRM, *E-DRM*, Security, Digital content protection, Secret sharing

1. **Introduction.** Novel information technologies give rise to both new conveniences and new problems. All businesses are confronted with the challenge of effectively preventing improper processes and malicious abuse of sensitive data. Many such methods are currently used to these ends; for example, firewalls are used to isolate networks to limit access to them. The New Technology File System (NTFS) can strengthen controls on access to file systems; the Encryption File System (EFS) can provide advanced secure file storage; and the Virtual Private Network (VPN), Internet Protocol Security (IPSec), and Secure Socket Layer (SSL) can protect digital content during transmission. All of the above technologies are widely used by businesses and work well.

However, the above defensive methods cannot control the uses and distribution of legally accessed digital content once it is in the possession of the consumer. That is to say, once a user passes authentication and gains access to the encrypted information, its retransmission cannot be limited. Numerous businesses are searching for solutions to this problem.