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

ICIC International ©2009 ISSN 1349-4198
pp. 1379–1394

BROADCAST YOURSELF SECURELY: ENHANCED TRANSMISSION SCHEME FOR SHARING DIGITAL CREATIONS

Ren-Hung Lin[1] and Jinn-Ke Jan[2]

[1]Institute of Applied Mathematics
[2]Institute of Computer Science
National Chung Hsing University
250, Kuo Kuong Road, Taichung 402, Taiwan
rhlin328@ms77.hinet.net; jkjan@cs.nchu.edu.tw

Received November 2007; revised April 2008

Abstract. *This paper presents an innovative distribution protocol for accessing broadcast files securely on the Internet. By employing a tree-structure-based encryption, the proposal reduces the communication overhead dramatically when transmitting digital content to receivers. Also, an ID-based public key cryptosystem is seamlessly incorporated into our scheme to decrease the storage requirement of certifications management. Compared with the currently available encryption schemes on Internet, it will be evident that our proposal is more efficient and practical.*

Keywords: Broadcast, Bilinear pairing, Key tree, Encryption, IPsec, SSL/TLS

1. **Introduction.** Today server computers are capable of providing many different services for end users due to the vast improvement in speed and reliability of information technology. Broadcast service is one popular applications on Internet [12,16,20,21,24,27]. Examples of popular broadcast services include daily news feeds, live multi-party conferencing, video transmissions, and online video games. Millions of broadcast messages are transmitted to end users every day. Recently, users have been given the ability to upload their self made digital videos to servers such as YouTube and share their creations with others. If some end users are not authorized to access particular messages, senders should protect the confidentiality of what they are broadcasting. Therefore, providing an efficient method for controlling authorized access is a major security challenge for broadcast services.

Currently, the most popular way to keep digital content private is to encrypt the original message (plain text) with a secret information (secret key) [1,3,9,13,22,30]. After being processed with encryption techniques, the plain text will be transformed to a confused one (cipher text) and only authorized users can convert the cipher text to the original message, since they have the related secret key assigned by the servers. Conversely, even though unauthorized end users may receive each broadcast message through public mediums used for transmission, they cannot read the confidential messages because they do not own the specific secret key.

Appling the available security services such as IPsec (IP security) [15], SSL (Secure Sockets Layer) [10], or TLS (Transport Layer Security) [7] to secure packets, the system can achieve the privacy requirements when transmitting messages. In the TCP/IP model, IPsec protocol operates at the network layer (relative to layer 3 of the OSI model) and SSL or TLS operates from the transport layer up to the application layer (relative to layer 4 to 7 of the OSI model). Using IPsec protocol, we can secure the Internet Protocol (IP) communications by authenticating and encrypting each IP packet in a data stream.