International Journal of Innovative Computing, Information and Control
Volume **6**, Number **5**, May **2010**

ICIC International ©2010 ISSN 1349-4198
pp. **2181–2188**

AN ONLINE BIOMETRICS-BASED SECRET SHARING SCHEME FOR MULTIPARTY CRYPTOSYSTEM USING SMART CARDS

Chun-Ta Li[1] and Min-Shiang Hwang[2,*]

[1]Department of Information Management
Tainan University of Technology
529 Jhong Jheng Road, Yongkang, Tainan 710, Taiwan
th0040@mail.tut.edu.tw

[2]Department of Management Information Systems
National Chung Hsing University
250 Kuo Kuang Road, Taichung 402, Taiwan
*Corresponding author: mshwang@nchu.edu.tw

Received November 2008; revised June 2009

Abstract. *In this article, we propose an online (t, n) threshold secret sharing scheme, in which the system will disperse a primary secret sharing key K for n users, and at least t users together can reconstruct the secret K. The security of our scheme is based on biometric verification and threshold password authentication. Therefore, the scheme is not only secure against several common attacks, but is also appropriate to be applied to other applications such as entrance guard systems and treasury management systems.*

Keywords: Biometrics, Cryptosystem, Threshold password authentication, Secret sharing, Smart cards, Network security

1. Introduction.

In general, a system manager is assigned to protect momentous resources (for instance, encrypted secret information, etc.) in the cryptosystem with a master key. However, in practice, some drawbacks may occur. The circumstances of these drawbacks are briefly described as follows:

1. A system manager is only allowed to recover the secrets with the master key. So he or she is required to participate in person every time.
2. If accidents happen to the system manager, the master key might be lost. The idea of managing resources by a system manager is quite risky due to single-point-failure. With a result, that will hinder a user from accessing the system.
3. If the system manager is capable of betraying the master key, this kind of compromised attack will damage the security of the system.

According to the previously-mentioned drawbacks, the concept of (t, n) threshold scheme [1, 2, 6, 21, 22, 23] is proposed, so that scattering a primary secret to a group of n participants and at least t authorized participants can reconstruct the primary secret, where $1 \leq t \leq n$. Hence, the idea of sharing a key among multiple authentication system managers may reduce the risk of key exposure and can prevent an unfaithful system manager from holding all of the important resources to seek private gain at public expense. Moreover, in order to provide secure communication in an open network, some security services such as user authentication mechanisms and key distribution protocols are necessary in communication network environments [3, 4, 5].

Traditionally, password-based protocols [8, 19, 24] have been widely used for user authentication because they permit users to freely choose the passwords they want. However, storing password tables in the system may suffer from compromised, stolen-verifier. Also,