International Journal of Innovative
Computing, Information and Control
Volume **6**, Number **7**, July **2010**

 ISSN 1349-4198
pp. **3093–3103**

A NOVEL AUTHENTICATION SCHEME FOR MOBILE COMMERCE TRANSACTIONS

Nai Wei Lo and Kuo-Hui Yeh

Department of Information Management
National Taiwan University of Science and Technology
No. 43, Sec. 4, Keelung Rd., Taipei 106, Taiwan
nwlo@cs.ntust.edu.tw; D9409101@mail.ntust.edu.tw

Received January 2009; revised August 2009

Abstract. *User privacy and robust system security have become essential requirements for a secure authentication scheme on mobile commerce applications. In order to reduce data transmission delay, and achieve computation efficiency on data encryption for communication parties during mobile commerce transaction, lightweight cryptosystem technology must be adopted in the design of next generation authentication protocol. In 2008, Lee et al. [9] developed two human-memorable password based authentication protocols to secure online transactions in mobile commerce systems. One of the proposed protocols replaces the time-consuming public key cryptosystem with symmetric key cryptosystem and simple hash functions to achieve better performance on encryption computation. The authors claimed that their schemes can defend against replay attack, denial of service attack and password guessing attacks. In this study, we first show that Lee et al.'s protocols are insecure against offline password guessing attacks and undetectable online password guessing attacks. A novel authentication scheme is then introduced to eliminate identified security weaknesses in their protocols. Based on our performance analysis, our proposed protocol requires fewer transmission rounds and less computation cost than previously proposed schemes [8,9] while achieving stronger security properties at the same time.*
Keywords: Authentication, Electronic transactions, Mobile commerce, Security

1. **Introduction.** With the rising and flourishing advance of wireless communication technologies and rapid growth in the number of mobile device users, mobile commerce becomes the most promising web business model in the near future. Well known web applications, such as electronic payments, electronic auctions and electronic voting, have been deployed in our daily life. However, there is security concern [13] to current mobile devices. A user utilizing mobile commerce via a mobile handheld device must apply a certificate and install it in a smart chip associated with the mobile device. If a user's mobile device has fallen into an adversary's hand, the malicious attacker can misuse it easily. Meanwhile, as modern society relies on various kinds of mobile devices to provide convenient and efficient services to users, the prevention of illegal access and information leakage on consumer transactions and user preference data promptly becomes a necessary security requirement for mobile commerce applications. Among various security strategies on mobile commerce transactions [4,8,9,12,13], developing a robust authentication scheme is one of the most promising and efficient ways to achieve robust data exchange, authorized resource access and individual profile protection.

In general, a mobile commerce environment consists of mobile users, mobile network and mobile commerce providers [9]. Once a mobile user starts an electronic transaction with the corresponding mobile commerce provider through a mobile network, the mobile user utilizes his/her mobile handheld device to wirelessly transmit service request (or