International Journal of Innovative
Computing, Information and Control
Volume 4, Number 9, September 2008

 ISSN 1349-4198
pp. 2305–2314

SECURE AUTHENTICATION PROTOCOLS FOR MOBILE COMMERCE TRANSACTIONS

Jung-San Lee[1], Ya-Fen Chang[2] and Chin-Chen Chang[1]

[1]Department of Information Engineering and Computer Science
Feng Chia University
Taichung 40724, Taiwan
{ ljs; ccc }@cs.ccu.edu.tw

[2]Department of Logistics Engineering and Management
National Taichung Institute of Technology
Taichung 404, Taiwan
cyf@cs.ccu.edu.tw

Received July 2007; revised November 2007

Abstract. *Several years ago, handheld devices were regarded luxuries. But they are almost taking the place of the traditional phones. It is because of the speedy development of mobile and wireless communication technologies. Nowadays, the mobile station plays an important role in most people's daily life. Furthermore, the explosion of the Internet has led to an electronic commerce environment such that people can conduct most transactions electronically. To improve the convenience and portability of electronic commerce, the mobile commerce system is proposed. In 2003, Lam et al. proposed a lightweight security mechanism for mobile commerce. Unfortunately, we find that there exists a security weakness in their method. Hence, we provide improvements on their proposed authentication protocol to make it secure. Besides, we propose a new authentication protocol for the mobile commerce transactions without adopting the public key cryptosystem.*
Keywords: Mobile commerce, Electronic transaction, Authentication protocol, Communication privacy

1. **Introduction.** Conventional transactions are traded electronically due to the rapid development of computer science and network technologies. Many applications such as electronic payments, electronic auctions, and electronic voting are expanded over the Internet. That is to say, the Internet has led to the origin of electronic commerce, which is regarded as an environment that allows the commercial information transmitted electronically. Accordingly, the popularity of wireless and mobile communication is also getting more and more popular. Mobile phones are almost taking the place of conventional telephones now because of the convenience and portability of the handheld devices [1,6,7,11,12,14,21,22].

Mobile and wireless networks make people free from the tethers which had bound them to the fixed place in the past, and they also enable users to work more flexibly and conveniently. Therefore, it is more convenient for users to conduct electronic transactions over the mobile platform. So far, there are lots of wireless networks have been built for communications and electronic commerce, such as Personal Communication Network (PCN), Personal Communication System (PCS), Global System of Mobile Communication (GSM), and General Packet Radio Service (GPRS). With the explosive population of the wireless devices such as cell phones, PDA's (Personal Data Assistant), pocket PC's and notebooks, and the expeditious adoption of mobile network technologies, supporting for electronic commerce over the mobile platform has become a practical and attractive