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

ICIC International ©2010 ISSN 1349-4198
pp. **2595–2608**

CRYPTANALYSIS OF AN EFFICIENT REMOTE USER AUTHENTICATION SCHEME WITH SMART CARDS

Kuo-Hui Yeh, Nai Wei Lo and Enrico Winata

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

Received December 2008; revised July 2009

Abstract. *From user point of view, smart card based authentication is one of the most popular technologies for system access and data exchange. However, its pervasive usage on new applications has been slowed down and restricted due to the concerns of potential security threats on resource-limited smart card. Therefore, a more efficient and secure remote authentication protocol for smart card users is devastatingly required nowadays. Recently, Huang and Wei [2] developed a remote user authentication scheme in which only an exclusive-or operator and a random number generator are utilized to provide a secure and efficient authentication service for smart card users. In this study, we first evaluate security robustness of Huang and Wei's scheme by engaging a series of planned active attack operations; our evaluation results show that the proposed attack can fully discover the secret information shared between a remote smart card user and the back-end server. To remedy identified security vulnerabilities, we develop a security-enhanced remote authentication protocol. The security and performance analyses show that our proposed authentication scheme delivers mutual authentication feature and stronger security robustness with the same order of computation complexity as Huang and Wei's scheme does.*

Keywords: Authentication, Smart card, Cryptanalysis, Probing-analysis attack, Security

1. **Introduction.** With the rapid growth of mobile commerce and business demand on automatic payment mechanism for a small amount of purchase, smart card has become one of the most popular technologies to provide a simple, convenient and user-friendly interface on application access and purchase payment. Successful application implementations with smart cards such as transport fare charge, electronic toll collection, online financial transaction and medical enquiry registration are widely deployed in our daily life. To support secure and efficient accessibility of smart card based applications, the design of corresponding authentication scheme has become a very important and challenging task. Since Lamport [4] first proposed a password-based authentication scheme under insecure communication environment, many studies [2-3,5-14] have been conducted by scholars to improve security robustness, performance efficiency and system functionality on remote user authentication protocol for smart card based applications. As the adoption of smart card technology has massively increased in recent years, more stringent requirement on security robustness and performance efficiency of authentication schemes has emerged in order to defend against new attack methodology and strategy invented by malicious adversaries. Accordingly, new authentication schemes are on demand to fulfill the amplified requirement. Recently, Huang and Wei [2] presented an efficient smart card based authentication protocol in which only lightweight computation units, such