International Journal of Innovative
Computing, Information and Control
Volume **6**, Number **8**, August **2010**

ICIC International ©2010 ISSN 1349-4198
pp. 3467–3478

A NOVEL REMOTE USER AUTHENTICATION SCHEME FOR MULTI-SERVER ENVIRONMENT WITHOUT USING SMART CARDS

Kuo-Hui Yeh and Nai Wei Lo

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 February 2009; revised August 2009

Abstract. *With the rapid growth of electronic commerce and demand on variants of the Internet based applications, the system providing resources and business services often consists of many servers around the world. For the reliability of accessing these remote services, user must pass a verification procedure to obtain the authorization for legal resource acquisition and data exchange. So far, a variety of authentication schemes have been published to solve this issue of remote user authentication for multi-server communication environment. However, most of previously proposed mechanisms are subject to system inefficiency or fail to fulfill their security claims. Recently, Lee et al. proposed an authentication protocol, which intends to possess both message exchange reliability and system computation efficiency, for multi-server architecture. At first glance, Lee et al.'s authentication scheme seems to be secure. Nevertheless, based on the protocol analysis derived by us, the proposed scheme is insecure against server spoofing attack, user impersonation attack and undetectable online password guessing attacks. In this study we demonstrate how these malicious attacks can be invoked by an adversary. Furthermore, a security enhanced authentication protocol is developed to eliminate all identified weaknesses and at the same time achieve the same order of computation complexity as Lee et al.'s protocol does.*

Keywords: Authentication, Communication, Key agreement, Multi-server, Security

1. **Introduction.** Following the advances in network technologies and the widespread distribution of remote system backup, lots of multi-server based applications have been deployed to make legitimate user access network service (or resource) more conveniently and efficiently. Primarily via the Internet, facilities and computers are linked together and the resource can be easily shared and exploited. As a result, an adequate remote user verification procedure must be adopted to ensure legal resource access and secure data exchange. As a password based user authentication scheme provides an efficient and accurate way to identify valid remote user and at the same time preserves the secrecy of communication, various authentication mechanisms [1-10] have been investigated in recent years. However, most of published protocols [1,4,5,9] are designed for single-server environment. Once the scale of the networks becomes larger, the password based authentication schemes which only supports the circumstance of single-server architecture does not suffice for users' need anymore. That is, this design may limit the future development and pervasive usage of existing Internet based applications. For example, to pursue the reliability and efficiency in a resource acquiring process, the remote service system often consists of many servers located at different places. Such communication architecture will result in single-server based authentication protocols hard to be implemented and even unworkable. In addition, a legal user, who intends to access distinct network services