International Journal of Innovative
Computing, Information and Control
Volume **7**, Number **8**, August **2011**

ICIC International ©2011 ISSN 1349-4198
pp. 4589–4602

A ROBUST AND EFFICIENT SMART CARD BASED REMOTE LOGIN MECHANISM FOR MULTI-SERVER ARCHITECTURE

Chin-Chen Chang[1,2] and Ting-Fang Cheng[2]

[1]Department of Information Engineering and Computer Science
Feng Chia University
No. 100, Wen-Hwa Road, Taichung 40724, Taiwan
alan3c@gmail.com

[2]Department of Computer Science
National Tsing-Hua University
No. 101, Sec. 2, Kuang-Fu Road, Hsinchu 30013, Taiwan
nthu.tiffany@gmail.com

Received February 2010; revised October 2010

Abstract. *With the explosive growth of computer networks, two-party authentication mechanism is no longer sufficient for real world. In 2008, Lee and Lee presented an efficient remote authenticated key agreement scheme for a multi-server environment. Their approach is efficient due to light operations such as hash function and exclusive-OR. Unfortunately, we discovered that their scheme is unable to withstand the forgery attack. We consequently propose a novel version with single registration using smart cards to resist this kind of attack and meanwhile achieve higher efficiency. In our proposed scheme, each service provider shares a distinct secret key with the registration center; this is to avoid risk of the whole system breaking down due to the destruction of a single service provider. Moreover, our method is nonce-based without the time synchronization problem. We also give a formal correctness analysis of mutual authentication to our scheme using BAN authentication logic. Our proposed scheme can prevent several malicious attacks and is more practical than related works.*

Keywords: Multi-server, Smart card, Single registration, Remote authentication, Key agreement, BAN logic

1. **Introduction.** Due to the explosive growth of network technologies, more and more traditional commercial businesses support online transactions. Since the early 1980s, password authentication has been widely used to safeguard the facility of a remote server from illegitimate access by unauthorized users [1]. Later, passwords were transformed into verifiers to enhance the security [2,3]. However, these methods are insecure since the verification patterns stored in the remote server may disclose some secrets. By adopting smart cards, improved versions were proposed to thwart the stolen-verifier attack [4-10].

With the rise of the Internet, two-party authentication is no longer sufficient. The remote system generally consists of many different service providers that supply different kinds of resources. As a result, various multi-server protocols have been proposed in recent years [11-22]. In general, a good multi-server authentication system should be applied in practice. It needs to contain as many properties as possible, such as single registration, mutual authentication, session key agreement, efficiency, security [11,12]. Single registration is the most important feature in a multi-server system. Users only need to register once to access all service providers in the system. On the other hand, multi-server authentication methods are generally divided into two types: (1) all service