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

ICIC International ©2010 ISSN 1349-4198
pp. **2469–2483**

A PRACTICAL THREE-PARTY AUTHENTICATED KEY EXCHANGE PROTOCOL

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 November 2008; revised March 2009

Abstract. *As people can easily choose and memorize simple or meaningful vocabulary as their own secret passwords, a password based three-party authenticated key exchange (3PAKE) protocol has been extensively investigated by scholars in the history of secure communication research area. However, it is very hard for most of the published schemes to meet the requirements of security and efficiency at the same time. Based on this observation, Lu and Cao [12] proposed a simple 3PAKE mechanism to achieve security criteria and system efficiency simultaneously. However, in 2008, Chang [19] demonstrated that Lu and Cao's 3PAKE scheme is vulnerable to undetectable on-line password guessing attacks, and developed an improved protocol to eliminate the identified security weakness. Nevertheless, Chang's protocol fails to fulfill their security claims. Based on our analyses, Chang's protocol suffers from man-in-the-middle attack, undetectable on-line password guessing attacks, and off-line password guessing attacks. Accordingly, we propose an enhanced protocol, which inherits the efficiency of Chang's 3PAKE protocol and eliminates its authentication flaws, to accomplish security robustness and system efficiency at the same time.*

Keywords: Three-party key exchange protocol (3PAKE), Authentication, Cryptanalysis, Security, Password guessing attacks, Man-in-the-middle attack.

1. Introduction.

As people can freely choose and memorize their own passwords without any assistant storage device, the practical usage of password mechanism on password based authenticated key exchange (PAKE) protocol has been broadly studied by scholars in recent two decades. In 1992, Bellovin and Merrit [1] proposed a two-party authenticated key exchange (2PAKE) protocol in which a high entropy cryptographic key is derived with the help of a pre-shared but low entropy password for any two communication entities. However, the scalability of Bellovin and Merrit's protocol is concerned by research society due to the inconvenience and high cost of maintaining all passwords for each pair of participants in a large scale communication environment. This limitation inspired research experts to extend 2PAKE protocol into the client-client-server based network architecture, i.e. three-party authenticated key exchange (3PAKE) protocol. Nowadays, the vast literature devoted to 3PAKE protocol and password based remote authentication mechanism has been reviewed on several occasions [1-17,19,21-26]; in addition, famous standards and applications such as IEEE P1363.2 [29], ISO/IEC 11770-4 [30], Kerberos [27] and KryptoKnight [28] have been introduced also.

Although a great deal of effort has been made on the research area of 3PAKE protocol, the usage of published schemes is limited due to their own security vulnerabilities and performance inefficiency. We present these observations as follows. In 1995, Steiner et al. [15] pointed out that Bellovin and Merrit's 2PAKE protocol has a potential security