International Journal of Innovative Computing, Information and Control
Volume **7**, Number **7(A)**, July **2011**

ICIC International ©2011 ISSN 1349-4198
pp. **3751–3760**

AN ENHANCED PASSWORD-BASED USER AUTHENTICATION SCHEME FOR GRID COMPUTING

Zhen-Yu Wu[1], Yufang Chung[2], Feipei Lai[1,3], Tzer-Shyong Chen[4] and Hung-Chang Lee[5]

[1]Department of Computer Science and Information Engineering
[3]Department of Electrical Engineering
[3]Graduate Institute of Biomedical Electronics and Bioinformatics
National Taiwan University
No. 1, Sec. 4, Roosevelt Road, Taipei 10617, Taiwan
{ d96922021; flai }@ntu.edu.tw

[2]Department of Electrical Engineering
[4]Department of Information Management
Tunghai University
No. 181, Sec. 3, Taichung Harbor Road, Taichung 40704, Taiwan
{ yfchung; arden }@thu.edu.tw

[5]Department of Information Management
Tamkang University
No. 151, Ying-Chuan Road, Taipei 25137, Taiwan
hclee@mail.im.tku.edu.tw

Received January 2010; revised May 2010

Abstract. *Based upon Elliptic Curve Cryptosystem, a simple password user authentication scheme was proposed by Lu et al. for grid computing. In their scheme, Lu et al. not only kept the advantages of Yoon et al.'s scheme, but enhanced the efficiency of mutual authentication and at the same time avoided the stolen-verifier attacks as well. However, their scheme is proven to be unable to resist the off-line password guessing attacks. Apart from that, the problem of people masquerading as a server to communicate with the other users in their scheme is also inevitable. Therefore, an ameliorative password-based authentication scheme is proposed subsequently in this paper to achieve perfect forward secrecy and to resist replay attacks, server spoofing attacks, on-line and off-line password guessing attacks and impersonation attacks. The proposed scheme is shown to be more secure and practical than those previously proposed schemes.*
Keywords: Password, Mutual authentication, Off-line password guessing attacks, Perfect forward secrecy, Server spoofing attacks

1. **Introduction.** Grid computing, also called computational grids, enables the sharing, selection, and aggregation of a wide variety of geographically distributed computational resources such as operating platforms, heterogeneous system constructions, storage systems, data sources, instruments, machine languages and human resources, and then presents them as a single, unified resource for solving a common task, usually, a scientific, technical or business problem that requires a huge number of computer processing cycles or the need to process large amounts of data.

I. Foster [1] listed three primary attributes for the question of what grid computing is. Firstly, the computing resources are not administered centrally, tending to be more loosely coupled, heterogeneous and geographically dispersed. Secondly, grid computing is