International Journal of Innovative Computing, Information and Control
Volume **4**, Number **11**, November **2008**

ICIC International ©2008 ISSN 1349-4198
pp. 2987–2996

TIME-BOUND BASED AUTHENTICATION SCHEME FOR MULTI-SERVER ARCHITECTURE

Chin-Chen Chang[1], Jung-San Lee[1] and Jui-Yi Kuo[2]

[1]Department of Information Engineering and Computer Science
Feng Chia University
Taichung, 40724, Taiwan
{ ccc; ljs }@cs.ccu.edu.tw

[2]Department of Computer Science and Information Engineering
National Chung Cheng University
Chiayi, 621, Taiwan
kjy92@cs.ccu.edu.tw

Received August 2007; revised December 2007

Abstract. *The distribution of the remote system hardware in different places makes legal users access the resource more conveniently and efficiently. Again, backup of the resource is also an important concern of the scatter. So far, most of the password authentication schemes are designed for single-server environments, users who want to access different remote servers need to register many times and keep many accounts and passwords. To solve this problem, we propose a more efficient version for multi-server architecture. In particular, the new method employs a time-bound mechanism such that the remote system can effectively conduct the valid access period for each legitimate user.*

Keywords: Authentication, Multi-server, Time-bound, Session key

1. Introduction.

The result of the combination between password authentication scheme and key agreement mechanism is a very practical solution to verify the validity of the remote user and to ensure secure communications. That is, while users want to access the remote server, they must pass a serial of examinations to make them be authenticated. After users are authorized, they can access the resource provided by the remote system and share a negotiated session key with the remote server to ensure the following communications; otherwise, their access requests will be rejected. In 1981, Lamport first proposed a remote password authentication scheme for communication through insecure channels [10]. In most password authentication schemes, users who want to access the remote server need to send a valid pair of the identity (ID) and the password (PW) to the remote system to make them authenticated, and Lamport's is no exception. Unfortunately, Lamport's scheme suffers from the stolen-verifier attack if the intruder has the ability to get the stored verifier someway. Shortly, smart cards are used widely in the password authentication scheme to confirm the legality of the user such that it is unnecessary to keep the verification table in the remote server's database. Therefore, the stolen-verifier attack is resolved. Recently, more and more password authentication schemes are proposed to improve the authentication efficiency or the security of these schemes so that password authentication has become a popular research topic [1,2,4,9,12-15,21].

The remote system providing resources to be accessed over the networks often consists of different servers around the world. The scatter of the remote system hardware in different places makes legal users access the resource more conveniently and efficiently. What is more, backup of the resource is also an important concern of the scatter. So far, most