Available online at www.sciencedirect.com

SCIENCE DIRECT®

ELSEVIER Applied Mathematics and Computation 170 (2005) 1185–1193

APPLIED MATHEMATICS AND COMPUTATION

www.elsevier.com/locate/amc

Weakness and improvement on Wang–Li–Tie's user-friendly remote authentication scheme

Da-Zhi Sun [a,*], Ji-Dong Zhong [a], Yu Sun [b]

[a] *Department of Computer Science, Shanghai Jiao Tong University, 1954 HuaShan Road, P.O. Box 282, Shanghai 200030, PR China*

[b] *Department of Management, Beijing Normal University, Beijing 100875, PR China*

Abstract

In an open network environment, the remote authentication scheme using smart cards is a very practical solution to validate the legitimacy of a remote user. In 2003, Wu and Chieu presented a user-friendly remote authentication scheme using smart cards. Recently, Wang, Li, and Tie found that Wu–Chieu's scheme is vulnerable to the forged login attack, and then presented an improvement to eliminate this vulnerability. In our opinion, the smart card plays an important role in those schemes. Therefore, we demonstrate that Wang–Li–Tie's scheme is not secure under the smart card loss assumption. If an adversary obtains a legal user's smart card even without the user's corresponding password, he can easily use it to impersonate the user to pass the server's authentication. We further propose an improved scheme to overcome this abuse of the smart card.

[*] Corresponding author.

E-mail addresses: sundazhi@sjtu.edu.cn (D.-Z. Sun), zhongjidong@sjtu.edu.cn (J.-D. Zhong), girlinsunshine@263.net (Y. Sun).

0096-3003/$ - see front matter © 2005 Elsevier Inc. All rights reserved.
doi:10.1016/j.amc.2005.01.013

Keywords: Network security; Cryptology; Remote authentication; Smart card loss assumption; Password; Impersonation

1. Introduction

In an open network environment, when a remote user requests a server's service, the server needs to authenticate the legitimacy of the user over an insecure channel. Through the authentication process, the server can determine if some services can be provided to the user.

In 2000, Sun [1] gave a remote user authentication scheme using smart cards. As a unilateral authentication mechanism, Sun's scheme is very efficient because it only requires few hashing operations. But an unreasonable requirement in Sun's scheme is that the user's password should be generated by the server. From the view of human psychology, it is very difficult and troublesome to memorize a long and irregular password assigned by the server. Therefore, Wu and Chieu [2] presented a solution to let the user freely choose his password. Recently, Wang et al. [3] found that Wu–Chieu's scheme is vulnerable to the forged login attack, and then presented an improvement to eliminate this vulnerability.

As a smart card-based scheme, we stress that the smart card loss scenario should be considered in detail. It is possible that a careless user loses his smart card, and then an adversary just obtains it. Another more serious situation is that an adversary actively steals a legal user's smart card to impersonate the user or reveal the secret information of the authentication system. For these reasons, we assume that the adversary can obtain the smart card and is allowed to sequentially use it as a black-box. Hence, a practical remote user authentication scheme using smart cards needs to achieve the security under the smart card loss assumption. That is, the adversary cannot get any benefit from a legal user's smart card without the user's corresponding password.

In this paper, we show that Wang–Li–Tie's scheme is not secure under the smart card loss assumption. If an adversary obtains a legal user's smart card even without the corresponding password, he can easily use it to produce a fabricated login message, and then impersonate the user to pass the server's authentication. Therefore, we further propose an improved scheme to overcome this abuse of the smart card.

The remainder of this paper is organized as follows. Wang–Li–Tie's scheme is described in Section 2. In Section 3, we demonstrate the weakness of Wang–Li–Tie's scheme under the smart card loss assumption. In Section 4, we propose an improved scheme. In Section 5, we examine the security of our improved scheme. Finally, we give comments and conclusions in Section 6.