Computers & Security (2005) **24**, 619–628

ELSEVIER

**Computers & Security**

www.elsevier.com/locate/cose

# Robust remote authentication scheme with smart cards☆

**Chun-I Fan *, Yung-Cheng Chan, Zhi-Kai Zhang**

*Department of Computer Science and Engineering, National Sun Yat-sen University, No. 70, Lien-Hai Road, Kaohsiung 804, Taiwan, ROC*

Received 13 August 2004; revised 1 March 2005; accepted 28 March 2005

**KEYWORDS**
Remote authentication;
Login;
Smart cards;
Information security;
Cryptology

**Abstract** Due to low-computation cost and convenient portability, smart cards are usually adopted to store the personal secret information of users for remote authentication. Although many remote authentication schemes using smart cards have been introduced in the literatures, they still suffer from some possible attacks or cannot guarantee the quality of performance for smart cards. In this paper, we classify the security criteria of remote authentication and propose a new remote login scheme using smart cards to satisfy all of these criteria. Not only does the proposed scheme achieve the low-computation requirement for smart cards, but also it can withstand the replay and the offline dictionary attacks as well. Moreover, our scheme requires neither any password table for verification nor clock synchronization between each user and the server while providing both mutual authentication and the uniqueness of valid cards.


## Introduction

In order to authenticate the clients or users, password-based security mechanisms have been widely used in many remote login systems because they are easily implemented. In a traditional authentication scheme, the server or system must keep a password table to store all of the passwords of the registered users in the system. Since the password tables cannot be revealed and they are usually large, it is hard and inefficient to maintain such tables. To cope with the problem, secure remote password authentication was firstly proposed by Lamport (1981) and several methods, based on one-way hashing functions (Evan et al., 1974; Lennon et al., 1981) and TTP (Kehne et al., 1992; Neuman and Stubblebine, 1993; Shieh and Yang, 1996), have also been introduced in the literatures. However, some known or unknown

☆ This research was partially supported by the National Science Council of the Republic of China under grant NSC93-2213-E-110-044.
* Corresponding author. Tel.: +886 7 5252000x4346; fax: +886 7 5254301.
*E-mail address:* cifan@cse.nsysu.edu.tw (C.-I. Fan).

0167-4048/$ - see front matter © 2005 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2005.03.006

attacks on the password tables may be still valid in these authentication schemes. To avoid all possible attacks on the password tables, many authentication schemes based on smart cards without password tables were proposed (Chang and Wu, 1991; Chien et al., 2002; Hwang and Li, 2000; Hwang et al., 2002; Juang, 2004; Lee et al., 2002; Lin et al., 2003; Sun, 2000; Tan and Zhu, 1999; Wang and Chang, 1996; Wang, 2003; Wu, 1995; Wu and Chieu, 2003; Yang and Shieh, 1999).

Since the computation capabilities of smart cards are limited, time-consuming operations are not suitable in such environments. The schemes of (Chang and Wu, 1991; Chien et al., 2002; Hwang et al., 2002; Juang, 2004; Lee et al., 2002; Lin et al., 2003; Sun, 2000; Wang, 2003) take low-cost functions or operators, such as hashing functions, exclusive-or operations, or multiplicative operations, instead of the operations with heavy computational workload, like exponentiation computations, to build their protocols. Besides, it is difficult for the users to memorize the long and meaningless passwords those are generated by the system. Hence, the schemes of (Chien et al., 2002; Hwang et al., 2002; Juang, 2004; Lee et al., 2002; Lin et al., 2003; Tan and Zhu, 1999; Wang and Chang, 1996; Wang, 2003; Wu, 1995; Wu and Chieu, 2003; Yang and Shieh, 1999) have been designed to allow the users themselves to choose their passwords freely.

In remote authentication protocols, intruders may intercept the login messages transmitted between the users and the system. They then resend the system the messages and attempt to impersonate the legitimate users to login the system. This is called the *replay* attack. In order to prevent the attack, timestamps are usually used in remote authentication schemes (Chang and Wu, 1991; Chien et al., 2002; Hwang and Li, 2000; Hwang et al., 2002; Lee et al., 2002; Sun, 2000; Tan and Zhu, 1999; Wang and Chang, 1996; Wang, 2003; Wu, 1995; Wu and Chieu, 2003). However, the schemes based on timestamps must overcome the problems of clock synchronization and delay-time limitation so that we better implement them in fast local area networks. In a large-scale network, it is almost impossible to maintain the synchronization of clocks among all entities in the network and to guarantee the delay time of transmission. For large-scale networks, Yang and Shieh (1999) proposed a remote authentication scheme based on ''nonce'' instead of timestamps without the problems of clock synchronization and delay-time limitation. Unfortunately, some security weaknesses have been found in Yang and Shieh's scheme (Chen and Zhong, 2003).

Malicious parties may catch the information stored in the smart card of some user by some ways, such as the attackers successfully crack the smart card that was lost by the user (Kocher et al., 1999; Messerges et al., 2002) or the attackers obtain the information in the smart card via an illegal card reader or device. With the information stored in the smart card and the messages intercepted during the previous login transactions between the user and the system, the attackers can repeatedly guess the user's password and examine if the guessed password is correct through performing an offline hacking program (Hsu, 2003; Ku and Chen, 2004; Yang and Wang, 2004; Yeh et al., 2001). This is called the *offline dictionary* attack with the *smart card*. If the attackers obtain the information in the smart card and find the correct password via the attack, they can pass the authentication process and then login the system successfully. Nevertheless, most of the schemes proposed in the literatures have not considered the protection mechanism in their protocols to withstand the attack (Chien et al., 2002; Hwang et al., 2002; Juang, 2004; Lee et al., 2002; Lin et al., 2003; Tan and Zhu, 1999; Wang and Chang, 1996; Wang, 2003; Wu, 1995; Wu and Chieu, 2003; Yang and Shieh, 1999).

In a basic remote authentication scheme, the system only checks the validation of the users but the users never verify whether the server is legal or not. It may affect the security of the entire protocol since an illegal system may cheat the users and obtain some secret information from them. In (Chien et al., 2002; Yen and Liao, 1997), the idea of mutual authentication is introduced such that the system and each of the users can be authenticated by each other.

If a remote authentication scheme can resist the offline dictionary attack with the smart card, then the user who lost her/his smart card just needs to re-register with the system and requests a new card from the system without changing the password. However, if the user lost both her/his card and the password, she/he has to acquire not only a new card but also a new password even though the scheme can withstand the offline dictionary attack with the smart card. There is another serious problem that the attackers may use the lost card and password to login the system successfully if the system cannot distinguish the new card from the lost one. Therefore, to avoid the misuse of the lost cards, the system should revoke or disable all of them. Most of the schemes proposed in the literatures cannot provide an efficient solution for this problem.