Available online at www.sciencedirect.com
ScienceDirect
Computer Standards & Interfaces 29 (2007) 507–512
COMPUTER STANDARDS & INTERFACES
www.elsevier.com/locate/csi

# Cryptanalysis and improvement on two efficient remote user authentication scheme using smart cards ☆

Xiao-Min Wang [a,*], Wen-Fang Zhang [b], Jia-Shu Zhang [a], Muhammad Khurram Khan [a]

[a] *Key Laboratory of Signal and Information Processing of Sichuan Province, Southwest Jiaotong University, Chengdu, 610031, PR China*
[b] *Key Laboratory of Information Security and National Computing Grid, Southwest Jiaotong University, Chengdu, 610031, PR China*

Received 15 February 2006; received in revised form 17 October 2006; accepted 11 November 2006
Available online 16 January 2007

**Abstract**

In 2002, Chien et al. proposed an efficient remote authentication scheme using smart cards, in which only few hashing operations are required. Later, Ku et al. gave an improved scheme to repair the security pitfalls found in Chien et al.'s scheme. Also Yoon et al. presented an enhancement on Ku et al.'s scheme. In this paper, we show that both Ku et al.'s scheme and Yoon et al.'s scheme are still vulnerable to the guessing attack, forgery attack and denial of service (DoS) attack. In addition, their schemes lack efficiency when users input wrong passwords. To remedy these flaws, this paper proposes an efficient improvement over Ku et al.'s and Yoon et al.'s schemes with more security. The computation cost, security, and efficiency of the improved scheme are embarking for the real application in the resource-limited environment.


*Keywords:* Authentication; Smart card; Session key; Password

**Contents**



☆ This work is supported by the National Natural Science Foundation of China (grant No. 60272096) and by the Doctor Innovation Fund of Southwest Jiaotong University, 2006.
* Corresponding author.
*E-mail address:* hornwong@hotmail.com (X.-M. Wang).

0920-5489/$ - see front matter © 2006 Elsevier B.V. All rights reserved.
doi:10.1016/j.csi.2006.11.005

## 1. Introduction

With the large scale development of network technology, remote user authentication in e-commerce and m-commerce has become an indispensable part to access the precious resources. Remote authentication is a mechanism to authenticate remote users over insecure communication network. During the past two decades, password-based remote authentication schemes have been widely deployed to verify the legitimacy of the remote users. Since Lamport [1] proposed his remote authentication scheme in 1981, several schemes [2,3] have been proposed to improve the security, the cost or the efficiency. One of the common features of these schemes is that a verification table should be securely stored in the server. If the verification table is stolen by the adversary, the system will be partially or totally broken.

Due to the low cost, the portability and the cryptographic capacity, smart cards have been widely adopted in remote authentication schemes [4–17]. In 2000, Hwang and Li [9] proposed a new remote user authentication scheme using smart cards. In 2002, based on Sun's scheme [14], Chien et al. [15] proposed a most cost-effective remote user authentication solution, and claimed that their scheme has the merits of providing mutual authentication, freely choosing password, no verification table, and involving only few hashing operations instead of the costly modular exponentiations. Unfortunately, Ku et al. [16] pointed out that Chien et al.'s scheme is vulnerable to reflection attack, insider attack, guessing attack and is not reparable once a user's permanent secret is compromised, and an improved scheme was given further to resolve these security pitfalls. Recently, however, Yoon et al. [17] showed that Ku et al.'s scheme is susceptible to parallel session attack and is insecure for changing the user's password, and also proposed an enhancement to Ku et al.'s scheme to overcome such problems.

Due to the power constraint of smart cards and the cost of implementation, the lower the cost, the great chance of success in practical realization. Among those smart card based schemes, Ku et al.'s and Yoon et al.'s schemes require only several hash operations instead of the costly modular exponentiations. Therefore, their schemes exhibit great application potentiality in smart card field, regardless of their security.

In this paper, however, we show that both Ku et al.'s scheme and Yoon et al.'s scheme are still vulnerable to the guessing attack, forgery attack and denial of service (DoS) attack. In addition, their schemes are inefficient when user inputs wrong password. To remedy these pitfalls, this paper presents an efficient improvement on them with more security. As a result, only requiring few additional hash operations, our scheme can withstand the previously proposed attacks. In the meanwhile, the wrong passwords input by users can be detected immediately, and a session key is also provided after authentication phase. The computational costs and efficiency of the improved scheme are encouraging for the practical implementation in the resource-constraint environment.

The rest of the paper is organized as follows: Section 2 reviews Ku et al.'s scheme. Section 3 gives the cryptanalysis of Ku et al.'s scheme. Section 4 shows the details of the proposed scheme. Section 5 makes the security analysis of the proposed method. Section 6 compares the performance of proposed scheme with Ku et al.'s and Yoon et al.'s schemes. Finally, the conclusion comes in Section 7.

## 2. Review of the Ku et al.'s scheme [16]

The notations used throughout the paper can be summarized as follows:

- $U$: denotes the user.
- $ID$: denotes the identity of $U$.
- $PW$: denotes the password of $U$.
- $S$: denotes the remote server.
- $x$: denotes the permanent secret key of $S$.
- $h(\cdot)$: represents a cryptographic unkeyed hash function.
- $h_k(\cdot)$: represents a cryptographic keyed hash function with secret $k$.
- $\Rightarrow$: represents a secure channel.
- $\rightarrow$: represents a common channel.

There are four phases in Ku et al.'s scheme: registration, login, verification and password change.

### 2.1. Registration

This phase is invoked whenever $U$ initially registers or re-registers to $S$. Let $n$ denote the number of times $U$ reregisters to $S$.

1 $U$ selects a random number $b$ and computes $h(b \oplus PW)$.
2 $U \Rightarrow S$: $ID$, $h(b \oplus PW)$.
3 If it is $U$'s initial registration, $S$ create an entry for $U$ in the account database and stores $n=0$ in this entry. Otherwise, $S$ sets $n=n+1$ in the existing entry for $U$. Next, $S$ performs the following computations: $R=h(EID \oplus x) \oplus h(b \oplus PW)$, where $EID=(\mathrm{ID}||\mathrm{n})$.
4 $S \Rightarrow U$: a smart card containing $R$ and $h(\cdot)$.
5 $U$ enters $b$ into his smart card.

Note that $U$'s smart card contains $R$, $b$ and $h(\cdot)$, and $U$ need not remember $b$ after finishing step 5.

### 2.2. Login

1 $U$ inserts his smart card into the card reader, and then enters $ID$ and $PW$.
2 Smart card performs the following computations: $c_1=R \oplus h(b \oplus PW)$ $c_2=h(c_1 \oplus T_u)$ where $T_u$ denotes $U$'s current timestamp.
3 $U \rightarrow S$: $\{ID, c_2, T_u\}$.

### 2.3. Verification

After $\{ID, c_2, T_u\}$ is received, $S$ and the smart card execute the following steps:

1 If either $ID$ or $T_u$ is invalid, $S$ rejects $U$'s login request. Otherwise, $S$ computes $h(h(EID \oplus x) \oplus T_u)$. If the computed