# Enhanced Forward-Secure User Authentication Scheme with Smart Cards

Eun-Jun Yoon and Kee-Young Yoo*

Department of Computer Engineering,
Kyungpook National University,
Daegu 702-701, South Korea
Tel.: +82-53-950-5553; Fax: +82-53-957-4846
ejyoon@infosec.knu.ac.kr, yook@knu.ac.kr

**Abstract.** In 2006, Wang-Li proposed a new user authentication scheme using smart cards which can offer forward secrecy. However, this paper will demonstrate that Wang-Li's scheme is vulnerable to parallel session attack and reflection attack. Furthermore, the current paper presents a more efficient and secure scheme that not only resolves such problems, but also involves fewer computations and communications than Wang-Li's scheme.

**Keywords:** Network security, Secure protocol, Smart card, Authentication, Password.

## 1 Introduction

User authentication is an important aspect of security, along with confidentiality and integrity, for systems that allow remote access over untrustworthy networks, like the Internet. As such, a remote password authentication scheme authenticates the legitimacy of users over an insecure channel, where the password is often regarded as a secret shared between the remote system and user. Based on knowledge of the password, a user can use it to create and send a valid login message to a remote system to gain the right to access the system. Meanwhile, the remote system also uses the shared password to check the validity of the login message and to authenticate the user.

In 1981, Lamport [1] proposed a password authentication scheme for insecure communication that scheme requires the remote server to maintain a password table for purpose of verification. In 2000, Hwang and Li [2] proposed a new scheme using smart cards. The advantage of the Hwang-Li's scheme is that it does not need any pass- word table. Subsequently, Yoon et al. [3] proposed a mutual authentication scheme based on generalized ElGamal signature scheme, which is more efficient than Hwang and Li's scheme in terms of computation and communication cost. In addition, the Yoon-Ryu-Yoo's scheme provides the function of key exchange. However, in 2005, Wang-Li [4] pointed out a security

* Corresponding author.

A.S. Atzeni and A. Lioy (Eds.): EuroPKI 2006, LNCS 4043, pp. 197–206, 2006.

leak of the Yoon-Ryu-Yoo's scheme in that an intruder is able to reveal previous session keys by means of disclosed secret parameters.

The current discussion will demonstrate that Wang-Li's scheme is vulnerable to parallel session attack [5] and that an attacker without knowing a user's password can masquerade as the legal user by creating a valid login message from an eavesdropped communication between authentication server and the user. Additionally, we will point out that Wang-Li's scheme is vulnerable to reflection attack [6] in which an attacker can masquerade as the legal authentication server by creating a valid response message from an eavesdropped communication between authentication server and the user. The current paper presents a more efficient and secure scheme that not only resolves such problems, but also involves fewer computations and communications than Wang-Li's scheme.

This paper is organized as follows: Section 2 briefly reviews Wang-Li's forward-secure remote user authentication scheme with smart cards, then Section 3 discusses its weaknesses. The proposed scheme is presented in Section 4, while Section 5 discuss the security and efficiency of the proposed scheme. Our conclusions are presented in Section 6.

## 2 Review of Wang-Li's Scheme

There are three phases in Wang-Li's scheme [4]: registration, login, and authentication. In addition, their scheme has a password change phase that allows users to update their passwords freely without the help of a remote system. Fig. 1 illustrates Wang-Li's remote user authentication scheme.

**Registration:** User $U_i$ submits his or her identifier $ID_i$ and $PW_i$ to the remote system, where $PW_i$ is the chosen password. Initially, the remote system performs the following steps:

(1) Chooses a secure one-way function $h(\cdot)$, $p$, $q$, and $g$, where $p$ is a large prime number with bit size 1024, $q$ is a prime divisor of $p-1$ with bit size 160, and $g$ is an element of order $q$ in the finite field $GF(p)$. The bit size of the output of $h(\cdot)$ is $|q|$;
(2) Computes $R_i = h(ID_i||x_s)$, $X_i = R_i \oplus h(ID_i||PW_i)$, where $||$ denotes a concatenation operation;
(3) Writes $ID_i$, $R_i$, $X_i$, $h(\cdot)$, $p$, $q$, $g$ to the memory of the smart card and issue the card to $U_i$. Note that $h(\cdot)$, $p$, $q$ and $g$ are the public parameters, while $R_i$ and $X$ are the kept secret.

**Login:** If user $U_i$ wants to log in to a remote system, he or she must insert his or her smart card into a card reader and key in his or her identifier $ID_i$ and password $PW_i$. Then the smart card performs the following steps:

(1) Generates a random number $r \in Z_q^*$;
(2) Computes $t = g^r \bmod p$;