An Improved Lu-Cao's Remote User Authentication Scheme Using Smart Card

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 2005, Lu-Cao proposed an improvement on Hwang-Li's remote user authentication scheme using a smart card that could withstand an impersonation attack, but also it required fewer computational costs. However, the current paper demonstrates that Lu-Cao's scheme has some drawbacks. We present an improved authentication scheme in order to isolate such problems.

Keywords: Authentication, Password, Network security, Smart card.

1 Introduction

A remote password authentication scheme is used to authenticate legitimacy of the remote users over an insecure channel. ISO 10202 standards have been established for the security of financial transaction systems that use integrated circuit cards (IC cards or smart cards). The main characteristics of a smart card are its small size and low-power consumption. In general, a smart card contains a microprocessor which can quickly manipulate logical and mathematical operations, RAM, which is used as a data or instruction buffer; and ROM, which stores the user's secret key and the necessary public parameters and algorithmic descriptions of the executing programs. The merits of a smart card regarding password authentication are its simplicity and its efficiency in terms of the log-in and authentication processes. The main merits of a smart card-based authentication scheme include: (1) there is no password or verification table kept in the remote server; (2) users can freely choose and change their passwords; and (3) lower communication and computation costs. In 1981, Lamport [1] proposed a remote password authentication scheme using a password table to achieve user authentication. In 2000, Hwang-Li [2] pointed out that Lamport's scheme suffers from the risk of a modified password table. Moreover, there is the cost of protecting and maintaining the password table. Therefore, they proposed a new user authentication scheme using smart cards to eliminate risks and costs. Hwang-Li's scheme can withstand replay attacks and can also authenticate users without maintaining a password table. However, there is a weakness in the scheme, as

* Corresponding author.

A.S. Atzeni and A. Lioy (Eds.): EuroPKI 2006, LNCS 4043, pp. 45–53, 2006.

previously noted [3][4], in that an attacker can easily impersonate other user to log in the system. To overcome such a weakness, Shen et al. [5] proposed a modified version that they claimed it is secure against such attacks. However, Leung et al. [6] showed the weakness still exists in Shen et al.'s scheme.

In 2005, Lu-Cao [7] proposed an improvement on Hwang-Li's scheme that not only could it withstand an impersonation attack, but that required fewer computational costs. Furthermore, it does not require modular exponentiation computations. However, the current paper demonstrates that Lu-Cao's scheme has some drawbacks; that is, the password of a user has to be computed by the system and the scheme has unnecessary computation costs. In general, this cannot satisfy a user's and an authentication scheme's requirements, respectively. To achieve the aim of user friendliness as well as low communication and low computation, we present an improved authentication scheme to the scheme in order to isolate such problems which still achieves the same advantages as Lu-Cao's scheme. The proposed scheme has the following two advantages. First, it is user friendly since a variable-length password can be chosen and changed freely by the user without the help of a remote server, while also providing mutual authentication. Secondly, it is more secure and efficient than Lu-Cao's scheme.

The remainder of this paper is organized as follows: Section 2 briefly reviews Lu-Cao's scheme. Some drawbacks of Lu-Cao's scheme are demonstrated in Section 3. The proposed authentication scheme is presented in Section 4, while Sections 5 and 6 discuss the security and efficiency of the proposed scheme. Our conclusions are given in Section 7.

2 Review of Lu-Cao's Authentication Scheme

This section briefly reviews the Lu-Cao's authentication scheme [7]. Lu-Cao's scheme consists of four phases: an initialization, registration, login, and authentication phase. Figure 1 shows Lu-Cao's authentication scheme. The scheme works as follows:

Initialization Phase: To set up a remote system, the remote server first must prepare the following parameters:

- p, q: two distinct security large primes, satisfying $p \equiv q \equiv 3 \bmod 4$;
- $n : n = p \cdot q$;
- a: a random number in Z_n^*, satisfying $(\frac{a}{n}) = -1$;
- $H(\cdot) : \{0,1\}^* \rightarrow Z_n^*$ is one-way hash function;
- $H_1(\cdot) : \{0,1\}^* \times Z_n^* \rightarrow Z_n^*$ is another one-way hash function.

Then, the remote server can accept the user registration request operation.

Registration Phase: When a new user U_i submits his or her identity ID_i to the remote server for registration. The server does the following:

(1) check the validity of ID_i. If it is valid, the operation will continue, otherwise stop;