Available online at www.sciencedirect.com
SCIENCE DIRECT®
APPLIED MATHEMATICS AND COMPUTATION
ELSEVIER Applied Mathematics and Computation 161 (2005) 101–107
www.elsevier.com/locate/amc

Cryptanalysis of Lee–Hwang–Li's key authentication scheme

Fangguo Zhang *, Kwangjo Kim

International Research center for Information Security (IRIS), Information and Communications University (ICU), 58-4 Hwaam-dong Yusong-ku, Taejon 305-732, South Korea

Abstract

Key authentication is very important in secret communications and data security. Recently, Lee, Hwang and Li proposed a new public key authentication scheme for cryptosystems with a trusty server. However, in this paper, we will show that Lee–Hwang–Li's key authentication scheme is not secure, from the obtained public information, any one can get the private key of the user. And then, we propose an improved scheme. We conclude that our new key authentication scheme not only resolves the problems appeared but also is secure.

Keywords: Key authentication scheme; Cryptanalysis; Certificate; Password

1. Introduction

The public key cryptography was introduced by Diffie and Hellman in 1976 [1], in such cryptosystem, each user has two keys: a public key and a private key. There is a possible danger event in public key cryptosystem: an intruder can revise the public key from the public key directory and substitute the public key of a target user. In this way, the intruder can impersonate the public key of this target user and, hence, raise a security threat of fabrication. The purpose of key authentication is to verify the public key of a legal user and prevent a

* Corresponding author. Address: School of Information Technology and Computer Science Informatics, Room 234, Building 3, University of Wollongong, Wollongong, NSW 2522, Australia.
E-mail addresses: fgzh@hotmail.com, fangguo@uow.edu.au (F. Zhang), kkj@icu.ac.kr (K. Kim).

0096-3003/$ - see front matter
doi:10.1016/j.amc.2003.12.012

forged public key. Therefore, key authentication is very important in secret communications and data security.

Many key authentication schemes have been proposed. In 1996, Horng and Yang [2] proposed a key authentication scheme based on the discrete logarithm problem, but three years later, Zhan et al. [3] pointed out that Horng–Yang's scheme could not prevent from the guessing attack [4] and gave an improved scheme. In [5], Lee, Hwang and Li showed that Zhan et al.'s improved scheme did not achieve non-repudiation of user's public key (i.e., a dishonest legal user can deny his public key), and proposed a new public key authentication scheme for cryptosystems with a trusty server. Their scheme is based on discrete logarithm too, and in their scheme, the certificate of the public key is a combination of user's password and private key. The authors declared that their scheme was secure for the others public key authentication. However, in this paper, we shall show that Lee–Hwang–Li's key authentication scheme is not secure, from the obtained public information, any one can get the private key of the user. And then, we propose an improved scheme. Through our analysis, our new key authentication scheme not only resolves the problems appeared but also is secure.

The organization of this paper is as follows: In Section 2 we describe Lee–Hwang–Li's key authentication scheme, and in Section 3, we propose an attack on this scheme. We propose a new key authentication scheme in Section 4, in Section 5 we give an analysis of our new scheme. We make a concluding remark in the final section.

2. Lee–Hwang–Li's key authentication scheme

First of all, we review Lee–Hwang–Li's key authentication scheme in brief using the same notation as [5].

The user of the system has **Prv** as his/her private key and **PWD** as his/her password. Let **Pub** of the user's public key be

$$\mathbf{Pub} = g^{\mathbf{Prv}} \bmod p,$$

where p is a large prime, g is a generator in Z_p^*. The p, g and one-way function $f : f(x) = g^x \bmod p$ are public parameters.

In the user's registration phase, each user chooses a random number $r \in Z_p^*$ such that $\gcd((\mathbf{PWD} + r), \mathbf{Prv}) = 1$, and then calculates $f(\mathbf{PWD} + r)$. When $\gcd((\mathbf{PWD} + r), \mathbf{Prv}) = 1$, we can find two integers a and b such that the following equation holds:

$$a \times (\mathbf{PWD} + r) + b \times \mathbf{Prv} = 1.$$

The user then sends $f(\mathbf{PWD} + r)$, $R = g^r \bmod p$, a and b to the server secretly. $f(\mathbf{PWD} + r)$, a and b are stored in public password table in the server. The