Available online at www.sciencedirect.com
SCIENCE DIRECT®
ELSEVIER Applied Mathematics and Computation 164 (2005) 675–678
APPLIED MATHEMATICS AND COMPUTATION
www.elsevier.com/locate/amc

Comment: cryptanalysis of Lee–Hwang–Li's key authentication scheme

Da-Zhi Sun [a,*], Zhen-Fu Cao [a], Yu Sun [b]

[a] *Department of Computer Science, Shanghai Jiao Tong University, 1954 HuaShan Road, Shanghai 200030, PR China*
[b] *Department of Management, Beijing Normal University, Beijing 100875, PR China*

Abstract

Recently, Zhang and Kim proposed an improved key authentication scheme [Appl. Math. Comput., in press]. Zhang and Kim claimed that the proposed key authentication scheme achieves the non-repudiation service. However, we show that a dishonest user can forge his public key via the verification equation. Hence this scheme cannot achieve the non-repudiation service like the previous variants.

Keywords: Key authentication; Public key; Non-repudiation

1. Introduction

In a public key cryptosystem, all public keys are usually stored in a public file called a public key directory. The public key directory is very important yet vulnerable. A concern regarding the public key cryptosystem is that an intruder can impersonate a legal user by substituting his public key with a forged

* Corresponding author.
E-mail address: sundazhi@sjtu.edu.cn (D.-Z. Sun).

0096-3003/$ - see front matter
doi:10.1016/j.amc.2004.04.098

key. Hence many schemes have been proposed to solve the key authentication problem.

In 1996, Horng and Yang [1] gave a key authentication scheme for cryptosystems based on discrete logarithms. As an authority, the server has a secure password table to store each user's hash password $f(pwd)$, where pwd is the user's password and $f(\cdot)$ is a one-way function. The certificate of the user's public key is a combination of his password and private key. Three years later, Zhan et al. [4] pointed out that Horng–Yang's scheme is vulnerable to the guessing attack [3]. Therefore, Zhan et al. presented a revised scheme. In 2003, Lee et al. [2] noticed that Zhan et al.'s scheme does not provide the non-repudiation service for the user's public key. From this observation, a new public key authentication scheme was proposed. However, Zhang and Kim [5] recently showed that Lee–Hwang–Li's scheme is insecure since the user's private key can be derived from the obtained public information. To overcome this weakness and maintain the non-repudiation service, an improved key authentication scheme was also proposed.

In this paper, we demonstrate that a dishonest user can successfully deny his signature. That is, Zhang–Kim's scheme does not achieve non-repudiation of the user's public key claiming in [5].

2. Zhang–Kim's scheme

For a self-contained discussion, we first review Zhang–Kim's scheme.

The system parameters are as follows: Let p and q be prime numbers such that $q|p-1$. The one-way function f is defined by $f(x) = g^x \bmod p$, where g is a generator with order q in Z_p^*. The user has a private key prv and a corresponding public key $pub = g^{prv} \bmod p$. In addition, the user has a password pwd.

In the registration phase, each user chooses a random number $r \in Z_q^*$, and then calculates $f(pwd + r)$. The certificate C of the user's public key is as follows:

$$C = pwd + r + prv \times pub \bmod q. \tag{1}$$

The user then sends the parameters $f(pwd + r)$, $R = g^r \bmod p$ and his ID to the server secretly. The server verifies if $f(pwd + r) = f(pwd) \times R$ and verifies the $f(pwd + r)$ sent by the legal user, and then stores ID and $f(pwd + r)$ in public password table in the server. The public password table cannot be modified or forged by an attacker because the server uses the technique access control to protect it. The user's certificate C and public key pub are opened to the public over the network.

In the key authentication phase, when someone wants to communicate with a user, the sender first downloads the receiver's C, pub and $f(pwd + r)$, and then