Remarks on Zhang-Kim's Key Authentication Scheme

Jianhua Li and Jie Liu
(Corresponding author: Jie Liu)

Department of Electronic Engineering, Shanghai Jiao Tong University
No.1954, Hua Shan Rd., Xu Hui District, Shanghai, 200030, China (Email: ljiesh@gmail.com)

(Received Oct. 22, 2007; revised and accepted Jan. 4, 2008)

Abstract

Key authentication is very important in secret communications and data security. Lee et al. proposed a new public key authentication scheme for cryptosystems based on discrete logarithms in 2003. Recently, Zhang et al. pointed out that Lee et al.'s scheme was not secure and proposed an improvement on it. However, in this paper, we will demonstrate that a dishonest user can forge the public key via the verification equation in the improved scheme. Therefore, Zhang et al.'s scheme does not achieve non-repudiation of the user's public key.

Keywords: Key authentication, non-repudiation, number theory

1 Introduction

Key authentication is very important in a public key cryptosystem. In such cryptosystem, each user has two keys: a public key and a private key. There is a possible threat 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 user by means of his/her public key 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 forgery of the public key.

In 2003, Lee et al. [1] proposed a new public key authentication scheme (called the LHL-scheme) for cryptosystems based on discrete logarithms, which uses a server as an authority. The certificate of the user's public key is a combination of his/her password and private key. Later, Sun et al. [2] pointed out that the LHL-scheme does not achieve non-repudiation of the user's public key (i.e., a dishonest legal user can deny his public key). Recently, Zhang et al. [3] proved that the LHL-scheme was not secure. From the obtained public information, anyone can get the private key of the user. Zhang et al. also proposed an improved scheme to overcome this weakness (called the ZK-scheme).

In this paper, we will show that a dishonest user can successfully deny his signature in the ZK-scheme. That is, the ZK-scheme does not achieve non-repudiation of the user's public key either.

2 Review of the ZK-scheme

Similar to the LHL-scheme, the ZK-scheme also employs a password table that needs a trusted server.

The system parameters of the ZK-scheme are as follows: Let p and q are prime numbers such that $q|p-1$, g is a generator with order q in $\mathbb{Z}_p^*$. The one-way function f is defined by $f(x) = g^x \bmod p$. The p, q, and $f(x)$ are made public. 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 is:

$$Pub = g^{Prv} \bmod p.$$

During the registration phase, the certificate of the public key is generated by the user with his/her password and private key. Each user chooses a random number $r \in \mathbb{Z}_q^*$, and then calculates $f(PWD+r)$. The certificate C of the user's public key is:

$$C = PWD + r + Prv \cdot Pub \bmod q.$$

The user then sends $f(PWD+r)$, $R = g^r \bmod p$ and his/her ID to the server secretly. The server verifies them by checking whether the following verification equation holds:

$$f(PWD+r) = f(PWD) \times R \bmod p.$$

If the above equation holds, then the server stores ID and $f(PWD+r)$ in public password table. To protect against illegal modification, the server uses the access control mechanisms. The certificate C and the public key Pub are opened to the public over the network.

During the key authentication phase, the sender first downloads the receiver's certificate C, public key Pub and $f(PWD+r)$ from the public directory in the network and public password table in the server. Then the sender checks the certificate C of the public key by computing the following equation:

$$f(C) = f(PWD + r) \times Pub^{Pub} \bmod p. \qquad (1)$$

If the above equation holds, the sender accepts the public key Pub of the receiver; otherwise, the sender rejects it.

Obviously, this scheme works correctly.

3 Weakness of the Non-Repudiation Service

Dispute of digital signatures is a common problem that could jeopardize electronic commerce applications. Non-repudiation is an essential security attribute, which can provide evidence to enable dispute resolution. Unfortunately, the ZK-scheme does not achieve this attribute that secure key authentication schemes should achieve.

In the ZK-scheme, when the public key Pub is odd (a dishonest user can ALWAYS choose his private key Prv in such a way that Pub will be an odd number, and this will later allow him to cheat), a dishonest legal user can deny the signature signed using his private key Prv. To do this, the dishonest user does as follows:

Computes $Pub' = p - Pub$. We have

$$\begin{aligned}
& (Pub')^{Pub'} \bmod p \\
= \ & (p - Pub)^{(p-Pub)} \\
= \ & p^{p-Pub} + \binom{p-Pub}{1} \times p^{(p-Pub)-1} \times (-Pub) \\
& \quad + \cdots + \binom{p-Pub}{p-Pub-1} \times p \times (-Pub)^{(p-Pub)-1} \\
& \quad + (-Pub)^{(p-Pub)} \\
= \ & (-Pub)^{(p-Pub)} \\
= \ & (-Pub)^{(p-1)} \times (-Pub)^{(1-Pub)} \\
= \ & (-Pub)^{(1-Pub)} \bmod p.
\end{aligned}$$

Since Pub is odd, $1 - Pub$ is an even number. So we have

$$\begin{aligned}
& (-Pub)^{(1-Pub)} \bmod p \\
= \ & (Pub)^{(1-Pub)} \\
= \ & (g^{Prv})^{(1-Pub)} \\
= \ & g^{(Prv-Prv\times Pub)} \bmod p.
\end{aligned}$$

Let $C' = C+Prv-2\times Prv\times Pub \bmod q$ and substitutes the fabrication certificate C' and public key Pub' in the public key directory. We can verify that (C', Pub') will pass the verification Equation (1).

$$\begin{aligned}
& f(PWD + r) \times (Pub')^{Pub'} \bmod p \\
= \ & g^{(PWD+r)} \times g^{(Prv-Prv\times Pub)} \\
= \ & g^{(PWD+r+Prv-Prv\times Pub)} \\
= \ & g^{PWD+r+Prv\times Pub+Prv-2\times Prv\times Pub} \\
= \ & g^{C+Prv-2\times Prv\times Pub} \\
= \ & f(C') \bmod p.
\end{aligned}$$

So anyone will also be convinced of the integrity of the forged public key Pub' via the same previously mentioned checking Equation (1). However, the signature generated using Prv and verified using Pub, cannot be verified using the forged public key Pub'. As a result, the dishonest user can deny his signature. Therefore, we have shown that the ZK-scheme does not achieve the non-repudiation service.

References

[1] C. C. Lee, M. S. Hwang, and L. H. Li, "A new key authentication scheme based on discrete logarithms," *Applied Mathematics and Computation*, vol. 139, no. 2-3, pp. 343-349, July 2003.

[2] D. Z. Sun, Z. F. Cao, and Y. Sun, "Remarks on a new key authentication scheme based on discrete logarithms," *Applied Mathematics and Computation*, vol. 167, no. 1, pp. 572-575, Aug. 2005.

[3] F. G. Zhang, and K. Kim, "Cryptanalysis of Lee-Hwang-Li's key authentication scheme", *Applied Mathematics and Computation*, vol. 161, no. 1, pp. 101-107, Feb. 2005.

Jie Liu is now a Ph.D. candidate in the Department of Electronic Engineering, Shanghai Jiao Tong University, Shanghai, China. His current research interests include information security, network security and public key cryptography.

Jianhua Li received his M.S. and Ph.D. in Communication and Information System from Shanghai Jiao Tong University. He is now a professor in the Department of Electronic Engineering, Shanghai Jiao Tong University. His research interests include mobile communications, network management and information security.