International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Nagpur, INDIA

Cryptanalysis of Zuhua Shao key authentication scheme

P.Kumaraswamy a*, C.V.Guru Rao b, V.Janaki c, K.V.T.K.N. Prashanth d

a*Research Scholar , Dept. of CSE, JNTU Hyderabad, Telangana, India
bProfessor , Dept of CSE, SREC W, Warangal, Telangana, India
cProfessor , Dept of CSE, VCEW, Warangal, Telangana, India
dP.G. Scholar , Dept. of CSE, OU, Hyderabad, Telangana, India

Abstract

In public key cryptosystem, the protecting of public keys against intruders is very important. Usually, key authentication schemes are required to preserve public keys. Most of the key authentication schemes require one or more authorities to authenticate public keys. Some other key authentication schemes require no authorities to authenticate public keys. The Zuhua Shao proposed a new scheme to overcome the drawbacks of existing schemes, but it has some vulnerabilities. This scheme relies only on key server for certificate generation. In a distributed network, the server can easily impersonate other legitimate users and listen the messages directed to them. Moreover, in this scheme, users’ passwords are stored in the form of plaintext. In this paper, slight modifications are pointed out to overcome these severe drawbacks.

© 2016 The Authors. Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).
Peer-review under responsibility of organizing committee of the ICISP2015

Keywords: Key authentication; Discrete logarithms; Certificate; Public key cryptography; Key server

1. Introduction

Cryptography algorithms are divided into two broad categories: Symmetric key cryptography and Public key cryptography. In Symmetric key cryptography, two people should mutually agree on a cryptosystem and a secret key
which is to be distributed in a secure manner with the help of trusted key distribution center (KDC). If one person wants to transmit messages to the other, the mutually recognized secret key is used to encrypt and decrypt messages. The serious problem in symmetric key cryptosystem is the key distribution, in a secure manner. This problem is the motivation to develop the public-key cryptosystem. In public-key cryptography, two people mutually agree on a cryptosystem and generate a pair of different keys, named as public key and private key. The public key of each user is publicly available and is accessible through public-key directory. If a sender wants to transmit message he/she uses the public key of the receiver accessed from the public-key directory to encrypt the messages. When the receiver receives the encrypted messages, receiver uses his/her private key to decrypt the messages.

In the past, many schemes have proposed to provide assurance on public key of all the authorized users, such as ID based schemes [8], certificate-based schemes [9, 10], and self-certified public-key scheme [11]. But these schemes require one or more authorities as a trusted center or third party for ratification.

In 1996, Horng and Yang [6] proposed a key authentication scheme, HY-scheme, which uses a server as an authority. In their scheme, each user generates his/her certificate using the combination of password from the server and his/he private key. The server stores each user’s hashed password, f(PWD), where PWD is the password of the user and f() is a one-way hash function, in a table known as verification table or secure password table. Hence, the server cannot derive and know the PWD of the user because one-way functions are not reversible [12,13]. Three years later, Zhan et al.[5] proved that HY-scheme was prone to the password guessing attack [14]. Password guessing attacks can be classified into two. An improved scheme, ZLYH-scheme succeeded in preventing the guessing attack, but failed to achieve nonrepudiation. In 2003, a new key authentication scheme was proposed by Chi Lee, Shiang, Hwang and Hua Li [4], LHL-scheme, to achieve non-repudiation. It is based on the research work on key authentication schemes of HY-scheme [6] and ZLYH-scheme [5]. But the LHL-scheme has two security flaws, as suggested by A.Peinado in 2004 [2], the primary being the recovery of user’s private key from his/her certificate and other public values. The second significant drawback is certificate verification process is independent of certificate, for a given public key. Later, A.Peinado improved LHL-scheme through the use of access control equation for public key verification without generating the certificate.

In 2004, Zhang and Kim [3] independently performed cryptanalysis of LHL-scheme and proposed a modified LHL-scheme. Their scheme is based on three security parameters and it is almost hard to calculate private key from certificate and other public parameters. Also it prevents guessing attack and achieves nonrepudiation along with thorough certificate verification. Later in 2004, Zuhua Shao proposed a new key authentication scheme for cryptosystems based on discrete logarithms [1]. It is based on A. Peinado [2], Zhang and Kim [3] and LHL [4] research work. He proved that A. Peinado’s modification is not secure as it suffers from guessing attack and also revealed that Zhang and Kim’s scheme which is based on three security prerequisites is expensive in an open environment. To overcome these drawbacks, Zuhua Shao proposed a new scheme in which a trusted key server is used, to generate certificate for each legal user. However, Zuhua Shao scheme’s dependency on key server as a trusted third party is not secure when the server is compromised. Moreover, the availability of passwords in plaintext form of each user in server as (ID, PWD) pairs is not preferable as suggested by Purdy [15]. Hence it is preferable to utilize the one-way function to hide original password to improve the security.

The rest of the paper is organized as follows: Section 2 refers detailed discussion of Zuhua Shao scheme is presented and its drawbacks are highlighted in Section 3. Our proposal is explained in Section 4. Finally conclusion and future research is given in Section 5.

2. The Zuhua Shao key authentication scheme

This scheme [1] consists of three phases such as Setup phase, Registration phase, and Authentication phase which are described in the following sub sections.
2.1 Setup phase

In this scheme, the key server S chooses the following public parameters:

1. \( p \) is a large prime number.
2. \( q \) is a prime divisor of \( p - 1 \).
3. \( g \) is an element of order \( q \) in the finite field \( \mathbb{GF}(p) \).
4. \( h() \) is a one-way hash function
5. The public key \( y_s = g^{x_s} \mod p \) of the key server S, where \( x_s \) is the private key of the key server S.

2.2 Registration phase

Every user (U) has a password \( \text{PWD}_u \) to log into the system. The user (U) chooses his private key \( x_u \) and computes the corresponding public key \( y_u = g^{x_u} \mod p \). To place his public key \( y_u \) on the public key server S the user (U) does the following steps:

1. Choose a random integer \( r \) in \( \mathbb{Z}_q \).
2. Compute \( R = g^r \mod p \) \hspace{1cm} (1)
3. Compute \( w = y_u^{\text{PWD}_u + r} \mod p \) \hspace{1cm} (2)
4. Compute \( v = h(\text{ID}_u, y_u) x_u + rR \mod q \) \hspace{1cm} (3)
5. Send \((\text{ID}_u, y_u, w, v)\) to the key server S in a public channel.

After receiving \((\text{ID}_u, y_u, w, v)\), the key server S does the following steps:

6. Recover the password \( \text{PWD}_u \) of the user U by using user’s identity \( \text{ID}_u \).
7. Compute \( R'/ = w^{(x_s)-1} / g^{\text{PWD}_u} \mod p \) \hspace{1cm} (4)
8. Check \( g^{v} = y_u^{h(\text{ID}_u, y_u) R'} \mod q \) \hspace{1cm} (5)
9. If the check fails, S terminates the protocol run with failure. Otherwise Server does the following:
   (i) Choose a random integer \( k \) in \( \mathbb{Z}_q \).
   (ii) Compute \( K = g^k \mod p \) \hspace{1cm} e = h(\text{ID}_u, y_u, K) \hspace{1cm} (6)
   (iii) Compute \( C = k - e(y_u x_u + v) \mod q \) \hspace{1cm} (7)
   (iv) The information \((\text{ID}_u, y_u, R, C, e)\) of the user (U) are stored in the public key table hosted in the key server.

2.3 Authentication phase

When one requester inquires the public key for the user (U) with the identity \( \text{ID}_u \), the requester does the following steps:

1. Ask the key server S for the public key and the certificate of the user (U) with the identity \( \text{ID}_u \) in a public channel \((\text{ID}_u, y_u, R, C, e)\).
2. Compute \( K' = g^{C} (y_u^{x_s} y_u^{h(\text{ID}_u, y_u)} R')^e \mod p \) \hspace{1cm} (8)
3. Check \( h(\text{ID}_u, y_u, K') = e \).
By following the above procedure, if the step3 equation found true the requester accepts \( y_u \) as the authorized public key of the user (U).

The above scheme prevents the guessing attack and the security of the password table and user’s public key is obtained through Schnorr and ElGamal Digital signatures respectively [1]. Also it achieves correct verification of user’s public key certificate. This scheme does not require any of the security pre-requisites similar to this of Zhang and Kim’s scheme except that key server is considered as trusted by users.

3. Cryptanalysis of the Zuhua Shao scheme

According to Zuhua Shao Scheme the passwords (PWD) are stored in the server which is also responsible for generation of certificates. Due to this, we pointed out the following drawbacks in his scheme.

(1) The storage of a user’s identity (ID) and his/her password (PWD) as pair of (ID, PWD) in a plaintext format, but neither in encrypted nor in hashed form, is a major drawback of Zuhua Shao scheme. This is because, such type of storage is more prone to attacks by ill-minded users and intruders as suggested by Purdy [15].

(2) Moreover, the complete dependence on server for certificate generation, and availability of users’ passwords in plaintext format stored in the server, leads to a serious security flaw in case when the server is compromised.

As a result of the compromised server, a user with identity \( ID_u \) may get a false certificate \( C_f \) which is calculated by using false public key \( y_{uf} \) and the corresponding false private key \( x_{uf} \). Also, the compromised server chooses a false random number \( r_f \), and computes corresponding \( R_f \). Then as server knows password PWD\(_u\) of user with identity \( ID_u \), it calculates false \( w_f \) as \( w_i \) and false \( v_f \) as \( v_i \) which leads to following Scenario.

\[
w_f = y_s^{PWD_u + r_f} \mod p
\]
\[
v_f = h(ID_u, y_{uf}) x_{uf} + r_f R_f \mod q
\]

Then the server chooses random number \( K \) in \( Z_q \).

Calculates \( K = g^k \mod p \), \( e = h(ID_u, y_{uf}, K) \)

Then compute \( C_f = k - e(y_s x_s + v_f) \mod q \)

Then the dishonest server stores in its public password table the forged public key \( y_{uf} \) of the forged Certificate \( C_f \) (\( ID_u, y_{uf}, R_f, C_f, e \)). Any Sender who wants to communicate with the user with identity \( ID_u \) accesses the values in public password table and computes

\[
K' = g^{C_f} \left( y_s^{x_s} y_{uf}^{h(ID_u, y_{uf})} R_f^{R_f} \right) \mod p
\]

And Checks \( h(ID_u, y_{uf}, K') = e \).

This is proved according to Zuhua shao scheme [1]. These results in, that the sender considers the forged public key \( y_{uf} \) as legal public key of user with identity \( ID_u \) and encrypts messages with this false public key. These messages intended to user with \( ID_u \) are intercepted and read by the intruders.

We analyze that, the Zuhua Shao scheme is similar to a public key authentication scheme based on Certificate Authority. But, the prime requisite of earlier schemes like HY [6], ZLYH [5] and others is to secure users’ passwords in the server and to make users generate their own certificates without any trusted third party. But in...
Zuhua Shao scheme, by the involvement of sever in certificate generation and storing the passwords in plaintext form, his scheme has diverted from the prime requisites of earlier schemes.

4. Modifications to the Zuhua Shao scheme

In order to overcome the security weaknesses, the following modifications to the Zuhua Shao scheme are proposed.

(a) Each user can generate his/her certificate without involvement of the server, similar to the earlier schemes except in Zuhua Shao scheme.

(b) In Equation 7 the certification generation is done by the explicit involvement of private key $x_s$. But the certificate generation can be done without explicit involvement of private key. It increases the complexity to the attacker to obtain the exact private key from the certificate.

(c) The new scheme can be developed, where the key server as a trusty authority only for publishing and accessing resources but not as a certificate generator, which avoids the insecurity of public key.

5. Conclusion and Future research

Zuhua Shao scheme’s dependency on key server as a trusted third party is not secure when the server is compromised. Moreover, in this scheme, the availability of passwords in plaintext form of each user in server is not preferable in a network. The Zuhua Shao scheme is similar to a public key authentication scheme based on certificate authority. But, the prime requisite of earlier schemes is to secure users’ passwords in the server and each user has to generate his/her certificate without any trusted third party.

The proposal, we presented so far comprises a naive idea, to develop a secure key authentication scheme. By storing hashed passwords in the key server also provides high security for users’ passwords. We can also further strengthen the process of authentication by incorporating digital signature verification in registration and authentication phases of the scheme.

References