Defence Science Journal, Vol. 66, No. 6, November 2016, pp. 590-593, DOI : 10.14429/dsj.66.9649

Key Authentication Scheme-based on Discrete Logarithms and Chinese Remainder Theorem

P. Kumaraswamy*, C.V. Guru Rao, V. Janaki, and K.V.T.K.N. Prashanth

Department of Computer Science and Engineering, S.R. Engineering College, Warangal - 506 371, India
**E-mail: palleboina.kumar@gmail.com*

ABSTRACT

Public key cryptosystems are secure only when the authenticity of the public key is assured. Shao proposed a new scheme to overcome the problems of the existing schemes, which suffers from two major drawbacks. The first drawback is the availability of users' passwords in plaintext format in key server which are prone to attacks by ill-minded users. The second one is depending on the key server blindly for certificate generation, without further verification by the user. To overcome these severe drawbacks, we proposed an improved key authentication scheme based on Chinese remainder theorem and discrete logarithms. Our scheme allows the user to generate his/her certificate without the help of any trusted third party. This scheme is intended for online services, military and defense applications to exchange keys securely.

Keywords: Certificate, authentication, chinese remainder theorem, discrete logarithms, confidentiality, non-repudiation, public key cryptosystem

1. INTRODUCTION

There are two types of commonly used cryptosystems in cryptography[7]: Symmetric key and public key cryptosystems. In symmetric key cryptosystem, a secret key should be distributed in a secure manner between the sender and the receiver with the help of trusted key distribution center (KDC) whereas in public key cryptosystem the sender and the receiver have different keys which are called public key and private key. Key distribution is the main problem in symmetric key cryptosystem. To overcome the problem, public key cryptosystem was developed. But there is a possibility that an intruder can modify the public key of the authorised user in public key cryptosystem. It leads to key authentication problem.

HY-scheme was proposed by Horng and Yang[6] tried to address the key authentication problem. The server plays an important role in the HY-scheme. In the scheme the certificate is generated by each user using the combination of password from the server and his/her private key. But according to Zhanetal.[5] the HY-scheme was prone to the password guessing attack. So he proposed ZLYH-scheme in which the problem was addressed. The scheme succeeded in avoiding the guessing attack, but failed to achieve non-repudiation.

Lee[4], *et al.* proposed a new key authentication scheme called LHL-scheme to achieve non-repudiation and succeeded in doing so. But Peinado[2] pointed out two security problems in the LHL-scheme. The first problem is the recovery of user's private key from his/her certificate and other public values. The second problem is the certificate verification process is done independently without involvement of certificate, for a given public key. So he improved the LHL-scheme using access control equation for public key verification without generating the certificate. Later, the LHL-scheme was modified by Zhang and Kim[3] who individually performed cryptanalysis of the scheme. The important aspects of the modified LHL-scheme are that it prevents guessing attack, achieves non-repudiation and makes calculating private key from certificate and other public parameters very difficult.

Considering all the above mentioned schemes, Shao[1] proposed a new key authentication scheme which addresses the problems of earlier schemes.

However, Shao scheme suffers from two security problems. The first one is that it depends on key server as a trusted third party which is not secure when the server is compromised. The second one is that the users' passwords are available in plaintext form in the server is not preferable according to Purdy[8]. To overcome the drawbacks of Shao scheme and earlier schemes, we propose an improved key authentication scheme.

2. AN IMPROVED KEY AUTHENTICATION SCHEME

Every user is allowed to choose a unique identity called user id (ID) and a password (PWD) to login in to the system. In general the system keeps a password table in a key server for all the authentic users and uses the key server as an authority. The password table stores each user's hashed password, f (PWD), where PWD is the password of the user and f is a one-way function. Hence, the server cannot derive and know the PWD of the user. This proposal consists of three phases: Setup phase, registration phase and authentication phase and are described below:

Received : 01 April 2016, Revised : 03 June 2016
Accepted : 18 July 2016, Online published : 31 October 2016

2.1 Setup Phase

In this phase, the key server initialises the following public parameters.

(i) p, where p is a large prime number
(ii) q, where q is a large prime divisor of $p-1$
(iii) g, where g is a generator of order q in the Galois Field, GF(p).
(iv) f is a one way function defined as

$$f(x) = g^x \bmod p \quad (1)$$

2.2 Registration Phase

In this phase, the initialised parameters are considered for registration of every user. For registration, every user has to compute his/her public key and certificate.

First, to compute the public key (Pub) every user selects his/her private key (Prv) and applies function f on private key as follows.

$$Pub = f(Prv) = g^{Prv} \bmod p \quad (2)$$

Next, the certificate of the user is generated with the help of the following three steps.

Step1: In this step, set of new parameters are computed by the user as shown below.

(i) Choose a random number r in Z_q^*.
(ii) Compute S, R and T values using the parameters PWD, r and f as follows:
  (a) $S = f(PWD + r)$ (3)
  (b) $R = f(r)$ (4)
  (c) $T = f(PWD * r)$ (5)
(iii) Select two random numbers v_1 and v_2 in Z_q^*, which are co-prime
(iv) Apply the Chinese remainder theorem to compute a value X

$$X \equiv Prv \pmod{v_1} \quad (6)$$

$$X \equiv (PWD * r) \pmod{v_2} \quad (7)$$

The value X is unique in the modulo of $v_1 * v_2$. Select the minimum positive value of X out of all possible values of X.

(v) Once again select k_1 and k_2 values to satisfy the following two equations

$$X = Prv + k_1 * v_1 \quad (8)$$

$$X = (PWD * r) + k_2 * v_2 \quad (9)$$

(vi) Finally compute two more parameters α and β as follows

$$\alpha = g^{v_1} \bmod p \quad (10)$$

$$\beta = g^{v_2} \bmod p \quad (11)$$

The step1 computes the values of S, R, T, X, α, β, k_1 and k_2, and then the user sends his/her ID, Pub and all these values except X to the server for registration. All these values are encrypted with the public key of the key server to prevent the attackers from impersonation.

Step2: The key server verifies the received parameters S, R, T, α, β, k_1 and k_2 with the following access control equations, Eqn. (12) and Eqn. (13). The generation of Eqns.(12), (13), and (15) is clearly explained in the proof (mentioned below) of our proposed theorem.

$$S = f(PWD) * R \bmod p \quad (12)$$

$$Pub * \alpha^{k_1} = T * \beta^{k_2} \bmod p \quad (13)$$

If the values of the received parameters satisfy the above two equations, then the key server accepts them. The parameters T, α, β, k_1, k_2, ID and Pub are stored in public password table. The remaining parameters S and R are stored in secret password table. The parameters X, Prv, PWD are kept as secret values with the user. In case, the verification process by the key server fails, the parameters of the user are not stored and also the user is declared as unauthentic.

Step3: If the verification is successful in step2, then the user generates his/her certificate (C) with the parameters PWD, r, X, Pub, q, α and β as follows

$$C = [\alpha * (PWD * r) + \beta * X * Pub)] \bmod q \quad (14)$$

Now, each user registers his/her computed public key and certificate in public key directory (PKD) as a pair of (C, Pub) with his/her user ID. Then the registration process is completed successfully.

2.3 Authentication Phase

In this phase, if a user (sender) wants to communicate with the other user (receiver), he/she (sender) has to verify the ID along with C and Pub of the other user (receiver). First, the sender obtains the pair (C, Pub) of the receiver along with ID from public key directory, accesses all other parameters related to the user from public password table stored in the key server and verifies using the Eqn. (13) and the following Eqn. (15).

$$f(C) = \left[T^{\alpha}\right] * [T * \beta^{k_2}]^{\beta * Pub} \bmod p \quad (15)$$

If the above two equations are satisfied, the sender accepts the public key of the receiver otherwise, the sender rejects it.

The trustworthiness of proposed key authentication scheme is based on the proposed theorem and its verification.

Theorem: If the user, the key server and the requester follow the proposed scheme, the requester always accepts the public key.

Proof: From Eqn. (3) and Eqn. (4), we have

$$S = f(PWD + r)$$
$$= g^{PWD} * g^r$$
$$\therefore S = f(PWD) * R \bmod p.$$

Also, from Eqn. (5) and Eqns. (8) - (11), we have

$$f(X) = g^{Prv + k_1 * v_1} \bmod p = g^{PWD * r + k_2 * v_2} \bmod p$$

$$\Rightarrow g^{Prv} * (g^{v_1})^{k_1} \bmod p = g^{PWD * r} * (g^{v_2})^{k_2} \bmod p \text{ so}$$

$$\Rightarrow f(X) = pub * \alpha^{k1} = T * \beta^{k_2} \bmod p,$$

Moreover, from Eqn. (14) and above conclusion we have,

$$f(C) = g^{[\alpha * (PWD * r) + \beta * X * pub)]} \bmod p$$
$$= \left[g^{(PWD * r)}\right]^{\alpha} * \left[g^{X}\right]^{\beta * Pub} \bmod p$$
$$= \left[T^{\alpha}\right] * \left[f(X)\right]^{\beta * Pub} \bmod p$$

from Eqn. (5) and Eqn. (1)

$$f(C) = \left[T^{\alpha}\right] * [T * \beta^{k_2}]^{\beta * Pub} \bmod p \text{ from Eqn. (14)}$$

Hence the Eqns. (12), (13), and (15) are proved.

3. SECURITY AND PERFORMANCE ANALYSIS

3.1 Security Analysis

It verifies whether the fundamental services; confidentiality, authentication, non-repudiation and security of the public key, are provided and prove that our proposed

scheme is a secured one. The above services are described in detail as follows:

3.1.1 Confidentiality

Our scheme ensures the confidentiality by making it difficult to compute Prv from other public parameters as it involves discrete logarithm computation.

One significant feature of this scheme is that the certificate is generated without explicit involvement of Prv and it uses a unique value *X*, which is computed using Chinese remainder theorem. This new concept of our scheme increases the complexity to a hacker to obtain the exact private key from the certificate.

3.1.2 Authentication

To forge a public key in our scheme, the intruder has to calculate false certificate *C*' by substituting false public key Pub' in the Eqn. (15) which is computed as

$$C' = f^{-1}(\lceil T^{\alpha} \rceil * [T * \beta^{k_2}]^{\beta * Pub'}) \bmod q \quad (16)$$

The false certificate C' can also be calculated by substituting false public key Pub' from Eqn. (14) and C' which is written as

$$C' = \alpha * f^{-1}(f(PWD * r)) + \beta * f^{-1}(f(X)) * Pub' \bmod q \quad (17)$$

It is very difficult to generate the pair (C', Pub'), which satisfies Eqn. (16) or Eqn. (17) unless the intruder solves discrete logarithm. Even though, an intruder is successful in guessing the pair (C', Pub') to satisfy Eqn. (15) or Eqn. (16), it is impossible to satisfy Eqn. (13) with the same Pub' which is used in authentication phase in this scheme. Therefore, an intruder cannot get through the authentication phase and hence forging of public key is impossible in this scheme.

One more significant feature of this scheme is using two equations in the authentication phase to provide the security service authentication. The first equation is used to check the integrity of the parameters received from the public password table and the second equation proves the authenticity of the certificate and public key of a user (receiver).

3.1.3 Non-repudiation

In our scheme, A user signs a certificate C with his/her (Prv, Pub) key pair. This certificate C can be verified by anyone using the user's public key Pub. But an ill minded user may deny this later, by showing false certificate C' and corresponding false public key Pub' that satisfy equations in authentication phase. However, this is almost impossible in our scheme, because it is clear from Eqn.(16) and Eqn.(17) that computation of C' for a chosen Pub' involves discrete logarithm computation.

3.1.4 Security of the Public Key

The forgery of public key is possible in Zuhua Shao scheme when the server is compromised[9]. In our scheme, the forgery of public key by a compromised server is avoided because of two reasons: First is the key server does not provide the public key and Second is the key server has no right to generate or send certificate to the user. So, if the key server tries to change any parameters for false acceptance of public key and sends them to sender, this fraud will be detected at verification phase, as the modified parameters will fail the access control Eqn. (13) at sender's side. This is because the changed parameters will not be compatible with the public key accessed from PKD.

Hence, our scheme can detect the situation whether the key server is compromised or not. This is advantageous to avoid any security compromises and breach of confidentiality due to forged public key.

3.2 Performance Analysis

Performance analysis of Zuhua Shao scheme and proposed scheme is discussed as follows:

3.2.1 Zuhua Shao Scheme

The time complexity to generate certificate of public key of Zuhua Shao scheme is

$$O(2\,RAND + 8\,EXP + 3\,HASH + 1\,TRANS) \quad (18)$$

where RAND is the time taken to generate one random number, EXP is the time to compute one arbitrary exponential operation, HASH is time to compute hash of a single input using arbitrary hash function h() and TRANS is the sum of transmission and propagation delays of sending 4 parameters from user to server.

3.2.2 Proposed Scheme

The time complexity to compute certificate in our scheme is expressed as

$$O((2*m+1)RAND + (m+2)GCD + 6\,EXP) \quad (19)$$

where **m** is the number of iterations performed to select two random numbers v_1 and v_2 such that $gcd(v_1,v_2)=1$. The number of iterations **m** are significantly less as the probability[10] Prob[$(gcd(v_1,v_2)=1)$] is $6/\pi^2 \approx 0.6$. Hence it can be concluded that our scheme takes less number of iterations to converge (for selecting two random numbers that are co-prime).

It is observed that, the time complexity of our scheme is independent of hashing, transmission and propagation delays, compared to Zuhua Shao scheme (because certificate is computed by the user itself). And as Prob[$(gcd(v_1,v_2)=1)$] ≈ 0.6, It can be asserted that **m** will be sufficiently less to make the total time taken by this scheme, considerably less than that of Zuhua Shao scheme.

Table 1. Comparison of zuhua shao scheme and proposed scheme

Parameter	Zuhua Shao scheme	Proposed scheme
Confidentiality	Yes	Yes
Non-repudiation	Yes	Yes
Authentication	Yes	Yes
Time complexity to generate certificate	High	Moderate
Security of public key	No	Yes

3.2.3 Summary of Security and Performance Analysis

By the above analysis, it is confirmed that our proposed scheme provides all the security services. Also it is simpler to implement without a trusted third party and takes less computational effort to compute the certificate of user.

4. CONCLUSION

The paper proposes an improved key authentication scheme based on Chinese remainder theorem and discrete logarithms. The significant feature of this scheme is, the key server is used as a trusted authority only for publishing and accessing resources but not as a certificate generator. The scheme also allows the user to generate his/her certificate without the help of any trusted third party to prevent the forgery of public key by a compromised server. Besides this, the certificate calculation is done in lesser time comparing to the existing schemes. Therefore, our proposed scheme demonstrates an improved and trustworthy key authentication scheme for public key cryptosystem.

REFERENCES

1. Shao, Zuhua. A new key authentication for cryptosystems based on discrete logarithms. *Appl. Math. Comp.*, 2004, **167**, 143-152 . doi: 10.1016/j.amc.2004.06.109
2. Peinado, A. Cryptanalysis of LHL- key authentication scheme. *Appl. Math. Comp.*, 2004, **152**, 721–724. doi:10.1016/j.procs.2016.02.016
3. Zhang, F. & Kim, K. Cryptanalysis of Lee–Hwang–Li_s key authentication scheme. *Appl. Math. Comp.*, 2005, **161**, 101-107. doi:10.1016/j.amc.2003.12.012
4. Lee, Cheng-Chi; Hwang, Min-Shiang & Li, Li-Hua-. A new key authentication scheme based on discrete logarithms. *Appl. Math. Comp.*, 2003, **139**, 343-349. doi:10.1016/S0096-3003(02)00192-3
5. Zhan, B.; Li, Z.; Yang, Y.; & Hu, Z. On the security of HY-key authentication scheme. *Computer Communication*, 1999, **22**, 739–741. doi: 10.1016/S0140-3664(99)00032-8
6. Horng, G. & Yang, C.S. key authentication scheme for cryptosystem is based on discrete logarithms. *Computer Communication*, 1996, **19**, 848–850. doi: 10.1016/S0140-3664(96)01112-7
7. Schneier, Bruce. Applied cryptography. Ed 2nd., John Wiley & Sons, New York, 1996.
8. Purdy, G.B. A high security log-in procedure. Communications of the ACM, 1974, **17**, 442– 445. doi:10.1145/361082.361089
9. Kumaraswamy, P.; Guru Rao C.V.; Janaki, V. & Prashanth, K.V.T.K.N. Cryptanalysis of Zuhua Shao key authentication scheme. Procedia Computer Science, Elsevier B.V., 2016, pp. 95-99. doi:10.1016/j.procs.2016.02.016
10. Hardy, G.H.E. & Wright, M. An introduction to the theory of numbers. Ed 6th, Oxford University Press. Theorem, , 2008, pp. 332.

CONTRIBUTORS

Mr P. Kumaraswamy, pursuing his PhD in Computer Science and Engineering at JNT University, Hyderabad, Telangana, India. He is an Assistant Professor in the Department of Computer Science and Engineering, S.R. Engineering College, Warangal, India. His research interest includes Cryptography, Information security and Computer networks.

Dr C.V. Guru Rao, Received his PhD in Computer Science and Engineering from IIT , Kharagpur, India. He is a professor in Computer Science and Engineering, Department, S.R. Engineering college Warangal. His research interests are related to Embedded system, Computer networks, Information security and Data Mining. A text book titled 'The Design and Analysis of Algorithms, 2e' authored by Anany Levitin was adapted by him in tune to the Indian standards and it was published by Pearson Education India.

Dr V. Janaki, received her PhD in Computer Science and Engineering from JNT University, Hyderabad, Telangana, India. She is Professor and HOD of CSE Department, Vaagdevi Engineering College, Warangal. Her research interest includes network security, cryptography, image processing, biometrics, pattern recognition.

Mr K.V.T.K.N Prashanth, pursuing his Master of Technology in Computer Science and Engineering in the Osmania University, Hyderabad, Telangana, India. He is a P.G. research scholar. His research interest includes cryptography, information security and Machine Learning.