ELSEVIER Applied Mathematics and Computation 139 (2003) 343–349

APPLIED MATHEMATICS AND COMPUTATION

www.elsevier.com/locate/amc

A new key authentication scheme based on discrete logarithms ☆

Cheng-Chi Lee [a], Min-Shiang Hwang [b,*], Li-Hua Li [b]

[a] *Department of Computer and Information Science, National Chiao-Tung University, 1001 Ta Hsueh Road, Hsinchu, Taiwan, ROC*

[b] *Department of Information Management, Chaoyang University of Technology, 168 Gifeng E. Rd., Wufeng, Taichung County 413, Taiwan, ROC*

Abstract

In this article, we propose a new public key authentication scheme for cryptosystems with a trusty server. The scheme is based on discrete logarithms. In the scheme, the certificate of the public key is a combination of user's password and private key. The scheme not only resolve the problems appeared but also is secure for the others public-key authentication.

Keywords: Key authentication; Public key; Certificate; Password

1. Introduction

There are two types of commonly used cryptosystem in cryptography [17]: secret key and public-key cryptosystems. In secret key cryptosystem, two people mutually agree on a cryptosystem and a secret key. The agreed key must be distributed in secret. If one person wants to transmit messages to the other, the mutually recognized secret key will be used to encrypt and decrypt messages. However, in public-key cryptosystem, two people mutually agree on a cryptosystem and generate a pair of different keys, the encryption and the

☆ This research was partially supported by the National Science Council, Taiwan, ROC, under contract no. NSC90-2213-E-324-004.

* Corresponding author.

E-mail addresses: mshwang@mail.cyut.edu.tw, mshwang@cyut.edu.tw (M.-S. Hwang).

0096-3003/02/$ - see front matter
PII: S0096-3003(02)00192-3

decryption keys, also named as public key and private key. The public key of each user is opened and can be accessed in the public-key directory. If a user wants to transmit messages to the other, the sender use the public key of the receiver accessed from the public-key directory to encrypt the messages. When the receiver receives the encrypted messages, he/she uses the private key to decrypt the messages.

A possible danger event in public-key cryptosystem is worth to notice as follows: 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 to prevent a forged public key. In the past, there are many schemes had been proposed to deal achieve the authentication goal, such as ID-based schemes [18], certificate-based schemes [12,19], and self-certified public-key scheme [3]. These schemes all require one or more authorities as a trusted center or third party for ratification.

In 1996, Horng and Yang [4] proposed a key authentication scheme, HY-scheme, that uses a server as an authority. In their scheme, the certificate uses the combination of password from particular server and private key of a user. The server has a secure password or verification table to store each user's hashing password, $f(\mathrm{PWD})$, where PWD is the password of the user and $f(\cdot)$ is a one-way function. Hence, the server cannot derive and know the PWD of the user because one-way function cannot inverse [1,15].

Three years later, Zhan et al. [20] point out that HY-scheme cannot prevent from the guessing attack [13]. An improved scheme, ZLYH-scheme [20] is therefore proposed. In their scheme, an intruder cannot use guessing attack to obtain password and forge a public key of a user. However, ZLYH-scheme does not achieve non-repudiation of user's public key. We will explain it in Section 4.

To prevent this problem, we shall propose a new key authentication scheme which is based on ZLYH-scheme but enhanced with the discrete logarithm technique [2,14]. Our scheme achieves not only a highly secure process but also the non-repudiation of user's public key. In addition, our scheme also uses a server as an authority which is the same as that of HY-scheme and ZLYH-scheme. The server also has a secure password or verification table which is also the same as that of HY-scheme and ZLYH-scheme. In addition, our scheme has a public password table to store each user's hashing password, $f(\mathrm{PWD}+r)$, where PWD is the password of the user; r is a random number generated by each user, and $f(\cdot)$ is a one-way function. We will explain it in Section 3.

The rest of the paper is organized as follows. In the next section, we give a brief review of password authentication system (PAS). In Section 3, a new key authentication scheme, based on the discrete logarithms, is presented. In

Section 4, we discussion the security of our scheme. Finally, conclusions are given in Section 5.

2. Summary of password authentication system

PAS has become popular in our society. The purpose of this system is to authenticate a legal user and to prevent any intruding from illegal users. In general, each user in PAS have a pair of message (ID, PWD), where ID is a user's identity and PWD is his/her password which is used to login into the system. When a user wants to access the resource from the system, he/she enters his/her (ID, PWD) to acquire the admission. Once the system receives the message, it checks if (ID, PWD) is registered and legal. If it is legal, the user then enters the system, otherwise, the user is rejected. The implementation of the previous process is that the system keeps a password table of paired (ID, PWD) of all the users. However, this method brings out a problem that once ill-minded user gains access to the password table, he/she can obviously endanger the who system [5–8].

To overcome this problem, a solution is proposed by Purdy [16] which utilizes a one-way function [2] to hide the original password and makes the information stored in the table difficult to solve, and, hence, protects the system from the intruder. An example of a password table is shown in Table 1.

3. A new key authentication scheme

In [4], Horng and Yang proposed a key authentication scheme, HY-scheme, that is so based on the password table that need a trusted server. However, HY-scheme cannot prevent from the guessing attack [13]. To prevent this, an improved scheme [20], ZLYH-scheme, is proposed by Zhan et al. They only added a long random number to prevent from the guessing attack. However, ZLYH-scheme is not achieve non-repudiation. We will explain it in Section 4. In this paper, we propose a new key authentication for non-repudiation. Our scheme is based on discrete logarithm. Our scheme also uses a trusted server as an authority.

Table 1
An example of a password table

User	Identity	Password
U_1	ID_1	$f(PWD_1)$
U_2	ID_2	$f(PWD_2)$
$\vdots$	$\vdots$	$\vdots$
U_n	ID_n	$f(PWD_n)$

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

$$\mathrm{Pub} = g^{\mathrm{Prv}} \bmod p, \tag{1}$$

where p is a large prime, g is a generator in Z_p^* and Prv is the user's private key. The p, g and one-way function f are public parameters. We assume that the one-way function f is

$$f(x) = g^x \bmod p. \tag{2}$$

In the user's registration phase, the certificate of the public key of the user is generated by the user with his/her password and private key. Each user chooses a random number r in Z_p^* such that the greatest common divisor of $(\mathrm{PWD} + r)$ and Prv, denoted $\gcd((\mathrm{PWD} + r), \mathrm{Prv})$, is equal to 1 and then calculates $f(\mathrm{PWD} + r)$. When $\gcd((\mathrm{PWD} + r), \mathrm{Prv}) = 1$, we can find two integers a and b such that the following equation holds [17]:

$$a(\mathrm{PWD} + r) + b\,\mathrm{Prv} = 1. \tag{3}$$

The user then sends $f(\mathrm{PWD} + r)$, $R = g^r \bmod p$, a, and b to the server secretly. $f(\mathrm{PWD} + r)$, a, and b are stored in public password table in the server. The public password table cannot modify or forge by an attacker because the server can use the technique access control to protect it [9–11]. The server then verifies if $f(\mathrm{PWD} + r) = f(\mathrm{PWD}) \times R$ and then verifies if $f(\mathrm{PWD} + r)^a \cdot \mathrm{Pub}^b = g \bmod p$. If the equations are equal, the server then verifies the $f(\mathrm{PWD} + r)$, a, and b sent by the legal user. The certificate C of user's public key is as follows:

$$C = \frac{(\mathrm{PWD} + r)}{f(\mathrm{PWD} + r) + \mathrm{Prv}} \bmod (p - 1). \tag{4}$$

The certificate C and public-key Pub of the user are opened to public in network. The $f(\mathrm{PWD} + r)$, a, and b are opened to public in the server that protected by the server using access control.

In the key authentication phase, when someone wants to communicate with a user, the sender first obtains C, Pub, a, b, and $f(\mathrm{PWD} + r)$ of the receiver from the public directory in network and public password table in the server, and then checks the certificate C of the public key of the receiver by computing the following equation:

$$\begin{aligned} f(C) &= f(\mathrm{PWD} + r)^{a \times C} \times \mathrm{Pub}^{b \times C} \bmod p \\ &= g^{a \times (\mathrm{PWD} + r) \times C} \times g^{b \times \mathrm{Prv} \times C} \bmod p \\ &= g^{a \times (\mathrm{PWD} + r) \times C + b \times \mathrm{Prv} \times C} \bmod p \\ &= g^{C \times (a \times (\mathrm{PWD} + r) + b \times \mathrm{Prv})} \bmod p = g^C \bmod p. \end{aligned} \tag{5}$$

If the above equation holds, the sender accepts the public-key Pub of the receiver to encrypt the transmission message, otherwise, the sender rejects the Pub of the receiver.

4. Security analysis

Our scheme provides verification of a user's public key. Preventing the impersonation of a public key is managed through the difficulty of discrete logarithm computing. If an intruder attempts to forge a user's public key, he/she must obtain the user's PWD and r. In our scheme, the forger can only determine $f(\mathrm{PWD}+r)$, and he/she cannot modify and forge it because it is protected by the server using the access control [9–11]. If the intruder attempts to forge the user's public key, he/she will be required to solve the discrete logarithms problem from Eq. (5).

In general, an intruder may try to use a guessing attack to obtain the PWD and r of the user. However, it is difficult to guess the PWD and r simultaneously, because the r is a very long random number. Since the intruder cannot obtain the PWD and r of the user, he/she cannot forge the user's public key. In order to forge someone's public key, an intruder must substitute Pub' for the user's public key and calculate C' of the user's public-key certificate. He/she must compute the equation:

$$f(C') = f(\mathrm{PWD}+r)^{a\times C'} \times \mathrm{Pub}'^{(b\times C')} \bmod p. \tag{6}$$

or

$$C = \frac{f^{-1}(f(\mathrm{PWD}+r))}{f(\mathrm{PWD}+r)+f^{-1}(\mathrm{Pub}')} \bmod (p-1). \tag{7}$$

It is difficult to generate the set, (C', Pub'), such that Eqs. (6) and (7) hold unless the intruder can solve the discrete logarithm problem [2,14]. Here, an intruder can only access the public directory in the network. Therefore, he/she can substitute Pub' and C'. However, he/she cannot access the $f(\mathrm{PWD}+r)$, a, and b because those are protected by the server using access control [9–11].

Another impossible attack is that an attacker may try to derive PWD or Prv from Eq. (3). However, this attack cannot work because the attacker does not know r and he/she must guest two values PWD and Prv simultaneously. Although the attacker knows a and b from public password table, he/she cannot also to derive $(\mathrm{PWD}+r)$ and Prv from Eq. (3) because it has too many combinations in Eq. (3). For example, Let $a=3$ and $b=-2$, the combinations are $\{(1,1),(3,4),(5,7),\ldots\}$. Hence, the attacker does know which the combination is right. Furthermore, $(\mathrm{PWD}+r)$ is protected by the one-way function $f(\cdot)$. Any one cannot derive $(\mathrm{PWD}+r)$ from $f(\mathrm{PWD}+r)$.

Our scheme does not have the two weaknesses that appeared in HY and ZLYH-schemes.

(1) In the HY-scheme [4], an intruder can guess the user's PWD using the guessing attack [13]. Then he/she can obtain the user's private key. Henceforward, an intruder can forge the user's public key. In our scheme, if an intruder attempts to forge the user's public key, he/she must simultaneously guess r and PWD. This is difficult because r is a very long random number. Therefore, an intruder cannot use the guessing attack in our scheme to forge the user's public key.

(2) The ZLYH-scheme [20] does not achieve non-repudiation of the user's public key. In order to explain why their scheme does not achieve the non-repudiation, we briefly introduce the ZLYH-scheme first. The ZLYH-scheme is similar to our scheme except Eqs. (3)–(5) are different. In the ZLYH-scheme, the certificate C of user's public key is

$$C = \mathrm{PWD} + \mathrm{Prv} + r \bmod (p-1). \tag{8}$$

And the verification of the public-key certificate C is

$$f(C) = f(\mathrm{PWD} + r) \times \mathrm{Pub} \bmod p. \tag{9}$$

If the above equation holds, the sender accepts the public-key Pub, otherwise, the sender rejects the public key.

We consider a case in which a dishonest legal user, has a pair public–private keys (Pub, Prv), uses his/her private key Prv to generate his/her signature for a document. Anyone can verify that signature using the signer's public-key Pub. However, the dishonest user can deny the signature later. Since, the signer, knows his/her $f(\mathrm{PWD} + r)$, he/she can choose a C' to derive the Pub$'$ using

$$\mathrm{Pub}' = \frac{f(C')}{f(\mathrm{PWD} + r)} \bmod p. \tag{10}$$

The dishonest user can substitute the fabrication C' and Pub$'$ in the public directory. The signer and others can also show that Pub$'$ is his/her public key using Eq. (9). Thus, the signatures, generated using Prv and verified using Pub, cannot be verified using the forged public key Pub$'$. Henceforth, the dishonest user can deny his/her signatures. Therefore, the ZLYH-scheme [20] does not achieve the non-repudiation of the user's public key. In our scheme, a dishonest legal user cannot derive another legal C' and Pub$'$ even if he/she knows $f(\mathrm{PWD} + r)$, a, and b. It had explained in the above Eq. (6). Therefore, our scheme can achieve non-repudiation of the user's public key.

5. Conclusions

Key authentication scheme can authenticate the public key of the user. In this paper, we have proposed a new key authentication scheme which is based on discrete logarithms. In our scheme, we resolve the problems appeared in

HY-scheme as guessing attack and ZLYH-scheme as non-repudiation. Our scheme not only withstands the guessing attack but also achieves non-repudiation of the user's public key. Our scheme is highly secure than HY-scheme and ZLYH-scheme.

References

[1] I.B. Damgard, A design principle for hash functions, in: Advances in Cryptology-CRYPTO'89 Proceedings, Springer-Verlag, 1990, pp. 416–427.
[2] W. Diffie, M.E. Hellman, New directions in cryptography, IEEE Transactions on Information Theory IT-22 (1976) 644–654.
[3] M. Girault, Self-certified public keys, in: Advances in Cryptology, EUROCRYPT'91, Lecture Notes in Computer Science, 1991, pp. 491–497.
[4] G. Horng, C.S. Yang, Key authentication scheme for cryptosystems based on discrete logarithms, Computer Communications 19 (1996) 848–850.
[5] M.-S. Hwang, Cryptanalysis of remote login authentication scheme, Computer Communications 22 (8) (1999) 742–744.
[6] M.-S. Hwang, Aremote password authentication scheme based on the digital signature method, International Journal of Computer Mathematics 70 (1999) 657–666.
[7] M.-S. Hwang, C.-C. Lee, Y.-L. Tang, An improvement of SPLICE/AS in WIDE against guessing attack, International Journal of Informatica 12 (2001) 297–302.
[8] M.-S. Hwang, L.H. Li, A new remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics 46 (1) (2000) 28–30.
[9] M.-S. Hwang, W.-G. Tzeng, W.-P. Yang, An access control scheme based on chinese remainder theorem and time stamp concept, Computers and Security 15 (1) (1996) 73–81.
[10] M.-S. Hwang, W.-P. Yang, A new dynamic access control scheme based on subject-object-list, Data and Knowledge Engineering 14 (1) (1994) 45–56.
[11] M.-S. Hwang, W.-G. Tzeng, W.-P. Yang, A two-key-lock-pair access control method using prime factorization and time stamp, IEICE Transactions on Information and Systems E77-D (9) (1994) 1042–1046.
[12] M. Kohnfelder, A method for certification, in: Tech. Rep. (MIT Laboratory for Computer Science), MIT Press, Cambridge, MA, 1978.
[13] G. Li, M.A. Lomas, R.M. Needham, J.H. Saltzer, Protecting poorly chosen secrets from guessing attacks, IEEE Journal on Selected Areas in Communications 11 (1993) 648–656.
[14] U.M. Maurer, Y. Yacobi, A non-interactive public-key distribution system, Designs, Codes and Cryptography 9 (3) (1996) 305–316.
[15] R. Merkle, One-way hash functions and DES, in: Advances in Cryptology CRYPTO'89, Lecture Note in Computer Science, vol. 435, 1989, pp. 428–446.
[16] G.B. Purdy, A high security log-in procedure, Communications of the ACM 17 (1974) 442–445.
[17] Bruce Schneier, Applied Cryptography, second ed., John Wiley & Sons, New York, 1996.
[18] A. Shamir, Identity based cryptosystems and signature schemes, in: Advances in Cryptology, CRYPTO'84, Lecture Notes in Computer Science, 1984, pp. 47–53.
[19] G. Simmons, Contemporary Cryptology: The Science of Information Integrity, IEEE Press, 1992.
[20] B. Zhan, Z. Li, Y. Yang, Z. Hu, On the security of HY-key authentication scheme, Computer Communications 22 (1999) 739–741.