Available online at www.sciencedirect.com

SCIENCE DIRECT®

Computer Networks 49 (2005) 535–540

Computer Networks

www.elsevier.com/locate/comnet

Efficient remote user authentication scheme using smart card

Rongxing Lu *, Zhenfu Cao

Department of Computer Science, Shanghai Jiao Tong University, 1954 Huashan Road, Shanghai 200030, PR China

Received 16 July 2004; received in revised form 16 July 2004; accepted 26 January 2005
Available online 7 March 2005

Responsible Editor: D. Frincke

Abstract

In this paper, we propose a new remote user authentication scheme using smart card. In our scheme, there are two attractive features: (i) no verification tables are required in the remote server; (ii) only one hash function computation and one modular multiplication computation are costed in smart card. Therefore, compared with other schemes, our scheme is more efficient.

Keywords: Cryptography; Remote login; Password authentication; Smart card

1. Introduction

With the rapid growth of computer network, more and more people have recourse to remote server's service in a distributed computer environment. However, since the data transmitted over an insecure channel without adequate protection is vulnerable to potential attacks from eavesdropping, illegal retrieval, and intended modification, etc, the security issue has gradually become a big concern in computer network.

In the last two decades, to protect the remote server from these malicious attacks, many elegant authentication schemes have been proposed [1–5]. However, some schemes [1,2,4,5] have to maintain a password verification table in the remote server for checking the legitimacy of the login users. And just as the password verification table maintained in the remote server, these schemes will suffer from the potential risks. For instance, if the verification table is modified by a malicious adversary, the system will be entirely broken. Hereby, to protect and maintain such a verification table, the relevant cost in the server will be rather high.

* Corresponding author. Tel.: +86 21 62932951; fax: +86 21 62932902.

E-mail addresses: rxlu@cs.sjtu.edu.cn (R. Lu), cao-zf@cs.sjtu.edu.cn (Z. Cao).

1389-1286/$ - see front matter © 2005 Elsevier B.V. All rights reserved.
doi:10.1016/j.comnet.2005.01.013

In 2000, Hwang and Li [6] proposed a new remote user authentication scheme using smart card, in which the remote server only keeps a secret key for computing the user passwords and doesn't need to maintain any verification table for verifying legal user. However, there is a weakness in the scheme as pointed out by the literatures [7,8], an evil user can easily impersonate other user to log in the system. To overcome such a weakness, Shen et al. [9] proposed a modified version and claimed it is secure against these attacks. But Leung et al. [10] showed the weakness still exists in Shen–Lin–Hwang's scheme.

Motivated by the mentioned above, in this paper, we would like to propose a new remote user authentication scheme using smart card. As it is based on the factorization problem and one-way hash function, the security can be guaranteed. At the same time, as it doesn't require modular exponentiation computations, it is more efficient than Hwang–Li's scheme.

The rest of the paper is organized as follows. In Section 2, we review Hwang–Li's scheme. Then we propose our scheme in Section 3. In Sections 4 and 5, we will analyze the scheme's security and performance, respectively. Finally, concluding remarks are made in Section 6.

2. Review of Hwang–Li's scheme

In 2000, Hwang and Li [6] proposed a password based remote user authentication scheme by using smart cards. In their scheme, the server only keeps a secret key for computing the user password, and no verification tables are required for verifying legal user. Here, we will first briefly review this scheme.

Hwang–Li's scheme consists of the following three phases: registration, login and authentication.

1. *Registration phase*
   The remote server first prepares some system parameters as follows:
   - p: a large prime number;
   - x_s: a secret key maintained by the server;
   - $h(\cdot)$: a one-way hash function.

   Suppose a new user U_i wants to register the server, he first submits his identity ID_i to the server. After the identity ID_i is identified, the server computes the user password PW_i for U_i, where $PW_i = ID_i^{x_s} \pmod p$.

   Then, the system issues the smart card, which contains the public parameters $(p, h(.))$, and PW_i to the user via a secure channel.
2. *Login phase*
   User U_i attaches his smart card to the login device and keys in his ID_i and PW_i. Then, the smart card will perform as follows:
   (a) select a random number r;
   (b) compute $C_1 = ID_i^r \pmod p$;
   (c) compute $t = h(T \oplus PW_i) \pmod{p-1}$, where T is the current date and time T of the login device and $\oplus$ denotes the exclusive or (XOR) operation;
   (d) compute $M = (ID_i)^t \pmod p$;
   (e) compute $C_2 = M(PW_i)^r \pmod p$;
   (f) send a message $C = (ID_i, C_1, C_2, T)$ to the remote server.
3. *Authentication phase*
   Suppose that the remote server receives the message C at T', where T' is the current date and time of the system.
   (a) check the validity of identity ID_i, if the format of ID_i is incorrect, the login request will be rejected;
   (b) check the time interval between T and T', if $(T' - T) \geqslant \Delta T$, where ΔT is the expected legal time interval for transmission delay, the server will reject the login request;
   (c) check $C_2(C_1^{x_s})^{-1} \overset{?}{=} (ID_i)^{f(T \oplus PW_i)} \bmod p$. If it holds, the server will accept the login request. Otherwise, the request will be rejected.

Although Hwang–Li's scheme doesn't need to maintain any verification tables in remote server, yet it suffers from an impersonation attack [7–10]. An evil user U_i with (ID_i, PW_i) can easily obtain another valid (ID_v, PW_v) by the following tricks:

- select a random number r;
- compute $ID_v = ID_i^r \pmod p$;
- compute PW_v, where

$$PW_v = ID_v^{x_s} \bmod p = ID_i^{r \cdot x_s} \bmod p = PW_i^r \bmod p.$$

Then, (ID_v, PW_v) is another valid pair. As a result, the evil user U_i can freely use it to login to the remote system.

3. Efficient remote user authentication scheme

In this section, based on an improved Rabin signature scheme, we will propose a new efficient remote user authentication scheme using smart card.

3.1. Improved Rabin signature scheme

Here, let us first review the improved Rabin signature scheme [11]. For convenience, it can be depicted as follow:

Let p and q be two security large primes, satisfying $p \equiv q \equiv 3 \pmod 4$. Compute $n = p \cdot q$ and select a parameter a satisfying Jacobi symbol $\left(\frac{a}{n}\right) = -1$. Then, the private key is (p,q) and the corresponding public key is (n,a). Besides, a cryptographic one-way hash functions $H : \{0,1\}^* \to \mathbb{Z}_n^*$ is also published.

- *Signing algorithm*
  Assume a message $m \in \{0,1\}^*$ should be signed. The signer will run the following steps:
  1. compute $H(m)$ and c_1, where
  $$c_1 = \begin{cases} 0 & \text{if } \left(\frac{H(m)}{n}\right) = 1, \\ 1 & \text{if } \left(\frac{H(m)}{n}\right) = -1. \end{cases}$$
  2. compute $t = a^{c_1} \cdot H(m)$ and c_2, where
  $$c_2 = \begin{cases} 0 & \text{if } \left(\frac{t}{p}\right) = \left(\frac{t}{q}\right) = 1, \\ 1 & \text{if } \left(\frac{t}{p}\right) = \left(\frac{t}{q}\right) = -1. \end{cases}$$
  3. compute $r = (-1)^{c_2} \cdot a^{c_1} \cdot H(m)$ and obtain four distinguishable solutions of the congruence $s^2 \equiv r \bmod n$. Since these solutions are computed by the Chinese Remainder Theorem, they can be distinguished as four cases:
  $$\begin{cases} s_1 & \text{if } \left(\frac{s_1}{p}\right) = \left(\frac{s_1}{q}\right) = 1, \\ s_2 & \text{if } \left(\frac{s_2}{p}\right) = \left(\frac{s_2}{q}\right) = -1, \\ s_3 & \text{if } \left(\frac{s_3}{p}\right) = 1 \quad \text{and} \quad \left(\frac{s_3}{q}\right) = -1, \\ s_4 & \text{if } \left(\frac{s_4}{p}\right) = -1 \quad \text{and} \quad \left(\frac{s_4}{q}\right) = 1. \end{cases}$$

In this signature scheme, the signer always chooses s_1 as the required solution s^*, then the signature on message m is (s^*, c_1, c_2).

- *Verifying algorithm*
  Any verifier can verify the signature (s^*, c_1, c_2) by the following equation
  $$s^{*2} \equiv (-1)^{c_2} \cdot a^{c_1} \cdot H(m) \bmod n,$$
  If it holds, the signature will be accepted, otherwise rejected.

Obviously, the improved Rabin signature scheme is based on the hardness of factorization problem. In the next subsection, we will use it to construct an efficient remote user authentication scheme using smart card.

3.2. The proposed scheme

The proposed scheme consists of four phases: the initialization, the registration, the login and the authentication phases. In below, these phases will be described in detail.

1. *Initialization phase*
   To set up a remote system, the remote server first prepares the following parameters:
   - p, q: two distinct security large primes, satisfying $p \equiv q \equiv 3 \bmod 4$;
   - $n : n = p \cdot q$;
   - a: a random number in $\mathbb{Z}_n^*$, satisfying $\left(\frac{a}{n}\right) = -1$;
   - $H : \{0,1\}^* \to \mathbb{Z}_n^*$ is one-way hash function;
   - $H_1 : \{0,1\}^* \times \mathbb{Z}_n^* \to \mathbb{Z}_n^*$ is another one-way hash function.

   Then, the remote server can accept the user registration request operation.

2. *Registration phase*
   When a new user U_i submits his identity ID_i to the remote server for registration. The server will do the following:
   (a) check the validity of ID_i. If it is valid, the operation will continue, otherwise stop;
   (b) use the improved Rabin signature scheme in Section 3.1 to compute (s^*, c_1, c_2), where $s^{*2} \equiv (-1)^{c_2} \cdot a^{c_1} \cdot H(ID_i) \pmod n$ and $(\frac{s^*}{p}) = (\frac{s^*}{q}) = 1$;
   (c) set the user password $PW_i = s^*$ and store the public parameters (n, H_1) to a smart card;
   (d) issue the smart card and PW_i to the user via a secure channel.
3. *Login phase*
   User U_i attaches his smart card to the login device and keys in his ID_i and PW_i. Then, the smart card will perform as follows:
   (a) select a random number $r \in_R \mathbb{Z}_n^*$;
   (b) compute $c \equiv r \cdot PW_i \pmod n$;
   (c) pick up the current date and time T of the login device;
   (d) compute $h = H_1(T, r)$;
   (e) send a message $C = (ID_i, T, c, h)$ to the remote server.
4. *Authentication phase*
   Suppose that the remote server receives the message C at T', where T' is the current date and time of the system.
   (a) check the time interval between T and T', if $(T' - T) \geqslant \Delta T$, where ΔT is the expected legal time interval for transmission delay, the server will reject the login request;
   (b) check the validity of identity ID_i, if the format of ID_i is incorrect, the login request will be rejected;
   (c) use the same way in the registration phase to compute the user password PW_i;
   (d) compute $r \equiv c \cdot PW_i^{-1} \pmod n$;
   (e) check $h \overset{?}{=} H^1(T, r)$. If it holds, the server will accept the login request. Otherwise, the request will be rejected;

4. Security analysis

The security of the proposed scheme is based on the hardness of factorization problem and the one-way hash function. Here, we first give the following theorem.

Theorem 1. *Let $n = p \cdot q$, where p and q are two distinct odd primes. If $R \equiv r^2 \bmod n$ and $c \equiv s \cdot r \bmod n$, then finding such a s in $\mathbb{Z}_n^*$ is equivalent to the factorization problem.*

Proof. From $c \equiv s \cdot r \bmod n$, we will have

$$c^2 \equiv (s \cdot r)^2 \equiv s^2 \cdot r^2 \equiv s^2 \cdot R \bmod n.$$

Since $\gcd(R, n)$, the greatest common divisor of R and n, must be 1, it will follow that

$$s^2 \equiv \frac{c^2}{R} \bmod n.$$

Therefore, as in the literature [12], finding such a s is equivalent to the factorization problem. □

From the Theorem 1, the random number r and the password PW_i can't be derived from the message C in the proposed scheme. At the same time, considering the one-way property of hash function, the proposed scheme can withstand the following three attacks.

- *Impersonation attack*
  Suppose a user U_i is an attacker, who owns (ID_i, PW_i) and wants to impersonate another user U_v. As he does not know the secret key p and q, he cannot directly compute the password PW_v from the identity ID_v. Thereupon, he may first select a random number k to forge a new password $PW_v = PW_i \cdot k (\bmod n)$, and use the password PW_v to compute the identity ID_v. However, since H is a one-way hash function, he can't obtain the identity ID_v from the equation $PW_v{}^2 \equiv H(ID_v)(\bmod n)$, here we have assumed $c_1 = c_2 = 0$.Therefore, the proposed scheme can withstand the impersonation attack.
- *Forgery attack*
  Suppose an attacker $\mathscr{A}$, who has ability to forge another valid message $C' = (ID_i, T', c, H_1(T', r))$ from $C = (ID_i, T, c, H_1(T, r))$. From the Theorem 1, he can't derive the random number r from c. Thus, he only can get it from $H_1(T, r)$, but which will contradict with the fact that H_1 is a one-way hash function.Then, the proposed scheme can also withstand the forgery attack.

Table 1
Comparison of Hwang–Li's scheme and proposed scheme

	Hwang–Li's Scheme		Our scheme	
	User	Server	User	Server
Registration	0	T_{exp}	0	$T_h + T_{sqr}$
Login	$T_h + T_{mul} + 3T_{exp}$	0	$T_h + T_{mul}$	0
Authentication	0	$T_h + T_{mul} + T_{inv} + 2T_{exp}$	0	$2T_h + T_{mul} + T_{inv} + T_{sqr}$

- *Replay attack*
  Because the remote server will check $(T' - T) \geqslant \Delta T$, where T' is the current date and time of the system and ΔT is the expected legal time interval caused by transmission delay, the replay attack also can be resisted. If a forgery or guess of T successfully passes the $(T' - T) \geqslant \Delta T$, the forger will still need to know the random value r, that can be computed only if PW_i is known. Since PW_i is private, the random value r is then unknown. Thus the $h \overset{?}{=} H_1(T, r)$ check fails, and the replay attack fails.

5. Performance comparison

Because the smart card is low-powered and resource-constrained device, when we implement our smart-based scheme, the efficiency is always an important issue. In this section, from the computation overhead view point, we will compare our scheme with Hwang–Li's scheme [6].

We denote T_{mul} the time of modular multiplication, T_{add} the time of modular addition, T_{sqr} the time of modular square root, T_{inv} the time of modular inversion, T_{exp} the time of modular exponentiation and T_h the time of hash evaluation. At the same time, in order to compare the efficiency of our scheme and Hwang–Li's easily, we assume that p in Hwang–Li's scheme and n in our scheme are of the same size, namely 1024 bits can guarantee both the discrete logarithm and factorization problems are hard. Then, we summarize the result in Table 1.

Because the smart card's efficiency is the most concerned in any smart card-based scheme, we thus only concentrate on the login phase's performance at the smart card side. From the Table 1, we will see the smart card's computational costs are very low in our scheme, only one hash function computation and one modular multiplication computation are required. While in Hwang–Li's scheme, additional three modular exponentiation computations are needed. Therefore, we can easily conclude that our proposed scheme is more efficient than Hwang–Li's scheme.

6. Conclusions

In this paper, based on the improved Rabin signature scheme, we have proposed a new remote user authentication scheme using smart card. By analyzing, our scheme is not only secure but also efficient. At the same time, like Hwang–Li's scheme, our scheme also doesn't need to maintain any verification tables in remote server. Therefore, we believe it will be a promising scheme in practical applications.

Acknowledgement

The authors would like to thank the anonymous reviewers for their valuable comments. This work was supported in part by the National Natural Science Foundation of China for Distinguished Young Scholars under Grant No. 60225007, the National Research Fund for the Doctoral Program of Higher Education of China under Grant No. 20020248024, and the Science and Technology Research Project of Shanghai under Grant Nos. 04JC14055 and 04DZ07067.

References

[1] L. Lamport, Password authentication with insecure communication, Comm. ACM 24 (1981) 770–772.

[2] R.E. Lennon, S.M. Matyas, C.H. Mayer, Cryptographic authentication of time-invariant quantities, IEEE Trans. Commun. COM-29 (6) (1981) 733–777.

[3] C.C. Chang, T.C. Wu, Remote password authentication with smart cards, IEE Proc.—E 138 (3) (1991) 165–168.

[4] S.M. Yen, K.H. Liao, Shared authentication token secure against replay and weak key attack, Inform. Process. Lett. (1997) 78–80.

[5] S.J. Wang, Remote table-based log-in authentication upon geometric triangle, Comp. Stand. Inter. 26 (2004) 85–92.

[6] M.S. Hwang, L.H. Li, A new remote user authentication scheme using smart card, IEEE Trans. Consum. Electr. 46 (1) (2000) 28–30.

[7] C.K. Chan, L.M. Cheng, Cryptanalysis of a remote user authentication scheme using smart cards, IEEE Trans. Consum. Electr. 46 (4) (2000) 992–993.

[8] C.C. Chang, K.F. Hwang, Some forgery attacks on a remote user authentication scheme using smart cards, Informatics 14 (3) (2003) 289–294.

[9] J.J. Shen, C.W. Lin, M.S. Hwang, A modified remote user authentication scheme using smart cards, IEEE Trans. Consum. Electr. 49 (2) (2003) 414–416.

[10] K.-C. Leung, L.M. Cheng, A.S. Fong, Chi-Kwong Chan, Cryptanalysis of a modified remote user authentication scheme using smart cards, IEEE Trans. Consum. Electr. 49 (4) (2003) 1243–1245.

[11] Z.F. Cao, A threshold key escrow scheme based on public key cryptosystem, Sci. China 44 (4) (2001) 441–448.

[12] M.O. Rabin, Digitalized signature and public key functions as intractable as factorization, Technical Report 212, MIT Laboratory for Computer Science, January 1979.

Rongxing Lu received his BS degree and MS in computer science from Tongji University in 2000 and 2003 respectively. Currently, he is a doctoral candidate in the Department of Computer and Engineering, Shanghai Jiao Tong University. His research interests in cryptography and network security.

Zhenfu Cao is a professor and the doctoral supervisor of Computer Software and Theory at the Department of Computer Science of Shanghai Jiao Tong University. His main research areas are number theory and modern cryptography, theory and technology of information security etc. He is the gainer of the first prize of award for science and technology in Chinese University and other term awards for Heilongjiang Province and Chinese Ministry of Aeronautics and Astronautics. In addition, he is also the gainer of Ying-Tung Fok Young Teacher Award (1989), the First Ten Outstanding Youth in Harbin (1996), best Ph.D thesis award in Harbin Institute of Technology (2001) and the National Outstanding Youth Fund in 2002.