Available at www.ElsevierComputerScience.com
POWERED BY SCIENCE DIRECT

Computer Standards & Interfaces xx (2004) xxx–xxx

COMPUTER STANDARDS & INTERFACES

www.elsevier.com/locate/csi

An efficient user identification scheme based on ID-based cryptosystem

Min-Shiang Hwang[a,*], Jung-Wen Lo[b], Shu-Chen Lin[c]

[a] Department of Management Information System, National Chung Hsing University, 250 Kuo Kuang Road, 402 Taichung 250, Taiwan, ROC
[b] Department of Information Management, National Taichung Institute of Technology, 129 Sec. 3, San-min Road, Taichung 404, Taiwan, ROC
[c] Department of Information Management, Chaoyang University of Technology, 168 Gifeng East Road, Wufeng, Taichung 413, Taiwan, ROC

Received 26 November 2003; received in revised form 15 March 2004; accepted 17 March 2004

Abstract

Tseng-Jan modified a non-interactive public key distribution system and also proposed several applications based on the Maurer–Yacobi scheme. In their scheme, a user can prove his identity to another user without revealing his secret key. They use a challenge-response-type interactive protocol to achieve their objective. However, in wireless environment, waiting for a corresponding response from the other is time-wasting and consumes the battery of the mobile device. The ability of computing and the capacity of the battery of a mobile device are limited. Therefore, we propose an efficient scheme based on ID-based cryptosystem that is more suitable to be applied in the mobile environment.

Keywords: Challenge-response protocol; Identity-based cryptosystem; User identification

1. Introduction

Shamir proposed a concept based on a public key cryptosystem in 1984 that can let each user's identification information be his public key [4]. Each user has the ability to verify the signature without exchanging his secret and public keys and without using the services of a third party. In other words, the user uses a unique identification information (e.g., name, address and e-mail address) as his public key, so that it is impossible for him to deny that the public key does not belong to him. Many identity-based public key systems have been proposed based on Shamir's idea [1,2,6]. In these schemes, the trusted authority center holds the secret number and decides whether the secret is locked by the receiver. In other words, the public user's ID is not his real identification information. To public user's secrets or not is decided by the trusted authority center.

In 1991, Maurer–Yacobi proposed an identity-based non-interactive public key distribution system based on a novel trapdoor one-way function of exponentiation modulo a composite number. They released the final version in 1996 [3]. Users are verified by their identity information without doing an interactive public key authentication. They adopted the squaring method and the Jacobi symbol method to ensure that each identity number corresponds to the identification information. In their scheme, there are no public keys,

* Corresponding author. Tel.: +886-422855401; fax: +886-422857173.
E-mail address: mshwang@nchu.edu.tw (M.-S. Hwang).

0920-5489/$ - see front matter © 2004 Published by Elsevier B.V.
doi:10.1016/j.csi.2004.03.006

certificates or other information. Each user applies his/her information as the public key.

Tseng–Jan improved the squaring method based on the Maurer–Yacobi scheme and also proposed a user identification scheme [5]. However, in the wireless environment, the capacity of the battery of a mobile device is limited. The time for waiting and responding must be reduced. Therefore, we propose an improved scheme that is suitable for the wireless environment.

The remainder of the article is organized as follows. In Section 2, we briefly review Tseng–Jan's user identification scheme. In Section 3, the improved scheme proposed by us is presented. In Section 4, we analyze the security of our improved scheme. In Section 5, we discuss the efficiency and the security of our scheme. Finally, we give a brief conclusion in Section 6.

2. Review of Tseng–Jan's scheme

Tseng–Jan proposed a user identification scheme using a challenge-response-type interactive protocol. A trusted authority in their scheme is used to generate system parameters as follows: N denotes the product of four primes p_j, whose decimal digits are between 60 and 70; the numbers $(p_j-1)/2$ are odd and pairwise relatively prime; e denotes an integer in $Z^*_{\phi(N)}$ and the secret d, which satisfies $ed\equiv 1(\text{mod } \phi(N))$; t denotes a random number from $Z^*_{\phi(N)}$, where ϕ is the Euler's totient function; g is a primitive element in GF(p_j); and $h(\cdot)$ is a one-way function.

When a user Alice joins the system, she presents her unique identity ID_a to the trusted authority. The trusted authority then computes $s_a=et\log_g(\text{ID}_a^2)$ mod $\phi(N)$ and sends s_a to Alice as her secret key in secret. The trusted authority publishes $\{N,g,e,h(\cdot)\}$ and keeps $\{p_1,p_2,p_3,p_4,t,v,d\}$ secret for all users. And the legal user, Alice, publishes $\{\text{ID}_a\}$ and keeps $\{s_a\}$ secretly.

The scheme can be shown as Fig. 1 when Alice wants to show her identity to the verifier Bob.

Step 1. Alice sends her identity, ID_a, to the verifier Bob.

Step 2. Bob chooses a random integer k in Z^*_N and sends Y to Alice by computing Y=(ID_b^2)k mod N.

Step 3. After receiving Y, Alice computes $Z=Y^{s_a}$ mod N and sends Z to Bob.

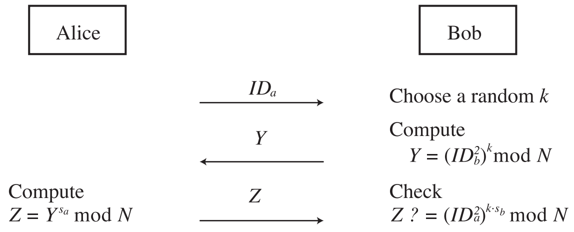

Fig. 1. Tseng–Jan's user identification scheme.

Step 4. In order to identify validity of Alice, Bob verifies the equation

$$Z?=(ID_a^2)^{ks_b}\text{mod } N. \tag{1}$$

If the equation holds, Bob will confirm that Alice's identity is valid.

In their scheme, Bob just uses Alice's identity ID_a as her public key to check the verification equation. From the above description of their scheme, Alice then sends out her identity ID_a and makes the correspondent response to Bob in Steps 1 and 3. However, the problem of using their scheme is that they waste too much time waiting for the responses. In next section, our improved scheme is shown in which there is only one pass verification.

3. The proposed scheme

Our scheme still inherits the advantage of Tseng–Jan's scheme that the user's identity is his/her public key. Furthermore, we only use one pass to show the validity of user's identity. The parameters $\{N,g,e,d,t,v,p_1,p_2,p_3,p_4\}$ are the same as those in Tseng–Jan's scheme. The notation is the bits connection. We add one notation T for the timestamp. Assuming the situation that the mobile device (M_1) wants to show his identity (ID_m) is legal to the base station (BS). The identity of BS is ID_b. We illustrate this scheme in Fig. 2.

Step 1. Mobile device (M) chooses a random integer k in Z^*_N and computes Y and Z as follows:

$$Y=(\text{ID}_m^2)^k\text{mod } N,$$

$$Z=(\text{ID}_b^2)^{ks_mT}\text{mod } N.$$

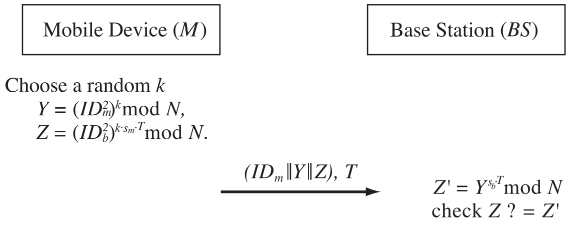

Fig. 2. The proposed scheme suitable for the wireless environment.

Then, he sends $\{(\mathrm{ID}_m \parallel Y \parallel Z),T\}$ to the base station (BS).

Step 2. After receiving the above messages from M, BS computes $Z' = Y^{s_b T} \mathrm{mod} N$.

Step 3. BS checks the equation $Z ? = Z'$. If the equation holds, BS will confirm that M's identity is validity.

In Tseng–Jan's scheme, three passes were needed to show the identity and the transmitted messages between two parties are $\{\mathrm{ID}_a,Y,Z\}$. All the transmitted messages in our scheme are the same as those in Tseng–Jan's system, expect the additional value, timestamp T. However, the proposed scheme needs only one pass to show the valid identity. We reduce the time used for responding and waiting so that the limited capacity of the battery of a mobile device will no longer be a problem. Thus, the proposed scheme is more efficient than Tseng–Jan's scheme.

4. Performance analysis

In this section, we present the performance of our proposed scheme. It is just as the analysis of the computational complexity of Tseng–Jan's scheme. Unfortunately, in their scheme, a great deal of running time is spent in waiting the responded value. Our scheme adds an extreme parameter to let the scheme be more efficient.

In their scheme, the user (Alice) proves her identity to the verifier (Bob), she has to spend much time waiting for obtaining Y from Bob in Step 2 because without getting Y, she cannot work. When the network congests, Alice may consume most of her device battery in waiting the responded value. She may also idle and exhaust the battery when she cannot get the responded value. However, our improved scheme can reduce the time for waiting. What the user (M) needs to do is only to send the message $\{(\mathrm{ID}_m \parallel Y \parallel Z),T\}$ to the verifier (BS). Therefore, our scheme can save the limited capacity of the battery of the mobile device.

Since the mobile device (M) wants to identify and his identity to transmit the message to the base station (BS) of our scheme, it requires 1 pass. In the phase of waiting responded value of our scheme, M need not spend any waiting time to require the value. The notation $|X|$ denotes the bit-string length of transmitted message. Total transmitted messages in this scheme require $|\mathrm{ID}|+|Y|+|Z|+|T|$. All of our transmitted messages are the same as those in Tseng–Jan's scheme except T which is much smaller. Moreover, our improved scheme takes less power by reducing the waiting time. Hence, our scheme is more suitable to be used in wireless environment.

5. Security analysis

Tseng–Jan's scheme is based on the Maurer–Yacobi scheme with an additional message. In the system setup phase, computing a discrete logarithm modulo prime N without knowing the prime factors of N is still infeasible. Our scheme is the same as Tseng–Jan's scheme on this point. Therefore, to compute the composite number N just means to face the difficult factoring problem.

In the following, some attacks are presented.

Attack 1: The intruder can obtain {Y,Z,T}, which are the transmitted messages between M and BS. However, computing M's secret key s_m from $Z=(ID_m2)^k\ sm^T$ mod N is a difficult factoring problem.

Attack 2: Let g be a generator in the range between 0 and N – 1, where N is a composite number. Let $y = g^x$ mod N. The Discrete Logarithm Problem is to find x from y. If the intruder wants to obtain the random number k from $Y=(ID_m2)k$ mod N, he will face the problem of solving the discrete logarithm problem. If he further chooses a random number k'to forge $\{ID_m \parallel Yint \parallel Zint\}$, he will fail in making Zint to pass the receiver's verification without correct s_m and k.

Attack 3: The intruder further adopts replay attack. He intercepts the message $\{(ID_m \| Y \| Z), T\}$ from network during the legal user ID_m sends it to the user ID_b. After a span time, he may pretend to be the user ID_m to re-send the message to the user ID_b. However, he will fail, because Z includes a timestamp T. To replace a new time stamp in Z also requires solving the difficult factoring problem.

6. Discussion

In this section, we discuss the efficiency and security of our scheme as follows.

6.1. Advantage of the parallel processing

In Tseng–Jan's scheme, there are three modular exponentiations in Steps 2, 3 and 4, respectively. We also need to execute three modular exponentiations to verify the user identification in Steps 1 and 2. However, when the device has two or more CPU, he can compute two equations in Step 1 in parallel, but Tseng–Jan's scheme cannot. Therefore, we can shorten the total computing time by using parallel processing technique.

6.2. Reduce the communication time and the cost

Tseng–Jan's scheme still needs three times of transmission. On the contrary, we only need handle it once. Both the user and verifier do not cost any time to wait for responding. Therefore, the communication time and transmission cost are decreased.

6.3. Ability of resisting the denial of service attack

Tseng–Jan's scheme cannot withstand the denial of service attack. Any malicious attacker can send a forged ID_i in Step 1 and any value Z_i in Step 3. The verifier ID_b should execute two modular exponentiations and one comparison to verify the identity. The ID_b could be weighed down with the heavy computing work and crashed. Nevertheless, in our scheme, the ID_b just needs to receive all the messages from the other user once. The verifier ID_b can verify the identity right away.

6.4. Economy of memory resource

In Tseng–Jan's scheme, the verifier must cost more storage memory to save random numbers and users' identities until after finishing the identification. Evidently, our scheme does not require any storage memory to do so.

7. Conclusions

We proposed an efficient scheme based on Tseng–Jan's scheme. Compared with their scheme, our reduce the time for responding and waiting. Also, our scheme uses the user's identity as his public key and does not need a key directory to store users' keys.

Our improved scheme costs less computing time and waiting time. Therefore, our scheme is more suitable to be employed in wireless network applications.

Acknowledgements

This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no. NSC91-2213-E-324-003.

References

[1] T. Hwang, J.L. Chen, Identity-based conference key broadcast system, IEE Proceedings. Computers and Digital Technology 141 (1) 1994, pp. 57–60.

[2] K. Koyama, K. Ohta, Security of improved identity-based conference key distribution systems, Advances in Cryptology, EUROCRYPT'88, 1988, pp. 11–19, Lecture Notes in Computer Science.

[3] U.M. Maurer, Y. Yacobi, A non-interactive public-key distribution system, Designs, Codes and Cryptography 9 (3) (1996) 305–316.

[4] A. Shamir, Identity based cryptosystems & signature schemes, Advances in Cryptology, CRYPTO'84, Lecture Notes-Computer Science, 1984, pp. 47–53.

[5] Y.M. Tseng, J.K. Jan, ID-based cryptographic schemes using a non-interactive public-key distribution system, Proceedings of the 14th Annual Computer Security Applications Conference (IEEE ACSAC98), Phoenix, Arizona, 1998 (Dec.), pp. 237–243.

[6] S. Tsujii, T. Itoh, An ID-based cryptosystem based on the discrete logarithm problem, Journal of Selected Areas in Communications 7 (4) (1989) 467–473.