Cryptanalysis of an efficient user identification scheme based on ID-based cryptosystem

Yalin Chen
Department of Information Management, National Sun Yat-Sen Unversity 804, Kaohsiung, Taiwan
m924020028@student.nsysu.edu.tw

Jue-Sam Chou
Department of Information Management, Nanhua University Chiayi, 622 Taiwan, R.O.C
jschou@mail.nhu.edu.tw

Chu-Hsing Lin
Department of Computer Science and Information Engineering,
Tunghai UniversityTaichung, 407 Taiwan, R.O.C
chlin@mail.thu.edu.tw

Abstract

In 2004, Hwang et al. proposed an efficient user identification scheme based on ID-based cryptosystem. This paper will show that Hwang et al.'s scheme is not secure by presenting an forgery attack on them.

1. Introduction

Since the idea of ID-Based cryptosystem was first introduced in 1984 by Shamir [1], there has been many studies focus on various kinds of this system [2, 3, 4, 5, 6, 7, 8, 14] such as ID-Based cryptosystem, ID-Based signature schemes and ID-Based key distribution systems. In these systems, the key generation is an opposite direction manner compared to the RSA-like public-key cryptosystem.

From 1991, Maurer and Yacobi [9, 10] proposed a non-interactive ID-Based public key distribution system. The final improved version was presented in 1996 [11]. In 1998, Tseng-Jan improved the scheme proposed by Maurer and Yacobi [11] and proposed a challenge-response-type interactive protocol [12] which a user can prove his identity to another without revealing his secret key, but their scheme uses a three passes protocol which is not suitable for application in a wireless environment. Therefore, Hwang et al. [13] improved Tseng-Jan's scheme to be more suitable to be applied in the mobile environment. However, in this paper, we point out that in Hwang et al.'s scheme, any malicious user can impersonate a legal user to communicate with the base station. Therefore, their scheme can not provide the authenticity as claimed.

The rest of this paper is organized as follows. In Section 2, we will briefly review Hwang et al.'s scheme. Section 3 shows the attack on their scheme. Finally, a conclusion is given in Section 4.

2. Review of Hwang et al.'s scheme

Basically, Hwang et al.'s scheme inherits the advantage of Tseng–Jan's scheme that the user's identity is his public key. The parameter set used, $\{N, g, e, d, t, v, p_1, p_2, p_3, p_4\}$, is the same as those in Tseng–Jan's scheme. In Tseng–Jan's scheme, a trusted authority (TA) exists to generate system parameters as follows: N denotes the product of four primes p_j, j=1 to 4, 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 $Z_{\varphi(N)}^*$ and the secret d, which satisfies $ed \equiv 1 (mod\ \varphi(N))$; t denotes a random number from $Z_{\varphi(N)}^*$, where $\varphi(N)$ denotes the Euler's totient function; g is a primitive element in $GF(p_j)$; and $h(\cdot)$ is a one-way hash function. When a user Alice wants to join the system, she registers her identity ID_a to the TA. TA computes $s_a = etlog_g(ID_a^2) \bmod \varphi(N)$ and sends s_a to Alice as her secret key via a secure channel. Then, Alice publishes $\{ID_a\}$ as her public key. Besides, they add the timestamp T to their scheme. We present their scheme as in figure 1 and describe the proposed protocol step by step as follows.

Assuming that the mobile device (M) having secret key s_m wants to prove his identity ID_m to the base station (BS) whose identity is ID_b and with secret key s_b. The one pass protocol performs the following steps.

Step 1. Mobile device (M) chooses a random number k in Z_N^*, generate a timestamp T, and computes Y and Z as follows:
$Y=(ID_m^2)^k \bmod N$,
$Z=(ID_b^2)^{ksm \cdot T} \bmod N$.

Where notation "·" means T is connected with the former in bit form. Then, M sends the message $L=\{(ID \| Y \| Z), T\}$ to the base station (BS).

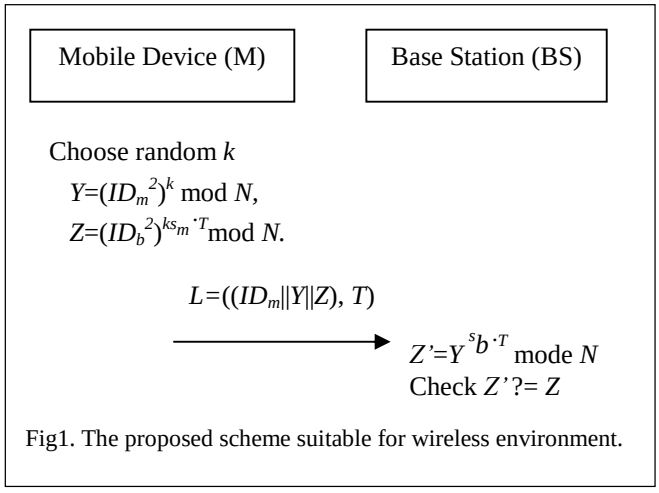

Fig1. The proposed scheme suitable for wireless environment.

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

Step 3. BS checks whether the equation $Z = Z'$ holds. If the equation holds, BS will assure that M's identity is valid.

We can see that all the transmitted messages in the above mentioned are the same as those in Tseng–Jan's scheme, expect the additional value, timestamp T. The improvement is that it uses only one pass to show the user's valid identity. Thus, they can reduce the time needed for responding and waiting for a mobile device in a wireless environment. For this reason, the proposed scheme is more efficient than Tseng–Jan's scheme, as claimed by the authors. Yet, after our cryptanalysis, we find that it still suffers from the forgery attack. We state our analysis in the following section.

3. Forgery attack on Hwang et al's scheme

After analyzing the bit connection operator, "•", in Hwang et al.'s protocol, we find it must possess the commutative property as the multiplication operator does. Otherwise, according to their definition, the verifying equation Z'=Z which equals to $((ID_m^2)^k)^{s_b \cdot T)} = (ID_b^2)^{(ks_m \cdot T)}$ would not hold. For example, $4^3=2^6$ but $4^{3 \cdot 101} \neq 2^{6 \cdot 101}$. That is, $4^{011101} \neq 2^{110101}$. Now, suppose a malicious user (*user h*) wants to impersonate as a legal user (*user m*) following the Hwang's protocol. From the analysis mentioned, we can easily show how he can succeed in the forgery attack as follows.

Step 1. User H intercepts the transmitted message $L=\{(ID_m \parallel Y \parallel Z), T\}$ and creates another timestamp T'..

Step 2. User H replaces the intercepted message components Y with Y' and Z with Z', where $Y'=(Y^{s_h \cdot T}) \ mod\ N$ and $Z'=(Z^{s_h \cdot T'}) \ mod\ N$. He can then replace the ID_m with his own ID, ID_h.

Step 3. User H sends this forged message $L'=\{(ID_h \parallel Y' \parallel Z'), T'\}$, to the base station.

Step 4. After receiving message L' from H, BS computes $Z'' = (Y')^{s_b \cdot T'} mod\ N$.

Step 5. BS checks whether the equation $Z' = Z''$ holds. If the equation holds, BS will assure that H's identity is valid.

We can obviously see, after doing the above five steps according to the protocol proposed by Hwang et al., the malicious user can easily impersonate as a legal user successfully without being detected by the base station. Since the verification equation $Z^{s_h \cdot T'} = (Y')^{s_b \cdot T'} mod\ N$ holds. Hence, the malicious user doesn't care about the value of T, he can always succeed when he launches the forgery attack.

4. Conclusion

In this paper, we show Hwang et al.'s scheme is vulnerable to the forgery attack. Indeed, we doubt the robustness of security for a scheme using just one-pass protocol in this kind of ID-based cryptosystem.

References

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

[2] Tanaka H, A realization scheme for the identity-based cryptosystem. Proc Crypto'87 1987; 340–9.

[3] Tsai YW, Hwang T, ID-based public key cryptosystems based on Okamoto and Tanaka's ID-based one way communication scheme. Electron Lett 1990;26(10):666–8.

[4] Tsujii S, Itoh T, Kurosawa K, ID-based cryptosystem using discrete logarithm problem. Electron Lett 1987;23:1318–20.

[5] Abe M, Okamoto T, Delegation chains secure up to constant length. IEICE Trans Fundam 2002;E85-A(1):110–6.

[6] Gunther CG, An identity-based key exchange protocol, Cryptology-Eurocrypt'89. New York: Springer; 1989.p. 29–37.

[7] Matsumoto T, lmai H, On the key predistribution system, Cryptology-Eurocrpt'89. New York: Springer; 1989.p. 29–37.

[8] Okamoto E, Tanaka K, Identity-based information security management for personal computer networks, IEEE J Sel Areas Commun 1989;7(2):290–4

[9] Maurer UM, Yacobi Y, Non-interactive public key cryptography, Cryptology-Eurocrypt'91. New York:

Springer; 1991. p. 498–507.

[10] Maurer UM, Yacobi Y, A remark on a noninteractive public-key distribution system, Proc Eurocrpt'92 1993; 458–60.

[11] Maurer UM, Yacobi Y, A non-interactive public-key distribution system, Des Codes Cryptogr 1996;9(3):305–16.

[12] 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.

[13] M.S. Hwang, J.W. Lo, S.C. Lin, An efficient user identification scheme based on ID-based cryptosystem, Computer Standards & Interfaces 26 (2004) 565–569.

[14] W.B. Lee, K.C. Liao, Constructing identity-based cryptosystems for discrete logarithm based cryptosystems, Journal of Network and Computer Applications 27 (2004) 191–199.