LETTER

Cryptanalysis of an Efficient User Identification Scheme Based on ID-Based Cryptosystem*

Chao-Liang LIU[†a)], **Gwoboa HORNG**[†], ***and*** **Hsin-Yu LIU**[†], ***Nonmembers***

SUMMARY In 1998, Tseng and Jan proposed a lightweight interactive user identification protocol based on ID-based cryptography. Recently, Hwang et al. modified their protocol to reduce the responding and waiting time for wireless network applications. In this letter, we show that their scheme is vulnerable to impersonation attacks.

key words: *cryptanalysis, user identification, ID-based cryptosystem, wireless network*

1. Introduction

In 1984, Shamir [6] introduced a new concept, namely ID-based cryptography, which relates user's public key to its ID such as user's name, e-mail address or social security number. Based on this concept, many researchers have devoted themselves to developing various ID-based schemes. The major advantage of these schemes is that there is no requirement for a trusted third party to authenticate user's public key.

In 1991, Maurer and Yacobi [3] proposed a new ID-based public-key distribution system which is a non-interactive protocol. It is based on a novel trapdoor one-way function. However, a flaw of the scheme was found and modification was proposed in literature [2], [4]. The final version was presented in 1996 [5].

In 1998, Tseng-Jan proposed a user identification scheme [7], which improved the squaring method in Maurer-Yacobi scheme. However Hwang et al. [1] argue that in the wireless environment, since the capacity of the battery of a mobile device is limited the waiting and responding time must be reduced. And a one-pass improvement suitable for wireless environment is proposed.

In this letter, we show that Hwang et al.'s scheme is vulnerable to impersonation attacks. More precisely, if an adversary intercepts previous identification messages from a user, then he can forge another identification message to impersonate that user. Therefore, dispute between the service providers and the users is unavoidable if the scheme is adopted in a system with service changes or used for retrieving confidential information.

Manuscript received October 12, 2004.

Manuscript revised January 12, 2005.

[†]The authors are with the Department of Computer Science, National Chung-Hsing University, 250 Kuo-Kuang Road, Taichung 40227, Taiwan, R.O.C.

*This research was partially supported by the National Science Council, Taiwan, R.O.C. (NSC93-2213-E-005-021)

a) E-mail: s9056001@cs.nchu.edu.tw

DOI: 10.1093/ietcom/e88–b.5.2171

2. Review of Hwang et al.'s Scheme

In Hwang et al.'s scheme, a trusted authority is used to generate system parameters. There are four primes (p_1, p_2, p_3, p_4) between 60 and 70 decimal and for $1 \le i \le 4$, $(p_i - 1)/2$ are odd and pair-wise relatively prime. Moreover, the length of these primes are small enough such that computing the discrete logarithm problem is feasible, but factoring the product $N = p_1 \cdot p_2 \cdot p_3 \cdot p_4$ is infeasible. Other parameters selected by the trusted authority are as follows.

1. ϕ: Euler's totient function.
2. e, d, t and v: integers in $Z^*_{\phi(N)}$ such that, $ed \equiv 1 \mod \phi(N)$, $tv \equiv 1 \mod \phi(N)$.
3. g: primitive element in each $GF(p_i)$.
4. $h(\cdot)$: one-way hash function.
5. ID_m, ID_b: identities of mobile device and base station, respectively.
6. s_m: secret key of mobile device, where $s_m = et \log_g(ID_m^2) \mod \phi(N)$.
7. s_b: secret key of base station, where $s_b = et \log_g(ID_b^2) \mod \phi(N)$.
8. T: timestamp.

When a mobile device (M with identity ID_m) needs to show the authorization, to a base station (BS with identity ID_b), M should do the following steps.

Step 1 Choose a random number k from Z^*_N, and compute
$Y = (ID_m^2)^k \mod N$,
$Z = (ID_b^2)^{k s_m T} \mod N$, where T is the current timestamp.

Step 2 Send $\{(ID_m||Y||Z), T\}$ to BS.

After receiving $\{(ID_m||Y||Z), T\}$ from M, BS computes $Z' = Y^{s_b T}$, checks $Z \stackrel{?}{=} Z'$. If it holds, BS confirms that M is valid.

Hwang et al.'s scheme is more efficient than Tseng-Jan's scheme since it simultaneously processes the parameters Y and Z. However, the correlation between these two parameters disappears. Therefore, it opens the door for adversaries to generate a valid login message with the current timestamp. In the following section, we show how to successfully launch such an impersonation attack.

3. Impersonation Attack on Hwang et al.'s Scheme

If an adversary (A) intercepts message $\{(ID_m||Y||Z), T\}$ from any mobile device M, then he can forge another message

$\{(ID_m||Y'||Z'), T'\}$ to pass the identification, by the following steps.

Step 1 A computes:
$Y' = Y^T = (ID_m^2)^{kT} \mod N$
$Z' = Z^{T'} = (ID_b^2)^{ks_mTT'} \mod N$
where T' is the current timestamp.

Step 2 A Sends $\{(ID_m||Y'||Z'), T'\}$ to the base station (BS).

We show that BS will accept $\{(ID_m||Y'||Z'), T'\}$ as valid since

$$Z'' = Y'^{s_bT'} = (ID_m^2)^{kTs_bT'} = (ID_b^2)^{ks_mTT'} = Z' \mod N.$$

Moreover, the attacker can simply take a random number α, compute $Y' = Y^{\alpha T} \mod N$ and $Z' = Z^{\alpha T'} \mod N$, then $\{(ID_m||Y'||Z'), T'\}$ will be still valid.

It seems to us that there is no simple way to fix this weakness without modifying all equations. In this situation, it is necessary to make tradeoff between performance and security.

References

[1] M.S. Hwang, J.W. Lo, and S.-C. Lin, "An efficient user identification scheme based on ID-based cryptosystem," Computer Standards & Interfaces, vol.26, pp.565–569, 2004.
[2] C.H. Lim and P.J. Lee, "Modified Maurer-Yacobi's scheme and its application," Proc. Auscrypt'92, pp.308–323, 1992.
[3] U.M. Maurer and Y. Yacobi, "Non-interactive public-key cryptography," Proc. EUROCRYPT'91, pp.498–507, 1992.
[4] U.M. Maurer and Y. Yacobi, "A remark on a non-interactive public-key distribution system," Proc. EUROCRYPT'92, pp.458–460, 1993.
[5] U.M. Maurer and Y. Yacobi, "A non-interactive public-key distribution system," Designs, Codes and Cryptography, vol.9, no.3, pp.305–316, 1996.
[6] A. Shamir, "Identity based cryptosystems & signature schemes," Advances in Cryptology, CRYPTO'84, Lecture Notes in Computer Science, pp.47–53, 1984.
[7] Y.M. Tseng and J.K. Jan, "ID-based cryptographic schemes using a non-interactive public-key distribution system," Proc. 14th Annual Computer Security Applications Conference (IEEE ACSAC98), pp.237–243, Phoenix, Arizona, Dec. 1998.