Cryptanalysis of two identification schemes based on an ID-based cryptosystem

Qiang Tang and Chris J. Mitchell

Information Security Group

Royal Holloway, University of London

Egham, Surrey TW20 0EX, UK

{qiang.tang, c.mitchell}@rhul.ac.uk

8th April 2005

Abstract

Two identification schemes based on the Maurer-Yacobi ID-based cryptosystem are analysed and shown to suffer from serious security problems.

1 Introduction

Tseng and Jan [1] proposed a user identification scheme (referred to as the TJ scheme) based on an identity-based (ID-based) non-interactive public

key distribution system due to Maurer and Yacobi [2]. Hwang, Lo and Lin [3] have proposed a further scheme, based on the TJ scheme, designed for use in the mobile environment (we refer to this as the HLL scheme). The authors of both schemes [1, 3] claim that they are secure. However, we show that both schemes suffer from serious security problems.

The reminder of this paper is organised as follows. In Section 2, we review the TJ and HLL schemes. In Section 3, we describe the security problems. In Section 4, brief conclusions are provided.

2 Review of the TJ and HLL schemes

Both schemes possess the same system initialisation phase. A trusted authority (TA) is required to perform the following initialisation steps.

- Select prime numbers p_j $(1 \leq j \leq 4)$ each 60–70 decimal digits long, where the values $\frac{p_j-1}{2}$ are odd and pairwise relatively prime. Put $N = p_1p_2p_3p_4$.
- Select a random number $e \in Z^*_{\phi(N)}$, and compute d satisfying $ed \equiv 1 \pmod{\phi(N)}$. Select another random number t in $Z^*_{\phi(N)}$.
- Select a value g such that g is a primitive element in $GF(p_j)$ for every j, $1 \leq j \leq 4$, and a one-way function h.

TA publishes $\{N, g, e, h\}$ and keeps $\{p_1, p_2, p_3, p_4, t, d\}$ secret. When a user wishes to join the system, he presents his unique identifier ID to the TA. The TA then computes

$$s = et \log_g(\mathrm{ID}^2) \bmod \phi(N)$$

and sends s to the user as his private key and publishes ID as his public key. Note that here, as throughout, $\log_g x$ (the discrete logarithm of x to the base g) means the smallest non-negative integer y such that $g^y \equiv x \pmod{N}$.

Note that the existence of the discrete logarithm necessary to compute s was established by Maurer and Yacobi [2]; computing this discrete logarithm is feasible by computing the base g logarithm of ID^2 modulo $p_j - 1$ for each j, and then combining the values (again as described in [2]).

2.1 Identification phase of the TJ scheme

Suppose Alice (with identity ID_a) wishes to identify herself to Bob (with identity ID_b). She follows the steps below.

1. Alice sends her identity ID_a to Bob.
2. Bob chooses a random integer k in Z_N^* and sends $Y = (\mathrm{ID}_b)^{2k} \bmod N$ to Alice.
3. On receiving Y, Alice computes and sends $Z = Y^{s_a} \bmod N$ to Bob.

4. Bob checks the equation $Z = (\mathrm{ID}_a)^{2ks_b} \bmod N$. If the check succeeds, then Bob has confirmed that Alice possesses the identity ID_a.

2.2 Identification phase of the HLL scheme

Suppose a mobile user (with identity ID_m) wishes to identify himself to the base station (with identity ID_b). The following steps are performed.

1. The mobile user chooses a random k in Z_N^* and sends $\{\mathrm{ID}_m, Y, Z, T\}$ to the base station, where T is a time-stamp and Y and Z are computed as follows:

$$Y = (\mathrm{ID}_m)^{2k} \bmod N$$

$$Z = (\mathrm{ID}_b)^{2ks_mT} \bmod N$$

2. On receiving $\{\mathrm{ID}_m, Y, Z, T\}$, the base station computes $Z' = Y^{s_bT} \bmod N$. If $Z' = Z$, then the base station has confirmed that the mobile user possesses the identity ID_m.

3 Cryptanalysis of the TJ and HLL schemes

The following security problems exist in the TJ and HLL schemes.

1. In the TJ scheme, an impersonation attack can be mounted because of the fact that Alice replies to the challenge Y, which should be from Bob, without authenticating its origin.

Suppose an attacker can freely manipulate the messages sent between Alice and Bob in the TJ scheme; then he can also impersonate Alice to any valid user except Alice. To impersonate Alice to Eve, the attack can be mounted as follows.

(a) When Alice sends her identity ID_a to Bob, the attacker also sends ID_a to Eve.

(b) The attacker then intercepts the reply message sent from Bob to Alice, and prevents it reaching Alice.

(c) After receiving ID_a from the attacker (masquerading as Alice), Eve chooses a random integer k in Z_N^* and sends $Y = (\mathrm{ID}_e)^{2k} \bmod N$ to the attacker. After receiving Y, the attacker impersonates Bob to forward it to Alice.

(d) On receiving Y, Alice computes and sends $Z = Y^{s_a} \bmod N$ to Bob. The attacker intercepts this message and sends it to Eve.

(e) Eve checks whether the equation $Z = (\mathrm{ID}_a)^{2ks_e} \bmod N$ holds, which it will. Eve now believes that the attacker possesses the identity ID_a. That is, Eve believes she is talking to Alice, whereas Alice believes she is talking to Bob.

To mount this attack, the attacker only needs to monitor the activities of Alice. It can be mounted whenever Alice initiates a new run of the identification protocol.

2. In the HLL scheme a time-stamp T is used to prevent replay attacks; however an attacker can still deploy a replay attack because of the way in which the time-stamp T is used.

   Suppose the attacker has intercepted $\{\mathrm{ID}_m, Y, Z, T\}$ in a previous run of the identification scheme. Then the attacker can initiate a new run of the identification protocol as follows.

   (a) The attacker constructs and sends $\{\mathrm{ID}_m, Y^*, Z^*, T^*\}$ to the base station, where T^* is the current time-stamp, $Y^* = Y^T \bmod N$, and $Z^* = Z^{T^*} \bmod N$.

   (b) On receiving $\{\mathrm{ID}_m, Y^*, Z^*, T^*\}$, the base station computes $Z^{'} = (Y^*)^{s_b T^*} \bmod N$. Because $Z \equiv Y^{s_b T} \pmod N$ in the previous run of the identification protocol, it is easy to verify that $Z^{'} = Z^*$ will hold. The base station now believes that the attacker possesses the identity ID_m.

3. In the HLL scheme, the identity of the mobile user is not involved in the verification by the base station, so that an attacker can impersonate any mobile user except Alice to the base station when Alice tries to identify herself to the base station.

   To mount this attack, the attacker only needs to replace $\{\mathrm{ID}_m, Y, Z, T\}$ with $\{\mathrm{ID}_x, Y, Z, T\}$ in step 1 of the protocol run, where ID_x is the identity of the mobile user that the attacker wishes to impersonate.

The validity of the attack is obvious.

4 Conclusion

We have shown that serious security problems exist in two identification schemes based on an ID-based cryptosystem.

5 Acknowledgements

The authors would like to express deep appreciation to the anonymous reviewers for their valuable comments.

References

[1] Y. M. Tseng and J. K. Jan. ID-based cryptographic schemes using a non-interactive public-key distribution system. In *ACSAC '98: Proceedings of the 14th Annual Computer Security Applications Conference*, pages 237–243. IEEE Computer Society, 1998.

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

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