# On the security of a group key agreement protocol

Qiang Tang
Département d'Informatique, École Normale Supérieure
45 Rue d'Ulm, 75230 Paris Cedex 05, France
tang@di.ens.fr

December 12, 2006

**Abstract**

In this paper we show that the group key agreement protocol proposed by Tseng suffers from a number of serious security vulnerabilities.

## 1 Introduction

Tseng [5] proposes a group key agreement protocol for use in a wireless network consisting of a number of low-power mobile nodes with limited computational and communicational resources, and a powerful wireless gateway with much greater resources. In such a wireless network, each low-power node can send messages to the powerful node via unicast communication, and the powerful node can broadcast or unicast messages to each low-power node. The scheme is claimed to be a contributory group key agreement protocol, that provides forward secrecy as well as implicit key authentication. It is also claimed to be provably secure against passive attackers and secure against impersonation attacks.

However, we show that the proposed protocol possesses a number of security vulnerabilities, of which probably the most serious is that an active attacker can obtain the session key of all low-power nodes.

The rest of this paper is organised as follows. In Section 2 we describe the protocol proposed by Tseng. In Section 3 we present our comments on the protocol. In Section 4 we conclude this paper.

## 2 Description of the protocol of Tseng

Let $U_i$ $(i \geq 1)$ denote the low-power mobile nodes, and $S$ denote the powerful node. Let $\mathbb{G}$ be a cyclic group of prime order $p$, and let $g$ be a generator of $\mathbb{G}$. $U_i$ possesses a key pair $(PK_i, SK_i)$ for a signature scheme such as ElGamal [3], where $SK_i$ is randomly chosen from $\mathbb{Z}_p$ and $PK_i = g^{SK_i}$. The powerful node $S$ possesses a similar key pair $(PK_S, SK_S)$ where $PK_S$ is known by all the low-power nodes. In addition $\mathsf{H}$ is a hash function.

Before every protocol execution, $U_i$ is required to store $x_i, x_i^{-1}, \alpha_i, y_i, \sigma_i$ in its memory, where $x_i$ is randomly chosen $(0 < x_i < p)$, $\alpha_i = (PK_S)^{x_i}$, $y_i = g^{x_i}$, and $\sigma_i$ is $U_i$'s signature on $y_i$. If $U_i$ $(1 \leq i \leq n)$ and $S$ wish to negotiate a key, then they perform in the following protocol:

1. $U_i$ sends $y_i, \sigma_i$ to $S$.
2. After receiving the values from each of $U_1, U_2, \cdots, U_n$, $S$ checks whether or not $\sigma_i$ is the signature for $y_i$, for all $1 \leq i \leq n$. If all the checks succeed, $S$ broadcasts $C$, $\alpha'_i$ $(1 \leq i \leq n)$, and $z_i$ $(1 \leq i \leq n)$, where $x$ is randomly chosen from $\mathbb{Z}_p$,
$$X = g^x, z_i = y_i^x,\ \alpha'_i = (y_i)^{SK_S},\ C = \mathsf{H}(X \oplus z_1 \oplus z_2 \cdots \oplus z_n).$$
3. $U_i$ checks whether or not $\alpha'_i = \alpha_i$ and $C = \mathsf{H}(X' \oplus z_1 \oplus z_2 \cdots \oplus z_n)$, where $X' = (z_i)^{x_i^{-1}}$. $U_i$ also checks whether or not $z_i \neq 1$ for all $1 \leq i \leq n$. If all the checks succeed, $U_i$ computes the session key as $K = X' \prod_i^n z_i$.

Tseng [5] claims that the proposed protocol is a provably secure group key agreement protocol, which is secure against passive attackers and provides mutual authentication between the powerful node and low-power nodes. In Section 4.1 of [5], a passive attacker is defined to be an attacker that can only eavesdrop upon messages transmitted over the broadcast channel. Tseng also claims that the protocol achieves implicit key authentication and forward secrecy.

## 3 Our comments

The security analysis in [5] is performed heuristically, without referring to any security model, such as the Bellare-Rogaway model [1]. Therefore, it is not surprising that the protocol does not achieve the claimed properties. Next, we show that the protocol suffers from a number of potential security vulnerabilities.

- The protocol does not achieve key authentication in the presence of an active attacker which is capable of manipulating the messages sent among all the nodes. To mount an attack against $U_i$, an active attacker simply needs to replace the original broadcast message, sent from $S$ to $U_i$, with $(C^*; \alpha'_i(1 \le i \le n); z^*_i(1 \le i \le n))$, where $z^*_i = y^r_1$ and $r$ is randomly chosen from $\mathbb{Z}_q$, $z^*_j = z'_j$ for $j \neq i$, and $C^*$ is computed as

  $$C^* = \mathsf{H}(g^r \oplus z^*_1 \oplus z^*_2 \cdots \oplus z^*_n).$$

  It is clear that $U_i$ will succeed in computing the session key $K = g^r \prod_{i=1}^n z^*_i$. The attack is depicted in the Figure 1.

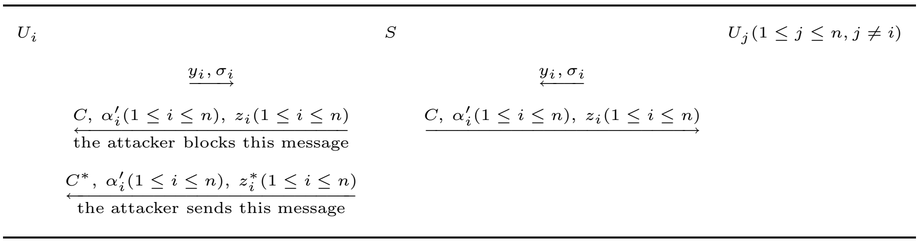
$U_i$
$S$
$U_j(1 \le j \le n, j \neq i)$
$y_i, \sigma_i$
$y_i, \sigma_i$
$C,\ \alpha'_i(1 \le i \le n),\ z_i(1 \le i \le n)$
the attacker blocks this message
$C,\ \alpha'_i(1 \le i \le n),\ z_i(1 \le i \le n)$
$C^*,\ \alpha'_i(1 \le i \le n),\ z^*_i(1 \le i \le n)$
the attacker sends this message

Figure 1: The attack

- Following the above attack, the argument that the proposed protocol achieves mutual authentication between the powerful node and low-power nodes is incorrect in the sense of lacking matching conversations as described in [1]. Alternatively speaking, the low-power nodes cannot be sure that the messages they receive are actually from the powerful node $S$.

- In the protocol, the powerful node $S$ can force other nodes to compute any session key it chooses. To make $U_i$ compute a key $K^*$, $S$ sends $C$, $\alpha'_i$ $(1 \le i \le n)$, and $z_i$ $(1 \le i \le n)$ to $U_i$, where $z_{i+1} = \frac{K^*}{X' \prod_{j=1, j \neq i+1}^n z_j}$.

Besides these serious security vulnerabilities, we have the following additional comments:

- During the protocol, $U_i$ knows nothing about who else is involved in the protocol execution. We regard this as an undesirable property for a key agreement protocol, especially in the case when the protocol might be run concurrently.

- The protocol is not semantically secure in most security models for key agreement protocols, such as those given in [1, 2]. Note that the session key is computed as $K = X' \prod_{i=1}^{n} z_i$, therefore, given $K'$, it is straightforward to check whether or not $K' = K$ by testing
$$C \overset{?}{=} \mathsf{H}((K'(\prod_{i=1}^{n} z_i)^{-1}) \oplus z_1 \oplus z_2 \cdots \oplus z_n).$$
Lack of semantic security implies that an attacker can always successfully distinguish between the session key and a random string from the key agreement protocol execution, regardless of how the session key is used in the following communication. It is a similar situation to a public key encryption scheme, where semantic security is more important than one-wayness. Although it is debatable whether or not the semantic security requirement makes sense in the design of key agreement protocols, nevertheless, it is good practice to generate the ultimate session key using a key derivation function [4]. In fact, the key control vulnerability, mentioned above, is partially caused by the way that $K$ is computed.

- In [5] Tseng briefly mentions that the signature from every low-power node can contain a time-stamp in order to prevent replay attack, although no description appears in the protocol specification. In the group setting, especially for a mobile network, it is not easy to synchronise the clocks of all involved parties. Potentially, a Denial of Service (DoS) might be mounted against the powerful node by replaying the messages from low-power nodes. The situation would get much worse if the group size become very large.

As far as efficiency is concerned, $S$ need not send $\alpha'_j$ $(1 \leq j \leq n, j \neq i)$ to $U_i$ in order to save bandwidth, because these values are not used by $U_i$.

# 4 Conclusion

We have shown that the group key agreement protocol proposed by Tseng suffers from a number of security vulnerabilities.

# Acknowledgment

The author thanks Chris J. Mitchell for bringing Tseng's paper to his attention and providing many helpful comments.

# References

[1] M. Bellare and P. Rogaway. Entity authentication and key distribution. In D. R. Stinson, editor, *Advances in Cryptology – Crypto '93*, volume 773 of *Lecture Notes in Computer Science*, pages 110–125. Springer-Verlag, 1993.

[2] E. Bresson, O. Chevassut, D. Pointcheval, and J.-J. Quisquater. Provably authenticated group Diffie-Hellman key exchange. In *Proceedings of the 8th ACM Conference on Computer and Communications Security*, pages 255–264. ACM Press, 2001.

[3] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In G. R. Blakley and D. Chaum, editors, *Advances in Cryptology, Proceedings of CRYPTO '84*, volume 196 of *Lecture Notes in Computer Science*, pages 10–18. Springer, 1985.

[4] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography.* CRC Press, 1997.

[5] Y. Tseng. A secure authenticated group key agreement protocol for resource-limited mobile devices. *Comput. J.*, 50(1):41–52, 2007.