Authenticated Group Key Agreement for Multicast

Liming Wang[1,2] and Chuan-Kun Wu[1]

[1] State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing 100080, P.R. China
[2] Graduate School of Chinese Academy of Sciences, Beijing 100039, P.R. China
{limingwang, ckwu}@is.iscas.ac.cn

Abstract. Secure multicast communication provides an efficient way to deliver data to a large group of recipients. Scalability, efficiency and authenticity are the key challenges for secure multicast. In this paper, we propose a novel group key agreement scheme called logical identity hierarchy(LIH) for multicast to support secure communications for large and dynamic groups, which is based on bilinear pairing. Compared with the previous tree-based schemes, LIH provides dual authentication between group controller(GC) and group members and hierarchical authentication among group members. GC and all the users do not need to execute any encryption/decryption process during the rekeying operation. Moreover, in LIH, the group members can be stateless receivers, who do not need to update their state during the protocol execution. Using a public board, GC does not need to multicast any rekeying message when a user joins/leaves the communication group. Security analysis shows that LIH satisfies both backward secrecy and forward secrecy.

1 Introduction

Many web and multimedia applications such as audio and video conference, pay-TV systems, secure distribution of copyright-protected material, require a secure and reliable group communication. Multicast is the core component of the group communications, which greatly reduces the server's communication overhead and network bandwidth usage by sending one multicast message instead of n messages to n destinations.

However, IP multicast [1,2,3] by itself does not provide any security services. Anyone can join a multicast group to receive data or to send data to the group. Therefore, security is crucial for the multicast communications. Basic security services needed in multicast communication are largely the same as in the unicast communications: data secrecy, integrity and entity authentication. But often the cryptography mechanisms used in the unicast environment may not be directly deployed into multicast environment. In the most basic form, the first step towards securing traffic within a multicast group is to provide a cryptographic key that is shared by the group members [4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17]. Having such a key allows group members to decode the messages, while the entities outside the group cannot decode them. The group key is updated on every

D. Pointcheval, Y. Mu, and K. Chen (Eds.): CANS 2006, LNCS 4301, pp. 55–72, 2006.

membership change for forward and backward secrecy. Because the group rekeying is very consumptive and frequently performed due to the dynamic nature of multicast communication, the way to update it in a scalable and secure fashion is required.

1.1 Related Work

The logical key hierarchy(LKH) method was proposed by Wallner et al. [11] and Wong et al. [12] independently. In this approach, the group controller(GC) maintains a logical key tree where each node represents a key encryption key(KEK). The root of the key tree is the group key used for encrypting data in group communications and it is shared by all users. The leaf node of the key tree is associated with a user in the communication group. Each user secretly maintains the keys related to the nodes in the path from its leaf node to the root. As a result, in an addition or eviction of a user, the rekeying communication cost is equivalent to $2\log_2 n - 1$ keys. In a balanced binary tree, each user stores $\log_2 n + 1$ keys, where n is the number of users. The joining operation in LKH can be improved to run in constant time as suggested by Waldvoggel et al. [18]. The new group key can be computed by applying a one-way function to the keys affected by the membership change. Hence, each member that already knew the old key can compute the new one.

Another optimization of the logical key hierarchy approach is one-way function tree(OFT) proposed by McGrew and Sherman [13,19]. Their scheme reduces the size of rekeying messages from $2\log_2 n$ to $\log_2 n$. Canetti et al. [5] proposed a slightly different method that achieves the same communication overhead using a pseudo-random generator tree. This algorithm is known as the one-way function chain tree(OFCT) and it is applied only on users removal.

Kim et al. proposed a tree-based key agreement protocol(TGDH) [14, 16]. TGDH is a contributive tree key management protocol which is a combination of key tree and Diffie-Hellman key exchange to generate and maintain the group key. It is similar to OFT but each member can act as a sponsor according to its position in the tree. The sponsor is responsible for the communication and the broadcasting of intermediate node keys to other members of the group.

Chang et al. [6] used boolean function minimization technique to binary trees to minimize the cost of communication. Although the size of rekeying messages and the storage of GC are reduced, their scheme is not secure against the attack by colluding or compromised members who can cooperate to determine all the keys of the system.

1.2 Our Contribution

We present a novel group key agreement scheme called logical identity hierarchy(LIH) for multicast, which uses a bilinear pairing based cryptography [20,21, 22, 23, 24, 25, 26, 27, 28, 29]. LIH is an identity tree where each node in the tree is associated with an identity and a key generation key(KGK). The leaf node's identity is corresponding to the user's identity and the interior node's identity is generated by its children's identities. So in LIH, an interior node represents