A Distributed Key Assignment Protocol for Secure Multicast Based on Proxy Cryptography

Chun-Ying Huang, Yun-Peng Chiu, Kuan-Ta Chen, and Chin-Laung Lei
Department of Electrical Engineering
National Taiwan University
Taipei, Taiwan
{huangant, frank, jethro}@fractal.ee.ntu.edu.tw, lei@cc.ee.ntu.edu.tw

ABSTRACT

A secure multicast framework should only allow authorized members of a group to decrypt received messages; usually one "group key" is shared by all approved members. However, this raises the problem of "one affects all," whereby the actions of one member affect the whole group. Many researchers solve the problem by dividing a group into several subgroups, but most existing solutions require a centralized trusted controller to coordinate cryptographic keys for subgroups. We believe this is a constraint on network scalability. In this paper, we propose a novel framework to solve key management problems in multicast networks. Our contribution is three-fold: 1) We exploit the ElGamal cryptosystem and propose the idea of key composition; 2) A distributed key assignment protocol is proposed to eliminate the need for a centralized trust controller in a secure multicast network that leverages proxy cryptography; and 3) We adopt a hybrid encryption technique that makes our framework more efficient and practical. Comparison with similar frameworks shows the proposed scheme is efficient in both time and space complexity. In addition, costs of most protocol operations are bounded by constants regardless of a group's size and the degree of transit nodes.

Keywords

ElGamal cryptosystem, key composition, proxy cryptography, secure multicast

A great deal of research has focused on security mechanisms for multicast trees and group communications. In general, secure multicast mechanisms, can be classified as centralized, decentralized, or distributed. Centralized mechanisms, like LKH, employ a single entity to control the whole group and seek to minimize storage, computational power, and bandwidth requirements. However, since there is only a single entity, the possibility of single point of failure increases. Decentralized methods, such as IOLUS, DEP, and cipher sequence, divide a group into several subgroups. Better scalability and reliability are achieved by confining failures to subgroups. Nevertheless, these methods still require a centralized controller to coordinate the cryptographic keys for different subgroups. Distributed approaches, like GDH and TGDH, eliminate centralized controllers. All group members can contribute to the required cryptographic key or it can be generated by one member. The result is a group key shared by all members. Thus, each user must be aware of the group membership list. In addition, computation and communication requirements may grow linearly as the number of group members increases. Each approach has benefits and drawbacks. However, to construct a large-scale secure multicast network, especially one that requires the collaboration of nodes in different administrative domains, we believe a hybrid framework that uses a decentralized model working in a distributed manner is a good choice.

In this paper, we propose a secure multicast framework that takes advantage of both the decentralized and distributed approaches. We construct the framework in two steps. First, we exploit the mathematics used in ElGamal cryptography [2] and proxy cryptography [1] and extend the calculations to develop a technique for key composition. Then, using key composition, we propose a distributed key assignment protocol (DKAP) that eliminates the centralized controller used in proxy cryptography-based secure multicast networks. The framework leverages proxy cryptography to deliver key encryption keys (KEKs). *Proxy cryptography has several benefits, including lower key storage requirements, content invisibility on intermediate proxies, and low computational complexity regardless of degrees of a proxy.* Since a proxy converts an encrypted message without understanding the original message, it is suitable for a large-scale network, especially when most intermediate nodes are not totally trusted.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.
ASIACCS '06, March 21—24, 2006, Taipei, Taiwan
Copyright 2006 ACM 1-59593-272-0/06/0003 ...$5.00.

1. REFERENCES

[1] M. Blaze, G. Bleumer, and M. Strauss. Divertible protocols and atomic proxy cryptography. In *Proceedings of Advances in Cryptology: EUROCRYPT'98: International Conference on the Theory and Applications of Cryptology Techniques*, pages 127–144. LNCS, May 1998.

[2] T. Elgamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 31:469–472, 1985.