Secure Content Delivery using Key Composition

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

Abstract

In this paper, we propose a novel framework for secure multicast on overlay networks. Our contributions are threefold: 1) a technique key composition is proposed to cope with the secure multicast problems, 2) the proposed framework is totally distributed, i.e., no centralized control is required for subgroup configurations, and 3) a comparison of similar frameworks is provided, in which we show the proposed framework is more efficient in that its time and space complexity are bounded by constants, regardless of the number of coexisting groups, the group size, and the degree of transit nodes.

1. Introduction

Due to the lack of security considerations for multicast protocols, several researches [1–5] have been done to establish secure communications over multicast trees. Although these mechanisms could efficiently achieve key agreements in *one* multicast group, they may require a centralized key server, not scale well, or leak content during message delivery. As the emerging of multicast in overlay networks and the importance of secure multicast, in this paper, we construct a framework upon an overlay network that provides secure content delivery service for multiple groups in a single infrastructure. Besides access control and data confidentiality, the proposed framework should be lightweight enough to handle a great number of users in a large scale network.

2. Key Composition

The technique of key composition is a required building block to construct a secure content delivery service. Basically, the technique is derived from the cipher sequence [5] framework. However, instead of composing cryptography functions, the operation is done for secret keys. In key composition, we define two operation for a group of keys $\mathcal{K}$, namely the compose operation ("+") and the decompose operation ("−").

A key is composed by several sub-keys with the compose operation. A sub-key could also be removed from a composed key. The key composition and decomposition could be applied on several public key cryptography algorithms. However, we must keep in mind that *sub-keys cannot be identified from a composed key* by an eavesdropper.

A cryptography algorithm is said to be compatible with key composition if and only if the following two statements are true. 1) There are corresponding compose and decompose operations for secret keys. 2) Either the compose or the decompose operation should generate a new key in the same group of keys $\mathcal{K}$. A suitable candidate is the ElGamal algorithm. For the convenience of illustration (without the considerations for weak keys), we choose a finite cyclic group $\mathcal{K}$ of order q with generator g as the key group. The group contains q keys $\{0, 1, ..., q-1\}$. The compose and the decompose operation is then defined as the arithmetic add and minus operation modulo q, respectively. With these mappings, the resulted key of the compose/decompose operations will always fall in the key group $\mathcal{K}$.

Given $(\mathcal{K}, g^r, q)$, where r is a randomly chosen number from $\mathcal{K}$, the encryption function is defined as

$$E_k(m) = m \cdot g^{rk}, \tag{1}$$

where m is the plaintext and k is the sub-key. The corresponding decryption function is defined as

$$D_k(c) = \frac{c}{g^{rk}}, \tag{2}$$

where c is the ciphertext and k is the composed key. Consequently, the ElGamal algorithm is a proper candidate to work with key composition. In practice, to guarantee sufficient security strength of the ElGamal algorithm, the key group should be carefully chosen.

3. The Framework

We further construct the secure content delivery service with the previously defined building blocks. The service

Proceedings of the IEEE Conference on Local Computer Networks 30th Anniversary (LCN'05)
0-7695-2421-4/05 $20.00 © 2005 IEEE

	LKH	IOLUS	DEP	CS	KC
Total Number of keys	$O(m)$	$O(m)$	$O(m)$	$O(m)$	$O(m)$
Number of keys per member	$O(log(m))$	1	2	1	1
Number of keys at key server	–	2	$O(s)$	$O(s)$	–
Cost of a JOIN event	$O(log(m))$	$O(1)$	$O(1)$	$O(1)$	$O(1)$
Cost of a LEAVE event	$O(log(m))$	$O(1)$	$O(1)$	$O(1)$	$O(1)$
Number of encryptions by a distributor	$O(1)$	$O(d)$	$O(s)$	$O(1)$	$O(1)$
Need to trust intermediate nodes	–	Yes	No	Yes	Partially

— m: total number of members; s: number of subgroups; d: average degree of subgroups

Table 1. Performance comparison with similar frameworks

is constructed on an overlay network similar to [6], where clients and distributors access the overlay network thorough registered access points. Thus, the path between a server and a client forms a unique set, denoted as, for example, (D, A_1, A_2, C).

A naïve solution to construct a generic secure content delivery network is using a *centralized key distribution server*. The key server (KS) knows the detailed topology of the entire overlay network and it is responsible to distribute secret keys. Thus the KS could give sub-keys K_D, K_1, and K_2 to D, A_1, and A_2, respectively. Then, the KS could compute a composed key $K_D + K_1 + K_2$ to the client. During content delivery, a message is encrypted by a randomly generated symmetric secret key K, then the encrypted content is sent along with the K, which is encrypted by the sub-key of the distributor. For access points on the path, they also encrypt the key part by using their own sub-keys. Thus, the client could decrypt the symmetric secret key with the given composed key, and then access the message.

Turning into the distributed model, instead of assign the sub-keys by the KS, the sub-key is now generated by each node itself. Besides, a *pseudo sub-key* is also generated along with the sub-key. Before the message delivery, a client sent a key composition request to obtain the composed key on the path. While the request walks from the client to the distributor, each node X on the path compose both its sub-key K_x and pseudo-key P_x to the existing composed key. On the contrast, while the request returns back from the distributor to the client, intermediate nodes, except the distributor, remove their corresponding pseudo-key from the composed key. The pseudo key of the distributor P_D is sent to the client through a secure channel and the client could obtain the right composed key to decrypt further messages. Since P_D has to send to clients, the distributor has to generate different P_D for different key composition requests.

4. Evaluations

A brief comparison of our framework and other similar frameworks are given in Table 1. Since we allow multiple groups in a generic network, for the ease of comparison, it is done for a single group. In Table 1, the number of all members is denoted by m, the number of subgroups for the scheme that uses subgrouping technique is denoted as s, and the average degree of subgroups is d. Performance of the our framework is list in the column with a label of KC.

5. Conclusions

In this paper, we propose a scalable and lightweight framework that provides a secure content delivery service upon overlay networks. The framework is constructed with a novel technique named key composition. With these properties of the key composition and overlay networks, the framework could operate in a distributed manner, i.e., no explicitly centralized key server is required. The process of content delivery is very efficient. Each encryption-capable node requires only $O(1)$ encryption to guarantee the confidentiality of a message. Costs of storage and computations for the key distribution process are also bounded by constants. The performance comparison shows that our framework is efficient among similar frameworks.

References

[1] D. Wallner, E. Harder, and R. Agee, "Key management for multicast: Issues and architectures," *RFC 2627*, June 1999.

[2] C. K. Wong, M. Gouda, and S. S. Lam, "Secure group communications using key graphs," *IEEE/ACM Transactions on Networking*, vol. 8, no. 1, pp. 16–30, 2000.

[3] S. Mittra, "Iolus: a framework for scalable secure multicasting," in *Proceedings of the conference on Applications, technologies, architectures, and protocols for computer communication*. ACM SIGCOMM, 1997, pp. 277–288.

[4] L. Dondeti, S. Mukherjee, and A. Samal, "Scalable secure one-to-many group communication using dual encryption," *Computer Communication*, vol. 23, no. 17, 2000.

[5] R. Molva and A. Pannetrat, "Scalable multicast security with dynamic recipient groups," vol. 3, no. 3. ACM Press, 2000, pp. 136–160.

[6] A. D. Keromytis, V. Misra, and D. Rubenstein, "SOS: Secure overlay services," *IEEE Journal on Selected Areas in Communications*, vol. 22, pp. 176–188, Feb. 2004.