

An Information Theoretic Approach to Secure Multicast Key Management

R. Poovendran and J. S. Baras

Dept. of Electrical Engineering & Institute for Systems Research
University of Maryland, College Park, MD 20742, USA
{radha, baras}@isr.umd.edu

Abstract — New results are presented for recently proposed rooted tree based secure multicast key revocation schemes [1, 2] by studying the information theoretic properties of *member revocation events*. It is shown that the optimal average number of keys per person is given by the entropy of the member revocation event and the currently available solutions correspond to the worst case or the maximum entropy scenario. It is shown that the proposed key assignment in [2] corresponds to optimal source coding and is susceptible to attack by compromise or collusion of multiple members.

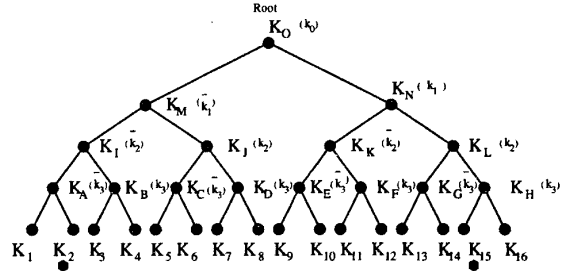


Figure 1: The rooted key distribution tree
Key allocation corresponding to [2] are shown in parenthesis
A possible collusion pair is shown by members 2 and 15

I. INTRODUCTION

Secure multicast communication requires all the members to share a common key to encrypt the traffic. In the event of a member compromise, it becomes necessary to revoke the old traffic keys and securely distribute the new traffic keys to remaining members of the group. Another important constraint is that members (revoked or otherwise) should not be able to *collude* among themselves and construct the (future or other) keys used by the group. Contacting individual members and securely updating the traffic keys takes $\mathcal{O}(N)$ computations at the group center node. Noting that all N members can be uniquely indexed using $\log_d N$ d -ary digits, a scheme based on d -ary rooted tree of depth $\log_d N$ has been proposed [1, 2]. Each of the member indices are directly mapped to a unique leaf of a d -ary tree and a set of keys representing the intermediate nodes of the tree between the root and each leaf is assigned to individual members.

Figure 1 illustrates the rooted tree scheme for $N = 16$ with the leaf key indices also representing the indices of the group members. For example, member 1 is indexed by the set of five keys $\{K_O, K_M, K_I, K_A, K_1\}$. In this structure, the whole group can update its keys in $\mathcal{O}(\log_d N)$ encryptions at the group center and one decryption at each leaf node. *e.g.*, if member 1 is to be revoked, keys $\{K_O, K_M, K_I, K_A, K_1\}$ need to be updated for relevant members. The following encryptions and transmissions achieve this task: (a) members with indices 9-16 receive new K_O encrypted with key K_N , (b) members with indices 5-8 receive new $\{K_O, K_M\}$ encrypted with key K_J , (c) members with indices 3-4 receive new $\{K_O, K_M, K_I\}$ encrypted with key K_B , (d) member with index 2 receives new $\{K_O, K_M, K_I, K_1\}$ encrypted with key K_2 .

II. INFORMATION THEORETIC FORMULATION

Since key updates are done in response to revocation of members, statistics of *member revocation events* are very appropriate for system design and performance characterization. We define p_i as the probability of revocation of member i ; $1 \leq i \leq N$ with $\sum_{i=1}^N p_i = 1$.

III. MAIN RESULTS

In order to make sure that revocation of a single member does not render *all* keys held by any other member invalid, no member should have its keys embedded in the set of keys held by another member. This is equivalent to unique decodability in source coding.

Theorem 1: If the concatenation of the set of keys held by each member is viewed as a “codeword” then this collection of codewords satisfy the Kraft inequality.

Theorem 2: Optimal average number of keys per member is given by the *entropy* $H_d = -\sum_{i=1}^N p_i \log_d p_i$ of the member revocation event.

This source-coding viewpoint reveals that currently proposed key management schemes [1, 2] have redundant key allocation. They correspond to the worst case or *maximum entropy* situation where each member is equally likely to be revoked.

Attack by colluding members: The key allocation scheme of [2] uses a set of $2 \log_2 N$ distinct keys as shown in Figure 1. This is shown to correspond to an optimal (Huffman) source coding procedure with $2H_d$ distinct keys. We show that this scheme can be attacked by two colluding or compromised members binary representations of whose indices are *one’s complements* of each other.

Theorem 3: Independent of the value of N or d , the optimal key assignment discussed above allows the integrity of the whole key management scheme to be broken by compromise of or collusion among appropriate subsets of members.

REFERENCES

- [1] D. M. Wallner, E. C. Harder, and R. C. Agee. “Key Management for Multicast: Issues and Architectures”. expired Internet Draft, July 1997.
- [2] G. Caronni, M. Waldvogel, D. Sun, and B. Plattner. “Efficient Security for Large and Dynamic Groups”. In *Proc. of the Seventh Workshop on Enabling Technologies*. IEEE Computer Society Press, 1998.
- [3] J. L. Massey. “An Information-Theoretic Approach to Algorithms”. Impact of Processing Techniques in Communications, In NATO Advanced Study Institutes Series E91, pp. 3-20, 1985.