# Cryptanalysis of Two Group Key Management Protocols for Secure Multicast

Wen Tao Zhu

State Key Laboratory of Information Security,
Graduate University of Chinese Academy of Sciences,
P.O. Box 4588, Beijing 100049, P.R. China
wtzhu@gucas.ac.cn

**Abstract.** Many emerging network applications are based upon group communication models and are implemented as either one-to-many or many-to-many multicast. As a result, providing multicast confidentiality is a critical networking issue and multicast security has become an active research area. To secure the sessions, a common group key is maintained to encrypt the traffic, and the key is updated whenever a new member joins the group or an existing member leaves. In this paper we analyze the security of a centralized key distribution protocol for one-to-many multicast and a decentralized key agreement protocol for many-to-many multicast. We show that they both fail to provide forward and backward security. The first protocol is revealed to be vulnerable to a single adversary due to an algorithmic issue. The second protocol, however, is subject to sophisticated collusion. Remedial approaches are proposed for both key management schemes to effectively resist relevant attacks.

## 1 Introduction

In the Internet, multicast has been used successfully to provide an efficient, best-effort delivery service to large user groups that are dynamic in nature. As a result, multicast confidentiality has become a critical networking issue, since the original Internet protocols paid little attention to security concerns [1]. Specifically, the Internet Group Management Protocol (IGMP) has been designed to provide an open group model and it does not provide an access control mechanism; anyone can join the group and thus obtain a copy of every multicast packet by simply sending membership reports to its neighboring router. It would be very easy to launch a theft of service when the multicast data is transmitted in plaintext.

The standard approach to control access to group communication is to use symmetric cryptography (for minimal computation) with a common shared group key, known as the session encryption key (SEK), to securely distribute data to all intended members. In this paper, we define secure multicast as a private session with such symmetric key encryption of group-oriented data content. Whenever there is a membership change, the SEK needs to be updated to assure backward security that a joining user cannot access previous group communication, and forward security that a leaving user cannot access data multicast after its departure unless

Y.G. Desmedt et al. (Eds.): CANS 2005, LNCS 3810, pp. 35–48, 2005.

it is added back. Ensuring only the valid members of the group hold the SEK at any instant is the secure multicast key management problem [2].

Secure multicast in the Internet has many applications such as subscription CD/TV broadcasting, stock quote updates, remote education, and distributed interactive simulation. Some of them have a single sender distributing secret data to a large number of subscribers while the others have multiple (usually all) registered users communicating privately with each other. In the first case, to protect SSM (Source-Specific Multicast) [3] confidentiality, a centralized key server known as the Group Controller (GC) is preferred to manage the SEK [1, 4–12]. In the second case, to support many-to-many secure multicast among dynamic peers, distributed group key agreement is desirable [13–17]. In this paper, the terms SSM and one-to-may multicast are used interchangeably, so do ASM (Any-Source Multicast) and many-to-many multicast.

The balance of this paper is organized as follows. Section 2 presents an overview of the centralized group key distribution approaches for SSM. One of these schemes, called the Secure Filter [7], is presented and analyzed in Section 3. We show that it has a security breach that may fail to assure forward and backward security, and propose a remedy to invalidate potential attacks. Section 4 presents DISEC [13], an efficient distributed framework for scalable secure many-to-many communication, as a case study of distributed group key agreement protocols for ASM. Section 5 performs security analysis on DISEC. We show that it also fails to provide forward and backward security, and propose two remedial approaches. Our conclusions are in Section 6.

Throughout this paper, we denote the group size of the secure multicast session by $N$. We use the notation $K\{m\}$ to denote the encryption of plaintext message $m$ with key $K$, and the notation A→B: $K\{m\}$ to denote the secure delivery of message $m$ from A to B. For instance, the Group Controller rekeys at time $t_1$ and sends the group key to member $\mathrm{M}_i$, encrypted with a pair-wise key $K_i$, and this is denoted as GC→$\mathrm{M}_i$: $K_i\{SEK(t_1)\}$. This $K_i$, usually pre-assigned, is secretly shared between $\mathrm{M}_i$ and the GC only, and thus we call it the user private key or the individual key of $\mathrm{M}_i$. As $K_i$ is used to protect another cryptographic key (herein the group key $SEK(t_1)$), it is called a Key Encryption Key (KEK). In most cases, a KEK is only used to encrypt one key per message, which conforms to the key-oriented strategy [8]. We now address the centralized group key distribution schemes for securing one-to-many group communication.

## 2 Centralized Group Key Distribution Approaches for SSM

As most of the commercial applications that benefit from multicast communication have a single sender and multiple recipients, it is the model of interest in this section. To secure SSM traffic, a trusted authority, the GC, is introduced to be responsible for the group key distribution. The main requirement is confidentiality: only valid users should be able to decrypt the group communication even if the data is broadcast to the entire network.