Group Security Policy Management for IP Multicast and Group Security

Thomas Hardjono[1] and Hugh Harney[2]

[1] VeriSign Inc., 401 Edgewater Place, Suite 280,
Wakefield, MA 01880, USA
thardjono@verisign.com

[2] Sparta Inc., Secure Systems Engineering Division,
9861 Broken Land Parkway, Suite 300,
Columbia, MD 21046, USA
hh@columbia.sparta.com

Abstract. The current work focuses on the area of group security policy within secure IP multicast and secure group communications. The work explains the background and context, introduces a Group Security Policy Framework, and describes how this fits within the broader Multicast Security Framework developed within the IETF. Finally, the current status of developments within group security policy in the IETF is discussed.

1 Introduction

Group communications, also commonly called multicast, refers to communications in a group where the messages can be sent by any member and are received by all members. They range from mailing lists to conference calls to IP Multicasting. Often the need for data protection arises, which requires the group to handle the messages in a consistently secure manner. To accomplish this, cryptographic mechanisms and security policy must be shared and supported by the group as a whole. Because of this, special problems arise in managing the cryptographic and policy material as it changes or as the group changes.

The current work discusses the need for policies and policy-management for secure groups, placing the discussion in the context of the SMuG/MSEC Framework for Multicast Security in the IETF. The work described the Multicast Security Framework and identified the entities and interactions involved in group security policy management. It then focuses on a framework for group policy management for secure-groups, and explains the current status of developments in the IETF.

E. Gregori et al. (Eds.): NETWORKING 2002, LNCS 2345, pp. 1123-1128, 2002.

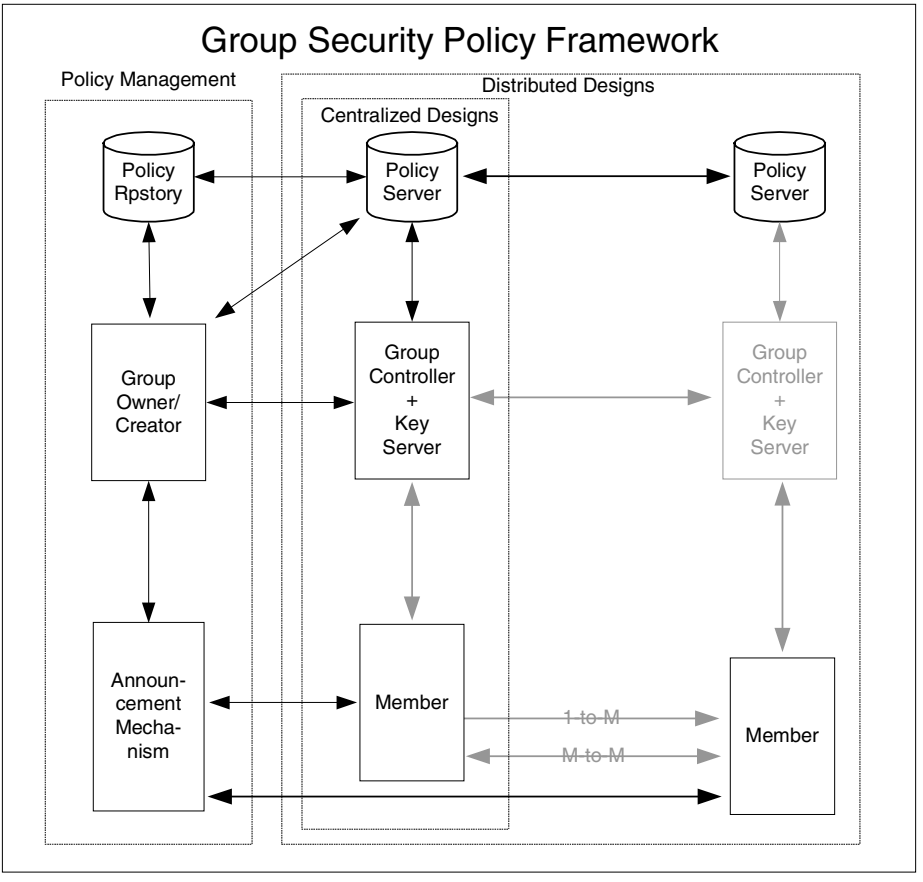

Fig. 1. Group Security Policy Framework

2 Group Security: Background & Framework

There is significant interest in the networking industry and content delivery network (CDN) industry to use IP multicast a vehicle for data delivery to a large audience. One major hindrance to the successful deployment of IP multicast and other group-oriented communication protocols has been the lack of security for both the content and the content-delivery infrastructure.

To this end, the IETF designated in mid-1998 the creation of the Secure Multicast Group (SMuG) under the umbrella of the Internet Research Task Force (IRTF) to research and develop protocols for multicast security. This IRTF group has since been formalized into a IETF Working Group, called Multicast Security (MSEC), early in 2001. The architecture and designs developed within SMuG have largely been

carried-over into the MSEC WG with the aim of further refining and formalizing into specifications for a set of standards documents (RFCs).

The Secure IP Multicast Framework and Building Blocks document [HCBD00] of the IETF describes a number of entities, which participate in the creation, maintenance, and removal of secure multicast groups. Those that are of concern for group security policy are the *Group Controller and Key Server* (GCKS), the *Group Policy Server* (GPS) and *Member* (Receiver and Sender).

The Framework of [HCBD00] identified three broad problem-areas that need to be addressed. These are group key management, data/content handling (i.e. treatment of messages in a crypto context) and group policy. It is the later problem area that is of interest here, and will be further discussed in the following sections.

3 Group Security Policy Framework

The intent of the Framework of [HCBD00] is to present a high-level roadmap for the development of technologies that implement group and multicast security. Thus, to that extent, it was intended that each problem-area would develop its specific or focused framework or architecture. An example of a more focused architecture is one for group key management as reported in [HBH00, BCD01]. In the following section, we discuss a framework for group security policy, using the Framework of [HCBD00] as the starting point. Figure 1 shows a framework for group security policy where additional entities (over those in [HCBD00]) have been introduced relating to group policy. Both centralized and distributed designs are still shown, though slightly skewed to emphasize the distributed designs involving the policy-related entities.

3.1 Group Owner/Creator (GOC)

The Group Owner/Creator (GOC) represents the entity that is understood by all participants and entities in the network as the ultimate controller of the secure group. The entity is understood as having among others the following tasks:

- *Defining group policy*:
  The GOC defines all types and levels of policies pertaining to the group. This assumes that the network infrastructure for policy creation and assignment exists and can be deployed.
- *Setting-up network services*:
  As the creator/owner of a group, the GOC is assumed to also have network resources at all necessary layers of the network to enable the running of the group.
- *Defining membership*:
  The GOC defines the constituency of the group which it is setting-up. The basis of the membership of the group can be loose or tight, using host/user identity, IP addresses, certificates, or even a predefined access control list.
- *Sending out announcements/invitations*:

The GOC is also responsible for putting out an announcement or call to join through the mechanisms it selects. This could be using IP broadcast or multicast, advertising on a website or other mechanisms.

- *Terminating groups*:
  The GOC is also responsible for concluding a secure group, particularly if that group consumes (network) resources.

3.2 Group Policy Servers (GPS)

The Group Policy Server represents the entity that holds available the policies pertaining to groups. This information can be split into the policy items available for the general public (of non-members) and those available only to designated members of a group.

- *Publicly available policy items*:
  This is information pertaining to a secure group that has been previously announced through some public medium and which can be used by hosts/users to evaluate their eligibility to join a group.
- *Private policy items*:
  This is information that is only available to entities that have passed the membership eligibility test. The policy items may represents additional group-related policies that a (strongly authenticated) member needs to know in order to proceed further with participating in the group.

3.3 Group Policy Repository (GPR)

The Group Policy Repository (GPR) has the function of storing the secure group policies, each with the suitable protection levels and with access to it subject to appropriate authorization. Typically, authorization to access the GPR is provided only to the Group Owner/Creator (read/write/modify) and to the GCKS and Policy Servers (read). The first aim of the GPR is to make the policies pertaining to secure groups available on-line. The same is true for GCKSs. The second aim of the GPR is to allow dynamic update of policies by the Group Owner/Creator in cases when updating some policies does not endanger a group in progress.

3.4 Group Policy Announcement Mechanisms

The Group Policy Announcement (GPA) is a functionality that is aimed at making available information about groups to the intended recipient of such announcements. In the case of a Closed Secure Group, the announcement's intended recipients would be the members pre-selected by the Group Owner/Creator. In the case of an Open Secure Groups, the announcement will be readable by the public.

4 Group Security Policy Token

Current work in the IETF have so far focused more on how to define and represent the *security mechanisms* policies in the context of IP multicast security, where IP multicast is seen as the primary transport for group-oriented communications. The *Group Security Policy Token* (GSPT) [HHMCD01] is a structure that represents security mechanisms (and their parameters) used within a secure group (Figure 2). Not all elements of a GSPT for an instance of a group are made public through the announcement. The work of [HHMCD01] is a continuation of earlier work on group policies within the framework of GSAKMP [HCHMF01]. The elements of a GSPT (or *categories* in [MHCPD00]) specify the policies that are to be followed by members of a group, and consist of the following:

- *Policy Identification*: A group must have some means by which it can identify an instance of Group Security Policy in an unambiguous manner.
- *Authorization for Group Actions*: A Group Security Policy must identify the entities allowed to perform actions that affect group members.
- *Access Control to Group Information*: Access control policy defines the entities that will have authorization to hold the key protecting the group data.
- *Mechanisms for Group Security Services*: Identification of the security services used to support group communication is required. For example, policy must state the algorithms used to derive session keys and the types of data transforms to be applied to the group content.
- *Verification of Group Security Policy*: Each policy must present evidence of its validity.

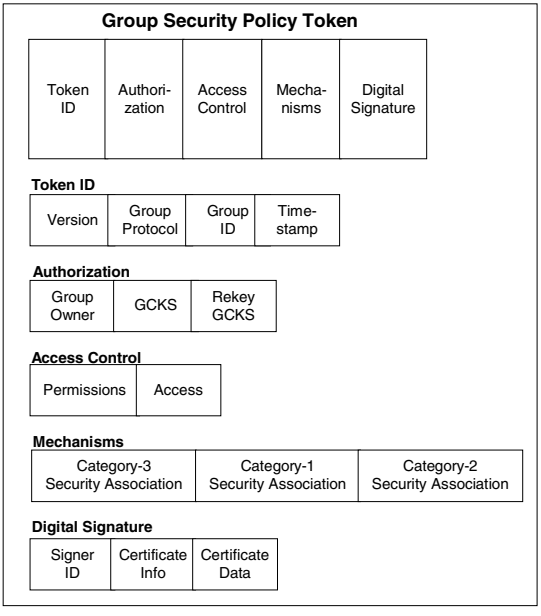

Fig. 2. GSPT Structure

5 Remarks and Conclusion

The current short paper has discussed the need for policies and policy-management for secure groups, placing the discussion in the context of the SMuG/MSEC Framework for Multicast Security in the IETF. The work then presented a more policy-focused framework/architecture using these existing entities, while introducing others that are relevant to group security policy management. The Group Security Policy Token (GSPT) was then presented and discussed. The GSPT represents the current status of development in the IETF in the MSEC Working Group with respect to group security policy.

References

[BCD01] M. Baugher, R. Canetti, L. Dondeti, *Group Key Management Architecture*, draft-ietf-msec-gkmarch-00.txt, June 2001, Work in Progress.

[HBH00] H. Harney, M. Baugher, T. Hardjono, *GKM Building Block: Group Security Association (GSA) Definition*, draft-irtf-smug-gkmbb-gsadef-01.txt, September 2000, Work in Progress.

[HHMCD01] T. Hardjono, H. Harney, P. McDaniel, A. Colgrove, P. Disnmore, *Group Security Policy Token*, draft-ietf-msec-gspt-00.txt, IETF, Work in Progress, Sept 2001.

[HCBD00] T. Hardjono, R. Canetti, M. Baugher, P. Dinsmore, *Secure IP Multicast: Problem Areas, Framework and Building Blocks*, draft-irtf-smug-framework-01.txt, September 2000, Work in Progress.

[HCD00] T. Hardjono, B. Cain, N. Doraswamy, *A Framework for Group Key Management for Multicast Security*, draft-ietf-ipsec-gkmframework-03.txt, August 2000, Work in Progress.

[HCHMF01] H Harney, A Colegrove, E Harder, U Meth, R Fleischer, *Group Secure Association Key Management Protocol (GSAKMP)*, draft-ietf-msec-gsakmp-sec-02.txt, December 2001, Work in Progress.

[MHCPD00] P. McDaniel, H. Harney, A. Colgrove, A. Prakash, P. Dinsmore, *Multicast Security Policy Requirements and Building Blocks*, draft-irtf-smug-polreq-00.txt, November 2000, Work in Progress.

[SMuG-MSEC01] `www.securemulticast.org`