

Internet Engineering Task Force
INTERNET-DRAFT
[draft-irtf-smug-gsadev-00.txt](#)
February 25, 1999

Indermohan Monga
Thomas Hardjono
Nortel Networks
Expires August 25, 1999

Group Security Association (GSA) Definition for IP Multicast

<[draft-irtf-smug-gsadev-00.txt](#)>

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

Abstract

This document provides a definition of the Group Security Association (GSA) for IP multicast, derived from the Security Association (SA) definition for unicast. The document describes the motivations of a GSA and other issues related to the GSA usage in the context of the existing IPsec implementations.

1. Introduction

The current document delves into the issue of the use of IPsec [[KA98a](#)] security associations (SA) in the context of IP multicast. Unlike the traditional unicast IPsec, multicast groups can have one or more senders, and one or more receivers. In the unicast IPsec, the SA parameters are negotiated between the sender and the receiver, where the receiver selects the Security Parameters Index

(SPI) that make-up the SA.

INTERNET DRAFT

25 February 1999

The concept of an IPsec Security Association cannot be easily mapped without modifications to the multicast environment due the nature of group-oriented communications. As an example, in the unicast case it is the receiver that selects the SPI related to that instance of communications. In multicast, however, there can be more than one receiver, and hence arises the issue of who selects the SPI.

In the remainder of the document we present the concepts and motivations underlying the current proposal for a GSA aimed at the 1-to-Many multicast. Other issues related to the 1-to-Many and Many-to-Many multicast, and issues specific to a "Multicast IPsec" (MIPsec) are also discussed.

[2. Multicast Security Associations: Concept](#)

The concept of multicast Security Associations was introduced in the Security Architecture document of [\[KA98a\]](#) and further elucidated in the group key management proposal of [\[HCM98\]](#). The idea is that unlike security associations for one-to-one unicast communications, the security association for a collection of communicating entities will be shared by more than two entities. Hence the notion of a "Group" Security Association (GSA). In the current document we focus on the unidirectional 1-to-Many (1-to-M) multicast applications type, since it represents the simplest group communications behavior. This does not preclude further developments to address the Many-to-Many multicast application type.

In the current document we propose the design and composition of a GSA that will make most use of the previous unicast Security Association (SA) definition of [\[KA98a\]](#) for one-to-one communications. The motivation behind this philosophy is to allow the existing developments of IPsec to be employed for IP multicast with minimum modification.

Unlike the security association in unicast communications where a well-defined entity (eg. the receiver) selects some of the parameters (eg. algorithm, security parameters index or SPI) that make-up the security association, in multicast groups consisting of multiple senders and receivers there is need for a single entity to

choose the parameters that make-up the group security association (GSA).

In the current document we propose that the security parameter index (SPI) of the GSA for a 1-to-Many multicast be selected by an entity involved in the initial steps of the multicast group creation and group key management. The SA parameters are either chosen by the sender or are well known fixed properties of the group. For example, a multicast group A.B.C.D started by a sender E.F.G.H might have fixed security characteristics of 3DES encryption with MD5 authentication.

Monga, Hardjono

[Page 2]

INTERNET DRAFT

25 February 1999

Two possible entities can be defined to select the SPI and/or the group-key:

- (a) The single sender in the 1-to-Many multicast
- (b) A key-management entity, such as the Domain Key Distributor (DKD) in [\[HCM98\]](#).

Regardless of which entity selects the SPI and the group-key, one fundamental issue that remains is the dissemination of the selected parameters to the other members (receivers) of the multicast group.

Since the key-management entities involved in the group-key management (GKM) protocol will be disseminating the group-key to the group members, we relegate the task of disseminating the GSA to these same entities, either through (or part of) the same GKM protocol or through a different GSA distribution protocol executed by these entities.

[3.](#) GSA for Multicast

The current work proposes a definition of a GSA based on the source IP address. A GSA will be uniquely identified by the tuple (source IP address, SPI and protocol).

This mirrors the tuple (destination IP address, SPI and protocol) used to uniquely identify unicast SAs (USA).

There are a number motivating reasons for using the source IP address in a GSA:

1. The current work seeks to address the demand today for IP multicast, which in most cases (if not all) consists of the 1-to-Many multicast.

2. Using the source IP address approach ensures that existing IPsec implementations will not need to change their storage or access mechanisms to their SA Database (SAD).
3. Some multicast routing protocols only admit the creation of 1-to-Many multicast groups (eg. PIMv2), with a unidirectional distribution tree towards the receivers at the leafs of the tree. Assuming a 1-to-Many multicast routing protocol (eg. PIMv2) is deployed, then source-authentication is provided as an inherent part of a (GSA, group-key) pair. Since the underlying 1-to-M multicast routing protocol only admits a single sender as part of its source access-control and since only the valid single sender knows the group-key for that 1-to-Many multicast, it follows that sender-authentication to the receivers is achieved. Even if a dishonest receiver holding the group-key attempts to send to the group, the multicast distribution tree itself may not permit this.

4. The anti-replay features of IPsec can still be deployed. Since there is only a single source per GSA, consistency and monotonicity of the sequence number can be guaranteed.

Note, that, if a host is a sender for more than one 1-to-M multicast groups, the sender needs to make sure that the SPI is different for each GSA it uses. Note also, that the current approach to defining the GSA solves some of the issues raised by [\[CCP99\]](#) ([Section 6](#)).

There are two general types of multicast: one-to-many and many-to-many. The one-to-many multicast involves one sender sending data via multicast to the members (receivers) of the group. The many-to-many multicast group assumes that each member of the multicast group can become a sender of data to the multicast group if it so chooses. The two cases are discussed in the sections below in the context of the GSA usage.

3.1 One-to-Many Multicast

Only one fixed sender sends multicast data using one GSA for the

group. The receivers in the multicast group save the (received) GSA in the inbound SAD. On receiving an encrypted packet, the source IP address, SPI and protocol from the packet are used to retrieve the proper GSA from the inbound SAD to decrypt the packet.

3.2 Many-to-Many Multicast

The case of the Many-to-Many multicast is more complex since multiple senders may exist and thus a mechanism to determine (negotiate) the parameters among the multiple senders must be employed. Unlike the 1-to-Many multicast, the Many-to-Many can involve more than one sender, and in reality the number of active receivers can even be less than the number of sender (ie. some senders are not receivers). The current document places the issue of Many-to-Many for later work.

Some points of consideration concern the behavior of the underlying multicast routing protocol with respect to the current definition of security associations for groups.

As mentioned above, some multicast routing protocols only admit the creation of 1-to-Many multicast groups, with a unidirectional distribution tree towards the receivers at the leafs of the tree. With such multicast routing protocols, the creation of a M-to-M multicast can be effected through the overlaying M of the 1-to-M multicast.

If such is the case with the multicast routing protocol, then each of the M layers (consisting of a 1-to-M multicast) can be served with a separate GSA. In essence, each receiver must maintain M GSAs (and M group-keys) corresponding to the M individual sources/senders. Although at first this may appear to be a possible overhead, there are some advantages of using M layers of the 1-to-Many multicast.

The first advantage, as mentioned previously, is that source-authentication is provided as an inherent part of a (GSA, group-key) pair.

The second advantage, is that having M separate 1-to-Many multicasts allows a receiver to choose particular sources from which it wishes to hear. This selective reception of sources can be done by the

receiver simply opting not to join one (or several) 1-to-M multicast, or it can be performed on a policy-basis by the local administration. This approach also falls inline with the future promise of IGMPv3 [[CDT99](#)] in which a host has the option of specifying with sources of a multicast group it wishes to listen to, through IGMPv3.

The third advantage, which ties into the first, is that the anti-replay features of IPsec can still be deployed in each of the 1-to-M multicast layers of the M-to-M multicast.

3.3 Dissemination of 1-to-Many GSAs

In the context of a 1-to-M multicast group, an important issue that needs to be addressed is that of the dissemination of the GSA to the M receivers in the group.

Assuming that the sender is already in possession of the GSA, one possible mechanism to deliver the GSA to the M receivers is through the same method as the group-key delivery. The motivation here is that since the GKM protocol is already delivering a crucial piece of information (the group-key) and is trusted to do so, then it makes sense for the delivery of the GSA to be coupled to the delivery of the group-key matching the GSA.

Note a GSA must be coupled with its respective group-key. Thus, when a group-key is to be re-keyed, a new SPI must be created, and thus a new GSA. Hence, in the current work we propose the delivery of the group-key and its GSA as a single unit.

3.4 GSA Parameters

This sections discusses certain unicast SA parameters [[KA98a](#)] which have a direct bearing on MIPsec.

- IPsec Protocol Mode:
The IP security architecture describes two different types of IPsec SAs: tunnel and transport. A transport mode SA is used to securely communicate between two hosts. A tunnel mode SA is used to protect communication between two security gateways or between a security gateway and a host. Since members of a multicast group are assumed to be end-hosts, we propose that GSAs be defined for

transport mode only. Note that this decision does not prevent multicast traffic being tunneled over a set of unicast IPsec SAs. Furthermore, this does not preclude the possibility of a gateway entity in itself becoming an "end-host" of a multicast group.

- Anti-replay window: All multicast receivers are REQUIRED to implement this window.
- AH Authentication algorithm, keys, ESP Encryption algorithm, authentication algorithm, keys etc: Unlike IPsec SAs, these parameters are not negotiated but generated by the sender(s) of the multicast group or a DKD entity [HCM98] and propagated to the multicast receivers using GKM protocol.
- Lifetime of GSA: The sender MUST choose the time interval the GSAs are valid, whether they be time based or kilobyte based. The sender is responsible for taking the appropriate action, either creating a new GSA or terminating the existing GSA, when the existing GSA expires. The receivers are NOT REQUIRED to track the lifetime of the GSA. The GSA lifetime must be constrained by the validity of the senders certificate, if that is provided in the GSA.

3.5 Combining GSAs

Multicast senders and receivers MUST support transport adjacency of GSAs as described in [Section 4.3](#) of IPsec Security Architecture [KA98a]. They are NOT REQUIRED to support iterated tunneling.

4. Security Association Database

The concept of GSAs integrates seamlessly with the SAD concept described in the IPsec Security Architecture document[KA98a]. Since GSAs have the same number of unique parameters which are of same/similar type, GSAs can be stored/accessed from the same SAD meant for unicast IPsec SAs. This reduces the complexity of multicast security implementation in the client.

5. References

[HCM98] T. Hardjono, B. Cain and I. Monga, "Intra-Domain Group Key Management Protocol", Internet Draft, July 1998.

[draft-ietf-ipsec-intragkm-00.txt](#)

[KA98a] S. Kent and R. Atkinson, "Security Architecture for the Internet Protocol", IETF, [RFC 2401](#), 1998.

[CDT99] B. Cain, S. Deering and A. Thyagarajan, "Internet Group Management Protocol, Version 3", Internet Draft, February 1999.

[draft-ietf-idmr-igmp-v3-01.txt](#)

[CCP99] R. Canetti, P-C. Cheng, D. Pendarakis, J.R. Rao, P.Rohatgi and D. Saha, "An Architecture for Secure Internet Multicast".

Internet Draft, February 1999. [draft-irtf-smug-sec-mcast-arch-00.txt](#)

6. Author Addresses

Indermohan Monga

Email: imonga@baynetworks.com

Thomas Hardjono

Email: thardjono@baynetworks.com

Nortel Networks

3 Federal Street, B13-03

Billerica, MA 01821, USA

Tel: +1-978-916-4538

