PIM
Internet-Draft
Intended status: Standards Track
Expires: January 5, 2015

W. Atwood
B. Li
Concordia University/CSE

July 4, 2014

Secure Internet Group Management Protocol
draft-atwood-pim-sigmp-01

Abstract

This document specifies a Secure Internet Group Management Protocol (SIGMP), which is an extension to IGMP to enforce receiver access control for secured multicast groups. In SIGMP, only the hosts operated by authorized end users are permitted to report their interest in secured groups. IPsec is used to filter the messages that report or query the interest in secured groups. SIGMP provides two working modes that are fully compatible with IGMP v2 and IGMP v3 respectively.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on January 5, 2015.

Copyright Notice

Table of Contents

1. Introduction

The Internet Group Management Protocol (IGMP) is used by IPv4 systems (hosts and routers) to report their IP multicast group memberships to any neighboring multicast routers. There are two popular versions: IGMP v2, as specified in [RFC2236] and IGMP v3, as specified in [RFC3376]. However, both versions establish a fully "open" multicast network, where any host can join any multicast group as a recipient without receiver access control.

This document specifies a Secure Internet Group Management Protocol (SIGMP) working in a "hybrid" multicast network. In a hybrid network, multicast groups are classified into two categories: open groups and secured groups. Open groups refer to multicast groups that any host can join unconditionally as a receiver. Secured groups refer to multicast groups with receiver access control, e.g., only hosts operated by authenticated and authorized end users are permitted to join as receivers. SIGMP retains most mechanisms of IGMP and enforces receiver access control to secured groups in a multicast network. On the one hand, any host could report its

interest in open groups freely as in IGMP. On the other hand, only hosts operated by the authenticated and authorized end users are permitted to report their interest in secured groups.

Instead of a new specific mechanism, SIGMP uses IPsec [RFC4301] to implement receiver access control to secured groups at the IP layer. Some Security Associations (SAs) are created to secure the SIGMP packets that are used to report or query secured groups. The packets coming from the unauthorized hosts will be discarded by the IPsec subsystem if they are used to report or query interest in secured groups.

1.1. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT","SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

It is assumed that the reader is familiar with the defining documents for IGMP [RFC2236] and [RFC3376]. Unless otherwise noted, terms defined in these documents are used with the same meaning in this one.

In addition, the following terms are used in this document.

open group: A multicast group without receiver access control. Any host can unconditionally join any open group as a receiver, e.g. the data in a open group can be received by any host.

secured group: A multicast group with receiver access control. Only hosts operated by authenticated and authorized end users are permitted to join a secured group as a receiver, e.g. the data in a secured group can only be received by hosts operated by authenticated and authorized end users.

1.2. Assumptions

In order to focus on the actions of group membership (e.g., joining and leaving groups), the following topics are assumed to be discussed elsewhere:

1. how to distinguish between secured groups and open groups;

2. how to authenticate and authorize the operators of the devices (hosts and routers);

3. how to distribute the necessary Security Associations to participant devices (hosts and routers).

The existence of the group property (secured or open) defines the hybrid nature of the environment in which SIGMP works. A variety of existing protocols (e.g., LDAP) can be used to enquire as to the status of a particular multicast group.

The hosts that show interest in secured groups MUST be operated by authenticated and authorized end users. One approach to the task of authentication and authorization of end users is based on the use of PANA [RFC5191] and EAP [RFC3748], and is described in [I-D.atwood-mboned-mrac-req], [I-D.atwood-mboned-mrac-arch] and draft-atwood-mboned-pana (not yet published).

A coordination protocol may be needed to manage and distribute the Security Associations (SAs) for secured groups among the routers and the hosts that correspond to authenticated and authorized end users. One set of possible procedures for SA creation and maintenance is specified in draft-atwood-pim-gsam (not yet published).

2. Overview of SIGMP

SIGMP is an extension to IGMP and performs receiver access control for groups in a multicast network. It retains most mechanisms of IGMP and has two working modes: 1) mode compatible with IGMP v2 and 2) mode compatible with IGMP v3. It works in either mode and is transparent for hosts that support only IGMP, i.e., that do not support SIGMP. In addition, SIGMP uses IPsec to secure part of its packets. For an open group, it delivers the data to any host unconditionally as IGMP does. However, for a secured group, SIGMP only delivers the data to the hosts that have established SAs in the IPsec subsystem in order to perform access control.

In a network segment, hosts show their interest in secured groups using IPsec protected packets although their interest for open groups is still reported using unprotected packets. Similarly, routers query the membership interest for a secured group using IPsec protected packets, although the general query and the query for the membership of open groups are performed using unprotected packets.

In general, the packets in SIGMP are classified into four categories, which are Query for Open Group (OGQ), Query for Secured Group (SGQ), Report for Open Group (OGR) and Report for Secured Group (SGR). OGQ and SGQ are sent by the the Querier and are used to learn the membership of open groups (or all groups for general query) and secured groups respectively. In detail, OGQ includes general query, specific-group query for open group and group-and-source-specific

query for the source of open group. SGQ includes specific-group query for secured group and group-and-source-specific query for the source of secured group. OGR and SGR are sent by hosts and used to report the membership of open groups and secured groups respectively. In detail, OGR includes report to specific-group query for open group, report to group-and-source-specific query for the source of open group, unsolicited report for open group and part of reports to general query. SGR includes report to specific-group query for secured group, report to group-and-source-specific query for the source of secured group, unsolicited report for secured group and part of reports to general query. SGQ and SGR are protected by IPsec at IP layer while OGQ and OGR are delivered without IPsec protection.

The destination address of packets in IP layer is specified as follows. In SGQ and SGR, the destination address is a secured group address. In OGQ, it is 224.0.0.1 if the packet is general query and otherwise it is an open group address. In OGR, it is 224.0.0.22 if the packet is the report to general query compatible with IGMP v3 and otherwise it is an open group address. The two addresses of 224.0.0.1 and 224.0.0.22 are the open group addresses. NOTE: When SIGMP works in the mode compatible with IGMP v3, the response to a general query contains zero or one OGR and zero or more SGR. It is described in detail in Section 5.2.1.

3. Packet Format

The packet format of SIGMP is identical to the packet format for IGMP. In detail, the format is the same as IGMP v2 when SIGMP works in the mode compatible with IGMP v2. The format is the same as IGMP v3 when SIGMP works in the mode compatible with IGMP v3.

4. Router Operations

Router operations in SIGMP are based on router operations in IGMP. However, some additional operations must be appended since access control to secured groups is extended into SIGMP. This section describes the additional operations for the two working modes.

4.1. Router Operations Compatible with IGMP v2

The additional router operations focus on the operations for a received report.

4.1.1. Router Operations for a Received Report

On receiving a report, a router checks the group address in the received report. If the group address indicates an open group, the report is considered as an OGR. A router will process an OGR as it

does that in IGMP v2 directly. Otherwise, the received report is an SGR that SHOULD just have been authenticated (and decrypted) by the IPsec subsystem (e.g., AH [RFC4302]). For SGR, a router must perform two verifications: address consistency and SA existence.

In the address consistency verification, a router compares two addresses: the group address in the SIGMP report and the destination address in the IP header. The verification fails if the two addresses are not the same. In the failure case, the sender of the IGMP Report has attempted to hide a request for a specific group (probably a secured group) in an IGMP Report for a different group (probably an open group). This will cause the IPsec subsystem to deliver the IGMP Report without requiring it to be protected. Therefore a router must discard the report if this address consistency verification fails.

In the SA existence verification, a router checks whether SAs have been established for the secured group whose address is contained in the received report. The verification fails if there are no valid SAs for the group in the router's IPsec subsystem. Since the IPsec subsystem is used to enforce the access control, no access to a secured group is permitted until its SAs have been established. Therefore a router must discard the report if this verification fails.

If the two verifications succeed on SGR, a router will proceed to update the group memberships and refresh the timers as it does in IGMP v2. In summary, the router operations for a received report are shown in Table 1.

#	Group Address	Address Consistency	SA Existence	Operations for Report
1	Open	-	-	Process as IGMP v2
2	Secured	No	-	Discard
3	Secured	Yes	No	Discard
4	Secured	Yes	Yes	Process as IGMP v2

Table 1: Router Operations for a Received Report for the Mode Compatible with IGMP v2

4.2. Router Operations Compatible with IGMP v3

The additional router operations still focus on the operations for a received report. However, there is a little difference between the operations in the mode compatible with IGMP v3 and the operations in the mode compatible with IGMP v2, since the formats of received reports in the two modes are different.

4.2.1. Router Operations on a Received Report

On receiving a report, a router checks the number of group records in the report. If the number is more than one, it indicates that the report is an OGR, but not an SGR, since only one group record is included in an SGR. In this case, every group record in the report must be verified further as follows. A router checks the multicast address in the group record. If the multicast address is an open group address, a router will process the group record as it does in IGMP v3. Otherwise, a secured group address is in the group record and a router must discard the group record. The OGR including more than one group records is not protected by IPsec systems and is not permitted to contain any information related to any secured group.

In contrast, if the number of the group records is just one, a router still checks the multicast address in the single group record. If the multicast address indicates an open group address, the received report is considered as an OGR and a router will process the group record as it does that in IGMP v3 directly. Otherwise, the received report SHOULD be an SGR that SHOULD just be authenticated (and decrypted) by the IPsec subsystem. For the single group record in the SGR, a router must perform two verifications, address consistency and SA existence, similar to Section 4.1.

In the address consistency verification, a router compares two addresses: the multicast address in the group record of the SIGMP report and the destination address in the IP header. A router must discard the report if the two addresses are not the same.

In SA existence verification, a router checks whether SAs have been established for the secured group whose address is contained in the group record of the received report. A router must discard the report if there are no SAs established in the router’s IPsec subsystem.

If the two verifications succeed on an SGR, a router will proceed to update the group memberships and refresh the timers as it does in IGMP v3. In summary, router operations for a received report are shown in Table 2.

#	#Group record in report	Multicast Address in Group Record	Address Consistency	SA Existence	Operations for Group Record
1	>1	Open	-	-	Process as IGMP v2
2	>1	Secured	-	-	Discard
3	=1	Open	-	-	Process as IGMP v2
4	=1	Secured	No	-	Discard
5	=1	Secured	Yes	No	Discard
6	=1	Secured	Yes	Yes	Process as IGMP v2

Table 2: Router Operations for a Received Report for Mode Compatible with IGMP v3

5. Host Operations

Host operations in SIGMP are based on host operations in IGMP. However, some additional operations must be appended since access control to secured group is extended into SIGMP. This section describes the additional operations for the two working modes.

5.1. Host Operations Compatible with IGMP v2

The additional host operations focus on the conditions for unsolicited report and the operations for a received query.

5.1.1. Conditions for Unsolicited Report

Before creating an unsolicited report, a host must check the reported group. If the report group is open, a host will do as in IGMP v2. If secured, a host must continue to check whether SAs have been established for the secured group. If no SA is defined for this group address, a host MUST return an error indication to the issuer of the request that provoked the unsolicited report. [[Is this the right behavior?]]

5.1.2. Host Operations for a Received Query

On receiving the query, a host does the additional operation as a router does in Section 4.2.1.

5.2. Host Operations Compatible with IGMP v3

The additional host operations focus on three aspects: 1) the conditions for unsolicited report, 2) the operations for a received non-general query and 3) the operations for a received general query. The first two are identical to those described in Section 5.1.1 and Section 5.1.2. In this subsection, only the last case is explained.

5.2.1. Host Operations for a Received General Query

When it determines to respond to a general query, a host creates zero or one OGR and zero or more SGR in SIGMP instead of one report in IGMP v3. The OGR reports the current state of all the open groups that the host is interested in. Each SGR reports the current state of one secured group that the host in interested in.

At the IP layer, the destination address of OGR is 224.0.0.22. In contrast, at the IP layer the destination addresses of SGRs are the secured group addresses. Since IPsec has established SAs for secured groups, SGRs will be protected and the OGR will not.

6. IANA Considerations

The protocol number of SIGMP is the same as IGMP.

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2236] Fenner, W., "Internet Group Management Protocol, Version 2", RFC 2236, November 1997.

[RFC3376] Cain, B., Deering, S., Kouvelas, I., Fenner, B., and A. Thyagarajan, "Internet Group Management Protocol, Version 3", RFC 3376, October 2002.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

7.2. Informative References

[I-D.atwood-mboned-mrac-arch]
william.atwood@concordia.ca, w., Li, B., and S. Islam, "Architecture for IP Multicast Receiver Access Control", draft-atwood-mboned-mrac-arch-00 (work in progress), October 2013.

[I-D.atwood-mboned-mrac-req]
william.atwood@concordia.ca, w., Islam, S., and B. Li, "Requirements for IP Multicast Receiver Access Control", draft-atwood-mboned-mrac-req-00 (work in progress), October 2013.

[RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.

[RFC4302] Kent, S., "IP Authentication Header", RFC 4302, December 2005.

[RFC5191] Forsberg, D., Ohba, Y., Patil, B., Tschofenig, H., and A. Yegin, "Protocol for Carrying Authentication for Network Access (PANA)", RFC 5191, May 2008.

Authors' Addresses

William Atwood
Concordia University/CSE
1455 de Maisonneuve Blvd, West
Montreal, QC H3G 1M8
Canada

Phone: +1(514)848-2424 ext3046
Email: william.atwood@concordia.ca
URI: http://users.encs.concordia.ca/~bill

Bing Li
Concordia University/CSE
1455 de Maisonneuve Blvd, West
Montreal, QC H3G 1M8
Canada

Email: leebingice@gmail.com