PIM Working Group
Internet-Draft
Expires: December 25, 2006

W. Atwood
S. Islam
Concordia University/CSE
June 23, 2006

Security Issues in PIM-SM Link-local Messages
draft-atwood-pim-sm-linklocal-01

Status of this Memo

Copyright Notice

Abstract

This document proposes some additions to the specification of the Protocol Independent Multicast - Sparse Mode (PIM-SM) Protocol regarding security issues of its link-local messages. Although the new specifications for IPsec architecture (RFC 4301) and Authorization Header (RFC 4302) permit the use of anti-replay, they counsel against its use for multi-sender, multicast Security Associations. This makes PIM-SM vulnerable to Denial of Service (DoS) attack. In this document, a new proposal is presented to

protect PIM link-local messages while activating the anti-replay mechanism as well. This proposal builds on the new Security Association lookup method that has been specified in RFC 4301 and RFC 4302.

1. Introduction

All the PIM-SM [1] control messages have IP protocol number 103. These messages are either unicast, or multicast with TTL = 1. The source address used for unicast messages is a domain-wide reachable address. For the multicast messages, a link-local address of the interface on which the message is being sent is used as the source address and a special multicast address, ALL_PIM_ROUTERS (224.0.0.13 in IPv4 and ff02::d in IPv6) is used as the destination address. These messages are called link-local messages. Hello, Join/Prune and Assert messages are included in this category. A forged link-local message may be sent to the ALL_PIM_ROUTERS multicast address by an attacker. This type of message affects the construction of the distribution tree [1]. The effects of these forged messages are outlined in section 6.1 of [1]. Some of the effects are very severe, whereas some are minor.

PIM-SM version 2 was originally specified in RFC 2117, and revised in RFC 2362. A PIM-SM Internet Draft [1] has been approved by the IESG for publication as an RFC. It is intended to obsolete RFC 2362, and to correct a number of deficiencies. The Security Considerations section of the PIM-SM Internet Draft is based primarily on the new Authentication Header (AH) specification described in RFC 4302 [2].

Securing the unicast messages can be achieved by the use of a normal unicast IPsec Security Association between the two communicants. Securing the user data exchanges is covered in RFC 3740 [4]. This document focuses on the security issues of link-local messages. It provides some guidelines to take advantage of the new permitted AH functionality, and to bring the PIM-SM Internet Draft into alignment with the new AH specification.

2. Terminology

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in RFC 2119 and indicate requirement levels for compliant PIM-SM implementations.

3. Authentication according to the PIM-SM Internet-Draft

In the PIM-SM Internet Draft, IP Security (IPsec) [[3] transport mode using Authentication Header (AH) [2] is recommended to prevent attacks generated by forged control messages. The Network Administrator will configure the specific AH authentication algorithm and parameters, including the choice of authentication algorithm and the choice of keys. The PIM-SM Internet Draft does not specify protocols for establishing Security Associations. The PIM-SM Internet Draft assumes that manual configuration of Security Associations will be performed, although it does not preclude the use of a negotiation protocol such as the Internet Key Exchange (IKE) [2] to establish Security Associations. Once the Security Associations have been established, all the control messages should go through the IPsec authentication process. A PIM-SM router should authenticate a control message before processing it, and should reject any unauthorized PIM protocol messages.

Given that IPsec [3] provides protection against replayed unicast and multicast messages, the PIM-SM Internet Draft further states that the IPsec anti-replay option SHOULD be enabled for these Security Associations. Unfortunately, the AH specification notes as follows:

> "If the key used to compute an ICV is manually distributed, correct provision of the anti-replay service would require correct maintenance of the counter state at the sender, until the key is replaced, and there would likely be no automated recovery provision if counter overflow were imminent. Thus, a compliant implementation SHOULD NOT provide this service in conjunction with SAs that are manually keyed."

All the link-local messages of the PIM-SM protocol are sent to the destination address, ALL_PIM_ROUTERS, which is a multicast address. The Security Policy Database (SPD) within IPsec (see section 4.4.2 of RFC 4301 [3]) is not capable of representing a policy for a multicast Security Association. RFC 4301 provides no specification for an automated way to create SAD entries for a multicast, inbound SA. Only manually configured SAD entries can be created to accomodate inbound, multicast traffic. As a result, the anti-replay option must be disabled while using the IPsec AH protocol for security of link-local messages.

4. Proposed Authentication Technique

The authentication mechanism [6][7] for PIM link-local messages presented in this document has following two criteria to achieve:

- o The anti-replay mechanism of Authetication Header protocol will be activated while sending/receiving any PIM link-local message.

- o To attain more flexibility, a PIM router will be able to deploy a different authentication method for each directly connected PIM router if necessary. In that case, a PIM router will maintain a separate Security Association per peer PIM router.

4.1. Security Association Lookup

For an SA that carries unicast traffic, three parameters (SPI, destination address and security protocol type (AH or ESP)) are used in the Security Association lookup process for inbound packets. The SPI is sufficient to specify an SA. However, an implementation may use the SPI in conjunction with the IPsec protocol type (AH or ESP) for the SA lookup process. According to RFC 4301 [3] and the AH specification [2], for multicast SAs, in conjunction with the SPI, the destination address or the destination address plus the sender address may also be used in the SA lookup. The security protocol field is not employed for a multicast SA lookup.

The reason for the various prohibitions in the IPsec RFCs concerning multisender multicast SAs lies in the difficulty of coordinating the multiple senders. However, if the use of multicast for link-local messages is examined, it may be seen that in fact the communication need not be coordinated---from the prospective of a receiving router, each peer router is an independent sender. In effect, link-local communication is an SSM communication that happens to use an ASM address (which is shared among all the routers). Two possibilities may be envisaged:

1. The address ALL_PIM_ROUTERS can be specified to operate as a set of SSM Security Associations, when IPsec is enabled;

2. Secure Link-local communication can be specified to occur on an SSM address, instead of ALL_PIM_ROUTERS.

Given that the sender address of an incoming packet will be (globally) unique for a specific sender and in conjunction with the SPI it will be possible for a receiver to sort out the associated SA for that sender from all the SAD entries (even if a single SAD is maintained regardless of the number of interfaces), we propose that the SPI and the sender address MUST be used in the SA lookup process.

4.2. Activating the Anti-replay Mechanism

Although link-level messages on a link constitute a multiple-sender, multiple-receiver group, the use of the sender address for SA lookup essentially resolves the communication into a separate SA for each sender/destination pair. Therefore, the statement in the AH RFC (section 2.5 of [2]) that "for a multi-sender SA, the anti-replay features are not available" becomes irrelevant to PIM-SM link-local message exchange.

To activate the anti-replay mechanism in a unicast communication, the receiver uses the sliding window protocol and it maintains a sequence number for this protocol. This sequence number starts from zero. Each time the sender sends a new packet, it increments this number by one. In a multi-sender multicast group communication, a single sequence number for the entire group would not be enough.

The whole scenario is different for PIM link-local messages. These messages are sent to local links with TTL = 1. A link-local message never propagates through one router to another. Given that the number of peer routers is small, and given that the use of the sender address for SA lookup converts the relationship from a multiple-sender group to multiple single-sender associations, the anti-replay mechanism SHOULD be activated while sending PIM link-local messages, and at that time a PIM router MUST maintain a different sliding window for each directly connected sender.

4.3. Implementing a Security Association Database per Interface

According to RFC 2401 [5], there is nominally a different Security Association Database (SAD) for each router interface. However, RFC 4301 explicitly removes this requirement. The PIM-SM Internet Draft, however, notes the possible utility of this feature. The proposal above to use the source address to resolve the SAs implies that the use of an SAD per interface is not necessary.

4.4. Manual Key Configuration

To establish the SAs at PIM-SM routers, manual key configuration will be feasible, since the number of peers will be small. The Network Administrator will configure a router manually during its boot up process. At that time, the authentication method and the keys per sender basis for each peer router SHOULD be configured. The SAD entry for each sender connected with this router will be created. The Network Admin will also configure the Security Policy Database of a router to ensure the use of the associated SA while sending a link-local message.

The addition of a new router to the set visible from a particular router will clearly require a re-configuration of that router.

A negotiation protocol such as the Internet Key Exchange [2] MAY also be used to negotiate and establish a suitable authentication method and keys for the SA between two routers. However, a PIM router is not expected to join/leave very frequently, so it is doubtful that the overhead of automatic key configuration will be justified. In any case, it will still be necessary to manually configure the basic information that will allow the router to trust its peers. For these reasons, manual key configuration SHOULD be used to establish SAs.

Unfortunately, the use of manual keying is called out in RFC 4302 as a specific reason why anit-replay should be prohibited. It will be necessary to either

1. explicitly override RFC 4302, or

2. design a negotiation protocol to deal with the case of counter overrun.

Once the WG decides that the present proposal is an acceptable direction to follow, the authors are prepared to work on the development of such a negotiation protocol.

4.5. Extended Sequence Number

In the [2], there is a provision for a 64-bit Extended Sequence Number (ESN) as the counter of the sliding window used in the anti-replay protocol. Both the sender and the receiver maintain a 64-bit counter for the sequence number, although only the lower order 32 bits is sent in the transmission. In other words, it will not affect the present header format of AH. If ESN is used, a sender router can send 2^64 -1 packets without any intervention. This number is very large, and from a PIM router's point of view, a PIM router can never exceed this number in its lifetime. This makes it reasonable to permit manual configuration, since the sequence number will never roll over. For this reason, when manual configuration is used, ESN SHOULD be deployed as the sequence number for the sliding window protocol.

5. Security Considerations

The whole document considers the security issues of PIM link-local messages and proposes a mechanism to protect them.

6. References

[1] Fenner, B., "Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification(Revised), draft-ietf-pim-sm-v2-new-12.txt", March 2006.

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

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

[4] Hardjono, T. and B. Weis, "The Multicast Group Security Architecture", RFC 3740, March 2004.

[5] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[6] Islam, S., "Security Issues in PIM-SM Link-local Messages, Master's Thesis, Concordia University", December 2003.

[7] Islam, S., "Security Issues in PIM-SM Link-local Messages, Proceedings of LCN 2004", November 2004.

Authors' Addresses

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

Phone: +1(514)848-2424 ext3046
Email: bill@cse.concordia.ca
URI: http://www.cs.concordia.ca/~bill

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

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.