Internet-Draft
draft-atwood-pim-sm-linklocal-00.txt
Expires: April 2005

J. William Atwood
Salekul Islam
Department of Computer Science
and Software Engineering
Concordia University
October 2004

Security Issues in PIM-SM Link-local Messages

Status of this Memo

Abstract

This document proposes some modifications to the Internet-Draft for Protocol Independent Multicast - Sparse Mode (PIM-SM) Protocol regarding security issues of its link-local messages. To protect these link-local messages, in the Internet-Draft for PIM-SM a security mechanism has been proposed that uses the IPsec Authentication Header (AH) protocol. While using IPsec AH protocol, the anti-replay mechanism has been disabled. This compromise 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 the Internet-Draft that revises the AH protocol.

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 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]. These effects vary for different types of forged messages. 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] is under development, which 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 Authentication Header (AH) described in RFC 2402 [8]. However, Internet-Drafts are in progress to revise the requirements for the AH [5] and the Security Architecture [6]. 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 AH Internet-Draft.

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) [7] transport mode using Authentication Header (AH) [8] 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. 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.

The IPsec anti-replay option has been disabled for these Security Associations. In the PIM-SM Internet-Draft [1], it is suggested as follows:

> "As of this writing, the IPsec anti-replay option does not handle the case of a Security Association identified by a multicast destination address. Thus, the anti-replay option currently must be disabled on these Security Associations. Until replay prevention for link-local multicast messages is addressed, the anti-replay option SHOULD be enabled on all security associations having a unicast destination address."

All the link-local messages of the PIM-SM protocol are sent to the destination address, ALL_PIM_ROUTERS, which is a multicast address. As a result, the anti-replay option must be disabled while using the IPsec AH protocol.

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. The administrator of a PIM network configures each PIM router with one or more Security Associations and the associated value of the Security Parameter Index (SPI).

For each link or interface of a PIM router, the Network Administrator will define a Security Association (SA) and a Security Parameter Index (SPI). To deploy the Security Association mechanism successfully two different databases, the Security Policy Database (SPD) and the Security Association Database (SAD), should

be maintained. The SPD of a router should be configured properly to ensure the use of the associated SA for a link while sending or receiving link-local messages by the router on that link. The SPI is required to be set to zero by a sender router.

According to RFC 2401 [7], there is nominally a different Security Association Database (SAD) for each router interface. The Network Administrator has to assign a different SAD for each router interface. Thus, although the destination address (ALL_PIM_ROUTERS) is same for all link-local PIM packets, the selected Security Association for an inbound PIM packet may vary depending on the interface on which the packet has arrived.

4. Proposed Authentication Technique

The authentication mechanism [3, 4] for PIM link-local messages presented in this document has following two criteria to achieve:

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

- 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 the Internet-Drafts of IPsec Architecture [6] and AH [5] protocol, 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.

In the PIM-SM Internet-Draft, for the PIM-SM link-local messages, the SPI is fixed and is equal to zero, the destination address is also fixed and is equal to ALL_PIM_ROUTERS. As a result, in the SA lookup process, using only the SPI and the destination address, will not be adequate. A PIM-SM router uses the interface address of its local link as the sender address for a link-local message. 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). For this reason, the SPI and the sender address MUST be used in the SA lookup process. As mentioned above, to comply with the IPsec Architecture [6] and AH [5] protocol, the destination address (i.e., ALL_PIM_ROUTERS) MAY be used with the SPI and the sender address. It is clear that adding the destination address to the SA lookup will not change the results of the SA lookup process.

The AH Internet-Draft prohibits the use of SPI=0 on the wire. Therefore, it will also be necessary to specify an SPI different from zero, to be used for link-local messages. This will probably require an IANA assignment to be requested.

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 Internet-Draft that "for a multi-sender SA, the anti-replay features are not available" becomes irrelevant to PIM-SM link-local message exchange. However, it may be necessary to alter the text of the AH Internet-Draft to specifically allow this case.

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.

Note that, the IPsec Architecture [6] and AH [5] protocol do not support the use of anti-replay mechanism if the corresponding Security Association is identified by a multicast destination address. Although the destination address (ALL_PIM_ROUTERS) of PIM link-local messages is a multicast address, the corresponding Security Associations are not identified by this multicast address, and in fact, there should be separate SA for each sender/destination pair.

4.3 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.

4.4 Extended Sequence Number

In the AH Internet-Draft [5], 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 [8]. 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, while 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.

References

[1] Fenner, B., Handley, M., Holbrook, H., Kouvelas, I., "Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification (Revised)", draft-ietf-pim-sm-v2-new-10.txt, work in progress.

[2] Harkins, D., Carrel, D, "The Internet Key Exchange (IKE)", RFC 2409.

[3] Islam, S., "Security Issues in PIM-SM Link-local Messages", Masters Thesis, Concordia University, Montreal, Canada, December 2003.

[4] Islam, S. Atwood, J. W., "Security Issues in PIM-SM Link-local

Messages", accepted for publication in Proceedings of LCN 2004, Tampa, FL, 2004 November 16--18, 2 pages.

[5] Kent, S, "IP Authentication Header", draft-ietf-ipsec-rfc2402bis-07.txt, work in progress.

[6] Kent, S., Atkinson, R., "Security Architecture for the Internet Protocol", draft-ietf-ipsec-rfc2401bis-02.txt, work in progress.

[7] Kent, S., Atkinson, R., "Security Architecture for the Internet Protocol", RFC 2401.

[8] Kent, S. Atkinson, R., "IP Authentication Header", RFC 2402.

Author's Addresses

J. William Atwood
Department of Computer Science and Software Engineering
Concordia University
1455 de Maisonneuve Blvd. West
Montreal, Quebec, H3G 1M8
Canada

Phone: +1 514 848 2424 ext 3046
Email: bill@cse.concordia.ca
URL: http://www.cse.concordia.ca/~bill/

Salekul Islam
Department of Computer Science and Software Engineering
Concordia University
1455 de Maisonneuve Blvd. West
Montreal, Quebec, H3G 1M8
Canada

Phone: +1 514 934 3923
Email: salek_is@cse.concordia.ca

URL: http://www.cse.concordia.ca/~salek_is/