PIM Working Group
Internet-Draft
Updates: 4601 (if approved)
Intended status: Standards Track
Expires: April 29, 2010

W. Atwood
Concordia University/CSE
S. Islam
INRS Energie, Materiaux et Telecommunications
M. Siami
Concordia University/CIISE

October 26, 2009

Authentication and Confidentiality in PIM-SM Link-local Messages
draft-ietf-pim-sm-linklocal-09

Status of this Memo

Copyright Notice

Abstract

RFC 4601 mandates the use of IPsec to ensure authentication of the link-local messages in the Protocol Independent Multicast - Sparse Mode (PIM-SM) routing protocol. This document specifies mechanisms to authenticate the PIM-SM link-local messages using the IP security (IPsec) Encapsulating Security Payload (ESP) or (optionally) the Authentication Header (AH). It specifies optional mechanisms to provide confidentiality using the ESP. Manual keying is specified as the mandatory and default group key management solution. To deal with issues of scalability and security that exist with manual keying, an optional support for automated group key management mechanism is provided. However, the procedures for implementing automated group key management are left to other documents. This document updates RFC 4601.

Table of Contents

1. Introduction

All the PIM-SM [RFC4601] 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 [RFC4601]. The effects of these forged messages are outlined in section 6.1 of [RFC4601]. 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 and RFC 4601. RFC 4601 obsoletes RFC 2362, and corrects a number of deficiencies. The Security Considerations section of RFC 4601 is based primarily on the Authentication Header (AH) specification described in RFC 4302 [RFC4302].

Securing the unicast messages can be achieved by the use of a normal unicast IPsec Security Association between the two communicants.

This document focuses on the security issues for link-local messages. It provides some guidelines to take advantage of the new permitted AH functionality in RFC 4302 and the new permitted ESP functionality in RFC 4303 [RFC4303], and to bring the PIM-SM specification into alignment with the new AH and ESP specifications. In particular, in accordance with RFC 4301, the use of ESP is made mandatory and AH is specified as optional. This document specifies manual key management as mandatory to implement, i.e., that all implementations MUST support, and provides the necessary structure for an automated key management protocol that the PIM routers may use.

1.1. Goals and Non-goals

The primary goal for link-local security is to provide data origin authentication for each link-local message. A secondary goal is to ensure that communication only happens between legitimate peers (i.e., adjacent routers). An optional goal is to provide data confidentiality for the link-local messages.

The first goal implies that each router has a unique identity. It is possible (but not mandatory) that this identity will be based on the unicast identity of the router. (The unicast identity could be, for

example, based on some individually-configured property of the router, or be part of a region-wide public key infrastructure.) The existence of this unique identity is assumed in this specification, but procedures for establishing it are out-of-scope for this document.

The second goal implies that there is some form of "adjacency matrix" that controls the establishment of security associations among adjacent multicast routers. For manual keying, this control will be exercised by the Administrator of the router(s), through the setting of initialization parameters. For automated keying, the existence of this control will be reflected by the contents of the Peer Authorization Database (PAD) (see RFC 4301 [RFC4301]) or the Group Security Policy Database (GSPD) (see RFC 5374 [RFC5374]) in each router. Procedures for controling the adjacency and building the asssociated PAD and GSPD are out-of-scope for this document.

2. 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]. They indicate requirement levels for compliant PIM-SM implementations.

3. Transport Mode vs. Tunnel Mode

All implementations conforming to this specification MUST support transport mode SA to provide required IPsec security to PIM-SM link-local messages. They MAY also support tunnel mode SA to provide required IPsec security to PIM-SM link-local messages. If tunnel mode is used, both destination address preservation and source address preservation MUST be used, as described in Section 3.1 of RFC 5374 [RFC5374].

4. Authentication

Implementations conforming to this specification MUST support authentication for PIM-SM link-local messages. Implementations conforming to this specification MUST support HMAC-SHA1.

In order to provide authentication of PIM-SM link-local messages, implementations MUST support ESP [RFC4303] and MAY support AH [RFC4302].

If ESP in transport mode is used, it will only provide authentication to PIM-SM protocol packets excluding the IP header, extension headers, and options.

If AH in transport mode is used, it will provide authentication to PIM-SM protocol packets, selected portions of the IP header, extension headers and options.

When authentication for PIM-SM link-local messages is enabled,

- o PIM-SM link-local packets that are not protected with AH or ESP MUST be silently discarded, although an implementation MAY maintain a counter of such packets.

- o PIM-SM link-local packets that fail the authentication checks MUST be silently discarded, although an implementation is RECOMMENDED to maintain a counter of such packets. Note: this is an auditable event as described in RFC 4302 [RFC4302] and RFC 4303 [RFC4303].

5. Confidentiality

Implementations conforming to this specification SHOULD support confidentiality for PIM-SM. Implementations supporting confidentiality MUST support AES-CBC with a 128-bit key.

If confidentiality is provided, ESP MUST be used.

When PIM-SM confidentiality is enabled,

- o PIM-SM packets that are not protected with ESP MUST be silently discarded, although an implementation MAY maintain a counter of such packets.

- o PIM-SM packets that fail the confidentiality checks MUST be silently discarded, although an implementation is RECOMMENDED to maintain a counter of such packets. Note: this is an auditable event as described in RFC 4302 [RFC4302] and RFC 4303 [RFC4303].

Note that since authentication MUST be supported by a conforming implementation, an implementation MUST NOT generate the combination of NON-NULL Encryption and NULL Authentication.

6. IPsec Requirements

In order to implement this specification, the following IPsec capabilities are required.

Transport mode
IPsec in transport mode MUST be supported.

Multiple Security Policy Databases (SPDs)
The implementation MUST support multiple SPDs with an SPD selection function that provides an ability to choose a specific SPD based on interface.

Selectors
The implementation MUST be able to use source address, destination address, protocol, and direction as selectors in the SPD.

Interface ID tagging
The implementation MUST be able to tag the inbound packets with the ID of the interface (physical or virtual) on which they arrived.

Manual key support
It MUST be possible to use manually configured keys to secure the specified traffic.

Encryption and authentication algorithms
Encryption and authentication algorithm requirements described in RFC 4835 [RFC4835] apply when ESP and AH are used to protect PIM-SM. Implementations MUST support ESP-NULL, and if providing confidentiality MUST support the RFC4835 [RFC4835] required ESP transforms providing confidentiality. However, in any case, implementations MUST NOT allow the user to choose a stream cipher or block mode cipher in counter mode for use with manual keys.

Encapsulation of ESP packet
IP encapsulation of ESP packets MUST be supported. For simplicity, UDP encapsulation of ESP packets SHOULD NOT be used.

If the automatic keying features of this specification are implemented, the following additional IPsec capabilities are required:

Group Security Policy Database (GSPD)
The implementation MUST support the GSPD that is described in RFC 5374 [RFC5374].

Multiple Group Security Policy Databases
The implementation MUST support multiple GSPDs with a GSPD selection function that provides an ability to choose a specific GSPD based on interface.

Selectors
The implementation MUST be able to use source address, destination address, protocol and direction as selectors in the GSPD.

7. Key Management

All the implementations MUST support manual configuration of the Security Associations (SAs) that will be used to authenticate PIM-SM link-local messages. This does not preclude the use of a negotiation protocol such as the Group Domain Of Interpretation (GDOI) [RFC3547] or Group Secure Association Key Management Protocol (GSAKMP) [RFC4535] to establish these SAs.

7.1. Manual Key Management

To establish the SAs at PIM-SM routers, manual key configuration will be feasible when the number of peers (directly connected routers) is small. The Network Administrator will configure a router manually. At that time, the authentication method and the choice of keys SHOULD be configured. The parameters for the Security Association Database (SAD) will be entered. The Network Administrator will also configure the Security Policy Database of a router to ensure the use of the associated SA while sending a link-local message.

7.2. Automated Key Management

All the link-local messages of the PIM-SM protocol are sent to the destination address, ALL_PIM_ROUTERS, which is a multicast address. By using the sender address in conjunction with the destination address for Security Association lookup, link-local communication turns into an SSM or "one to many" communication.

The procedures for automated key management are not specified in this document.

One option is to use Group Domain Of Interpretation (GDOI) [RFC3547], which enables a group of users or devices to exchange encrypted data using IPsec data encryption. GDOI has been developed to be used in multicast applications, where the number of end users or devices may be large and the end users or devices can dynamically join/leave a multicast group. However, a PIM router is not expected to join/leave very frequently, and the number of routers is small when compared to the possible number of users of a multicast application. Moreover, most of the PIM routers will be located inside the same administrative domain and are considered as trusted parties. It is possible that a subset of GDOI functionalities will be sufficient.

Another option is to use the Group Secure Association Key Management Protocol (GSAKMP) [RFC4535].

7.3. Communications Patterns

Before discussing the set of security associations that are required to properly manage a multicast region that is under the control of a single administration, it is necessary to understand the communications patterns that will exist among the routers in this region. From the perspective of a speaking router, the information from that router is sent (multicast) to all of its neighbors. From the perspective of a listening router, the information coming from each of its neighbors is distinct from the information coming from every other router to which it is directly connected. Thus an administrative region contains many (small) distinct groups, all of which happen to be using the same multicast destination address (e.g., ALL_PIM_ROUTERS, see Section 11), and each of which is centered on the associated speaking router.

Consider the example configuration as shown in Figure 1.

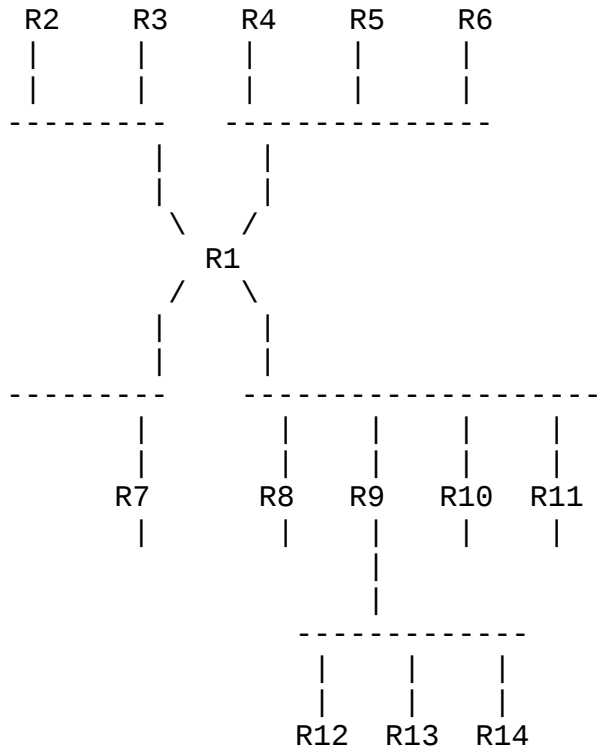

Figure 1: Set of router interconnections

In this configuration, router R1 has four interfaces, and is the speaking router for a group whose listening routers are routers R2 through R11. Router R9 is the speaking router for a group whose listening routers are routers R1, R8 and R10-R14.

From the perspective of R1 as a speaking router, if a Security Association SA1 is assigned to protect outgoing packets from R1, then it is necessary to distribute the key for this association to each of the routers R2 through R11. Similarly, from the perspective of R9 as a speaking router, if a Security Association is assigned to protect the outgoing packets from R9, then it is necessary to distribute the key for this association to each of the routers R1, R8, and R10 through R14.

From the perspective of R1 as a listening router, all packets arriving from R2 through R11 need to be distinguished from each other, to permit selecting the correct Security Association in the SAD. (Packets from each of the peer routers (R2 through R11) represent communication from a different speaker, with a separate sequence number space, even though they are sent using the same destination address.) For a multicast Security Association, RFC 4301 permits using the Source Address in the selection function. If the source addresses used by routers R2 through R11 are globally unique,

then the source addresses of the peer routers are sufficient to achieve the differentiation. If the sending routers use link-local addresses, then these addresses are unique only on a per-interface basis, and it is necessary to use the Interface ID tag as an additional selector, i.e., either the selection function has to have the Interface ID tag as one of its inputs, or separate SADs have to be maintained for each interface.

If the assumption of connectivity to the key server can be made (which is true in the PIM-SM case), then the Group Controller/Key Server (GC/KS) that is used for the management of the keys can be centrally located (and duplicated for reliability). If this assumption cannot be made (i.e., in the case of adjacencies for a unicast router), then some form of "local" key server must be available for each group. Given that the listening routers are never more than one hop away from the speaking router, the speaking router is the obvious place to locate the "local" key server. As such, this may be a useful approach even in the PIM-SM case. This approach has the additional advantage that there is no need to duplicate the local key server for reliability, since if the key server is down, it is very likely that the speaking router is also down.

7.4. Neighbor Relationships

Each distinct group consists of one speaker, and the set of directly connected listeners. If the decision is made to maintain one Security Association per speaker (see Section 8), then the key server will need to be aware of the adjacencies of each speaker. Procedures for managing and distributing these adjacencies are out-of-scope for this document.

8. Number of Security Associations

The number of Security Associations to be maintained by a PIM router depends on the required security level and available key management. This SHOULD be decided by the Network Administrator. Two different ways are shown in Figure 2 and 3. It is assumed that A, B and C are three PIM routers, where B and C are directly connected with A, and there is no direct link between B and C.

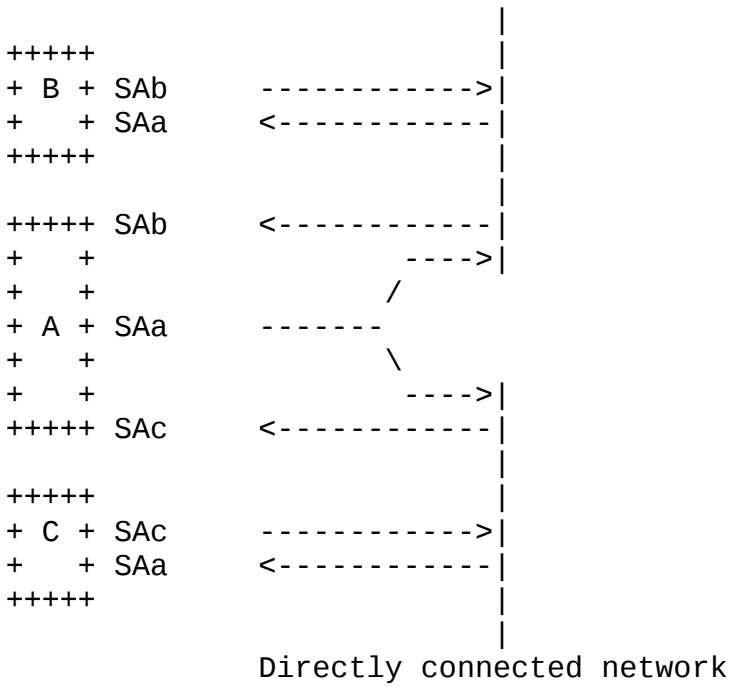

Figure 2: Activate unique Security Association for each peer

The first method, shown in Figure 2, is OPTIONAL to implement. In this method, each node will use a unique SA for its outbound traffic. A, B, and C will use SAa, SAb, and SAc, respectively for sending any traffic. Each node will include the source address when searching the SAD for a match. A will use SAb and SAc for packets received from B and C, respectively. The number of SAs to be activated and maintained by a PIM router will be equal to the number of directly connected routers, plus one for sending its own traffic. Also, the addition of a PIM router in the network will require the addition of another SA on every directly connected PIM router. This solution will be scalable and practically feasible with an automated key management protocol. However, it MAY be used with manual key management, if the number of directly connected routers is small.

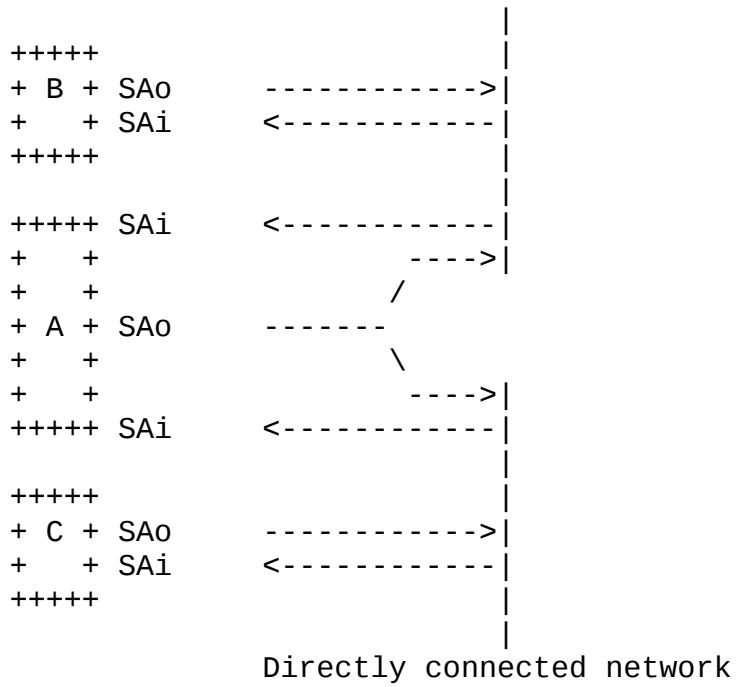

Figure 3: Activate two Security Associations

The second method, shown in Figure 3, MUST be supported by every implementation. In this simple method, all the nodes will use two SAs, one for sending (SAo) and the other for receiving (SAi) traffic. Thus, the number of SAs is always two and will not be affected by addition of a PIM router. Although two different SAs (i.e., SAo and SAi) are used in this method, the SA parameters (keys, Security Parameter Index (SPI), etc.) for the two SAs are identical, i.e., the same information is shared among all the routers in an administrative region. This document RECOMMENDS this second method for manual key configuration. However, it MAY also be used with automated key configuration.

9. Rekeying

Ananalysis of the considerations for key management is provided in RFC 4107 [RFC4107].

In PIM-SM deployments it is expected that secure sessions will be relatively long-lived, and it is not expected that keys will be significantly exposed through normal operational activity. Manual keying is judged acceptable in the light of the relatively low rate of change that is required.

To maintain the security of a link, the authentication and encryption

key values SHOULD be changed periodically, to limit the risk of undetected key disclosure. Keys SHOULD also be changed when there is a change of trusted personnel.

Manual keying offers the ability to change keys in a coordinated way, but it has several drawback in PIM-SM systems. Some of these are listed in Section 15 (Security Considerations) of this document.

According to an analysis in line with RFC 4107 [RFC4107], PIM-SM would benefit from automated key management and roll over because all the disadvantages of manual keys listed in Section 15 would be eliminated. However, suitable techniques for automated key management do not currently exist. Work is in hand in the IETF to develop suitable solutions. In the mean time, implementations MUST support manual rekeying as described below. Implementers and deployers need to be aware of the requirement to upgrade to support automated key management as soon as suitable techniques are available.

9.1. Manual Rekeying Procedure

In accordance with the requirements of RFC 4107 [RFC4107], the following three-step procedure provides a possible mechanism to rekey the routers on a link without dropping PIM-SM protocol packets or disrupting the adjacency, while ensuring that it is always clear which key is being used.

1. For every router on the link, create an additional inbound SA for the interface being rekeyed using a new SPI and the new key.

2. For every router on the link, replace the original outbound SA with one using the new SPI and key values. The SA replacement operation MUST be atomic with respect to sending PIM-SM packets on the link, so that no PIM-SM packets are sent without authentication/encryption

3. For every router on the link, remove the original inbound SA.

Note that all routers on the link MUST complete step 1 before any begin step 2. Likewise, all the routers on the link MUST complete step 2 before any begin step 3.

One way to control the progression from one step to another is for each router to have a configurable time constant KeyRolloverInterval. After the router begins step 1 on a given link, it waits for this interval and then moves to step 2. Likewise, after moving to step 2, it waits for this interval and then moves to step 3.

In order to achieve smooth key transition, all routers on a link MUST use the same value for KeyRolloverInterval and MUST initiate the key rollover process within this time period.

At the end of this time period, all the routers on the link will have a single inbound and outbound SA for PIM-SM with the new SPI and key values.

9.2. KeyRollover Interval

The configured value of KeyRolloverInterval needs to be long enough to allow the administrator to change keys on all the PIM-SM routers. As this value can vary significantly depending on the implementation and the deployment, it is left to the administrator to choose an appropriate value.

9.3. Rekeying Interval

In keeping with the goal of reducing key exposure, the encryption and authentication keys SHOULD be changed at least every 90 days.

10. IPsec Protection Barrier and SPD/GSPD

10.1. Manual Keying

10.1.1. SAD Entries

The Administrator must configure the necessary Security Associations. Each SA entry has the Source Address of an authorized peer, and a Destination Address of ALL_PIM_ROUTERS. Unique SPI values for the manually configured SAs MUST be assigned by the Administrator, to ensure that the SPI does not conflict with existing SPI values in the SAD.

10.1.2. SPD Entries

The Administrator must configure the necessary SPD entries. The SPD entry must ensure that any outbound IP traffic packet traversing the IPsec boundary, with PIM as its next layer protocol, and sent to the Destination Address of ALL_PIM_ROUTERS, is protected by ESP or AH. Note that this characterization includes all the link-local messages (Hello, Join/Prune, Bootstrap, Assert).

10.2. Automatic Keying

When automatic keying is used, the SA creation is done dynamically using a group key management protocol. The GSPD and PAD tables are

configured by the Administrator. The PAD table provides the link between the IPsec subsystem and the group key management protocol. For automatic keying, the implementation MUST support the multicast extensions described in [RFC5374].

10.2.1. SAD Entries

All PIM routers participate in an authentication scheme that identifies permitted neighbors and achieves peer authentication during SA negotiation, leading to child SAs being established and saved in the SAD.

10.2.2. GSPD Entries

The Administrator must configure the necessary GSPD entries for "send only" directionality. This rule MUST trigger the group key management protocol for a registration exchange. This exchange will set up the outbound SAD entry that encrypts the multicast PIM control message. Considering that this rule is "sender only", no inbound SA is created in the reverse direction.

In addition, the registration exchange will trigger the installation of the GSPD entries corresponding to each legitimate peer router, with direction "receive only". Procedures for achieving the registration exchange are out-of-scope for this document.

A router SHOULD NOT dynamically detect new neighbors as the result of receiving an unauthenticated PIM-SM link-local message or an IPsec packet that fails an SAD lookup. An automated key management protocol SHOULD provide a means of notifying a router of new, legitimate neighbors.

10.2.3. PAD Entries

The PAD will be configured with information to permit identification of legitimate group members and senders (i.e., to control the adjacency). Procedures for doing this are out-of-scope for this document.

11. 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 [RFC4301], 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. This applies to both ESP and AH. The security protocol field is not employed for a multicast SA lookup.

Given that, from the prospective of a receiving router, each peer router is an independent sender and given that the destination address will be the same for all senders, the receiving router MUST use SPI plus destination address plus sender address when performing the SA lookup. In effect, link-local communication is an SSM communication that happens to use an ASM address (which is shared among all the routers).

Given that it is always possible to distinguish a connection using IPsec from a connection not using IPsec, it is recommended that the address ALL_PIM_ROUTERS be used, to maintain consistency with present practice.

Given that the sender address of an incoming packet may be only locally unique (because of the use of link-local addresses), it is necessary for a receiver to use the interface ID tag to determine the associated SA for that sender. Therefore, this document mandates that the interface ID tag, the SPI and the sender address MUST be used in the SA lookup process.

12. Activating the Anti-replay Mechanism

Although link-level messages on a link constitute a multiple-sender, multiple-receiver group, the use of the interface ID tag and sender address for SA lookup essentially resolves the communication into a separate SA for each sender/destination pair, even for the case where only two SAs (with identical SA parameters) are used for the entire administrative region. Therefore, the statement in the AH RFC (section 2.5 of [RFC4302]) that "for a multi-sender SA, the anti-replay features are not available" becomes irrelevant to the 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. The use of the

sender address and the interface ID tag for SA lookup converts the relationship from a multiple-sender group to multiple single-sender associations. This specification RECOMMENDS activation of the anti-replay mechanism only if the SAs are assigned using an automated key management procedure. If manual key management is used, the anti-replay SHOULD NOT be activated.

If an existing router has to restart, in accordance with RFC 4303 [RFC4303], the sequence number counter at the sender MUST be correctly maintained across local reboots, etc., until the key is replaced.

13. Implementing a Security Policy Database per Interface

RFC 4601 suggests that it may be desirable to implement a separate Security Policy Database (SPD) for each router interface. The use of link-local addresses in certain circumstances implies that differentiation of ambiguous speaker addresses requires the use of the interface ID tag in the SA lookup. One way to do this is through the use of multiple SPDs. Alternatively, the interface ID tag may be a specific component of the selector algorithm. This is in conformance with RFC 4301, which explicitly removes the requirement for separate SPDs that was present in RFC 2401 [RFC2401].

14. Extended Sequence Number

In the [RFC4302], 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 are 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 for a small number of PIM routers, 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. In addition, when an ESN is used with a manually-keyed SA, it MUST be saved over a reboot, along with an indication of which sequence numbers have been used.

15. Security Considerations

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

Limitations of manual keys:

The following are some of the known limitations of the usage of manual keys.

- If replay protection cannot be provided, the PIM routers will not be secured against all the attacks that can be performed by replaying PIM packets.
- Manual keys are usually long lived (changing them often is a tedious task). This gives an attacker enough time to discover the keys.
- As the administrator is manually configuring the keys, there is a chance that the configured keys are weak (there are known weak keys for DES/3DES at least).

Impersonation attacks:

The usage of the same key on all the PIM routers connected to a link leaves them all insecure against impersonation attacks if any one of the PIM routers is compromised, malfunctioning, or misconfigured.

Detailed analysis of various vulnerabilities of routing protocols is provided in RFC 4593 [RFC4593]. For further discussion of PIM-SM and multicast security the reader is referred to RFC 5294 [RFC5294], RFC 4609 [RFC4609] and the Security Considerations section of RFC 4601 [RFC4601].

16. IANA Considerations

This document has no actions for IANA.

17. Acknowledgements

The structure and text of this document draw heavily from RFC 4552 [RFC4552]. The authors of this document thank M. Gupta and N. Melam for permisison to do this.

The quality of this document was substiantially improved after SECDIR pre-review by Brian Weis, and after AD review by Adrian Farrel.

18. References

18.1. Normative References

[RFC4601] Fenner, B., Handley, M., Holbrook, H., and I. Kouvelas, "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)", RFC 4601, August 2006.

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

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

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

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.

[RFC4835] Manral, V., "Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)", RFC 4835, April 2007.

[RFC5374] Weis, B., Gross, G., and D. Ignjatic, "Multicast Extensions to the Security Architecture for the Internet Protocol", RFC 5374, November 2008.

18.2. Informative References

[RFC2401] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[RFC4535] Harney, H., Meth, U., Colegrove, A., and G. Gross, "GSAKMP: Group Secure Association Key Management Protocol", RFC 4535, June 2006.

[RFC3547] Baugher, M., Weis, B., Hardjono, T., and H. Harney, "The Group Domain of Interpretation", RFC 3547, July 2003.

[RFC4593] Barbir, A., Murphy, S., and Y. Yang, "Generic Threats to Routing Protocols", RFC 4593, October 2006.

[RFC5294] Savola, P. and J. Lingard, "Host Threats to Protocol Independent Multicast (PIM)", RFC 5294, August 2008.

[RFC4609] Savola, P., Lehtonen, R., and D. Meyer, "Protocol Independent Multicast - Sparse Mode (PIM-SM) Multicast

Routing Security Issues and Enhancements", RFC 4609, October 2006.

[RFC4552] Gupta, M. and N. Melam, "Authentication/Confidentiality for OSPFv3", RFC 4552, June 2006.

[RFC4107] Bellovin, S. and R. Housley, "Guidelines for Cryptographic Key Management", BCP 107, RFC 4107, June 2005.

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://users.encs.concordia.ca/~bill

Salekul Islam
INRS Energie, Materiaux et Telecommunications
800, de La Gauchetiere, suite 800
Montreal, QC H5A 1K6
Canada

Email: Salekul.Islam@emt.inrs.ca
URI: http://users.encs.concordia.ca/~salek_is

Maziar Siami
Concordia University/CIISE
1455 de Maisonneuve Blvd, West
Montreal, QC H3G 1M8
Canada

Email: m_siamis@ciise.concordia.ca