Network Working Group
Internet-Draft
Intended status: Experimental
Expires: September 10, 2012

M. Bhatia
Alcatel-Lucent
D. Zhang
Huawei

March 9, 2012

In-Band Authentication Extension for Protocol Independent Multicast (PIM)
draft-bhatia-zhang-pim-auth-extension-01

Abstract

Existing security mechanisms for the Protocol Independent Multicast - Sparse Mode (PIM-SM) routing protocol mandates to use IPsec to provide message authenticity and integrity. This draft proposes an embedded authentication mechanism to facilitate data origin authentication and integrity verification for PIM packets in the cases where IPsec is not applied.

Requirements Language

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].

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 September 10, 2012.

Table of Contents

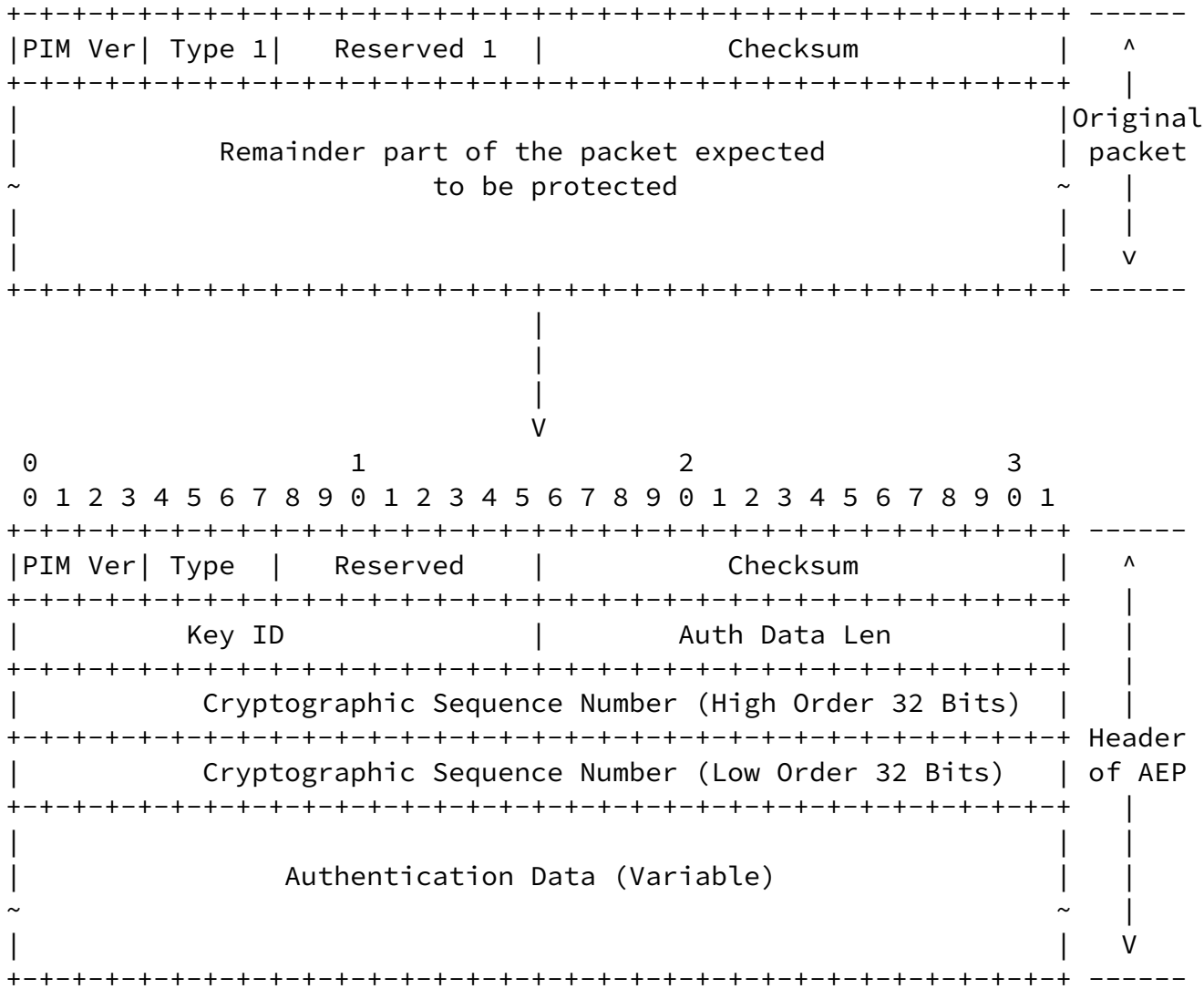
1. Introduction

[RFC5796] describes the methods of using the IP security (IPsec) Encapsulating Security Payload (ESP) [RFC4303] or the Authentication Header (AH) [RFC4302] (which is optional) to protect the authenticity and integrity of the link-local messages of Protocol Independent Multicast - Sparse Mode (PIM-SM)[RFC4601]. [RFC5796] mandates the application of manual key management mechanisms and provide optional support for an automated group key management mechanism. However, the procedures for implementing automated group key management are left undone yet.

It has been clarified in [I-D.bhatia-karp-pim-gap-analysis] that without the support of automated group key management mechanisms, the PIM packets protected by IPsec will be vulnerable to both inter-session and inner-session replay attacks. In addition, the poor scalability of manual keying may cause deployment issues in many typical scenarios. This document proposes a new type of PIM packet, called the Authentication Extension PIM packet (AEP), which is able to facilitate data origin authentication and message integrity verification for PIM packets without the support of IPsec. An AEP actually contains all the essential information of a PIM packet being protected and provides cryptographic methods for the receiver to assess the authenticity and integrity of the packet. In this solution, it is assumed that manual keying is performed while the automatic key management mechanisms are not precluded. Within a packet proposed in this document, a monotonically increasing sequence number is adopted to address the replay attack issues. However, the work of addressing the scalability issues imposed by manual keying is out of scope of this draft.

2. Proposed Solution

Figure 1 illustrates the format of an example packet header.


|PIM Ver| Type 1| Reserved 1 | Checksum |
Original packet
Remainder part of the packet expected to be protected
0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
|PIM Ver| Type | Reserved | Checksum |
Key ID | Auth Data Len |
Cryptographic Sequence Number (High Order 32 Bits)
Cryptographic Sequence Number (Low Order 32 Bits)
Header of AEP
Authentication Data (Variable)

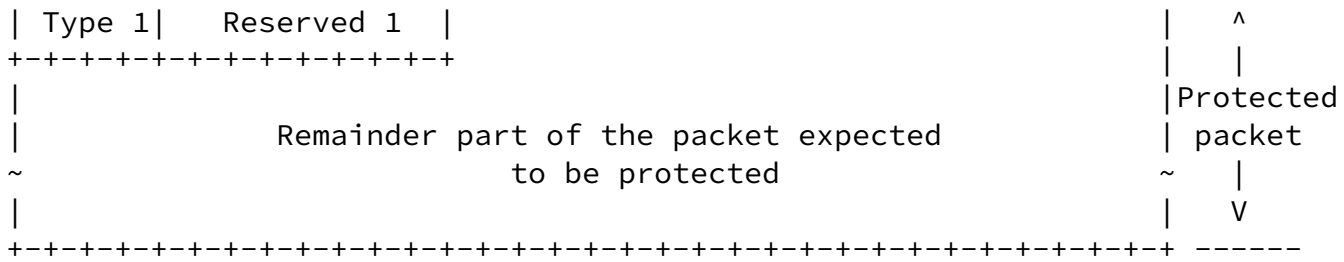


Figure 1. The format of an example AEP

In compliance with [RFC4601], the first four fields of the AEP header is identical to those of the original types of PIM packets. Particularly, the PIM Version number is set to 2. The type number of AEP is 9 in order to distinguish AEP from other types of PIM packets. The Reserved field is set to zero on transmission and ignored upon receipt. The checksum field of the AEP is set to zero, and the checksum calculation and verification are omitted.

Other fields of in the AEP header are described as follows:

Key ID: A 16-bit field that identifies the secret key and the algorithm used to create the authentication data.

Cryptographic Sequence Number: A 64-bit strictly increasing sequence number that is used to guard against replay attacks. The 64-bit sequence number MUST be incremented for every AEP packet sent by a PIM router. Upon reception, the sequence number MUST be greater than the sequence number in the last AEP packet accepted from the PIM router sending the packet. Otherwise, the AEP packet is considered a replayed packet and dropped. PIM routers implementing this specification SHOULD use available mechanisms to preserve the sequence number's strictly increasing property for the deployed life of the PIM router (including cold restarts). Techniques such as sequence number space partitioning and non-volatile storage preservation can be used but are beyond the scope of this specification.

Authentication Data: A field with a variable length. The field carries the digest for the protocol packet and other optional information.

Type 1: This 4-bit field indicate the type of the encapsulated PIM packet.

Reserved 1: This 8-bit field is identical to the Reserved field of the encapsulated PIM packet. Because the Version field and the Checksum field in the header of the encapsulated PIM packet are redundant, they are removed.

3. PIM Security Association

An PIM Security Association (SA) consists of a set of parameters for PIM routers to correctly generate or verify AEP packets. In manual keying, it is the responsibility of network operators to generate and deploy PIM SAs amongst PIM routers appropriately to ensure the routers can exchange PIM signalling messages securely.

The parameters associated with a PIM SA:

- Key Identifier (Key ID) : A 16-bit unsigned integer which is used to uniquely identify an PIM SA within a PIM domain.

- Authentication Algorithm: This parameter is used to indicate the authentication algorithm to be used with the PIM SA. The value of this parameter can be implementer specific. Currently, the

following algorithms SHOULD be supported: HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512.

- Key: The value of this parameter denotes the cryptographic key associated with the key ID. The length of this key is determined by the algorithm specified in the PIM SA.

- Key Start Accept: The time after which a PIM router will accept a packet if it is created with this PIM SA.

- Key Start Generate: The time after which a PIM router will begin using this PIM SA for PIM packet generation.

- Key Stop Generate: The time after which a PIM router will stop using this PIM SA for PIM packet generation.

- Key Stop Accept: The time after which a PIM router will refuse to accept a packet if it is generated with this PIM SA.

4. AEP Packet Processing

4.1. Cryptographic Aspects

In the algorithm description below, the following nomenclature, which is consistent with [FIPS-198], is used:

H is the specific hashing algorithm (e.g. SHA-256).

K is the Authentication Key for the PIM security association.

Ko is the cryptographic key used with the hash algorithm.

B is the block size of H, measured in octets rather than bits.

Note that B is the internal block size, not the hash size.

For SHA-1 and SHA-256: B == 64

For SHA-384 and SHA-512: B == 128

L is the length of the hash, measured in octets rather than bits.

XOR is the exclusive-or operation.

Opad is the hexadecimal value 0x5c repeated B times.

Ipad is the hexadecimal value 0x36 repeated B times.

Apad is a value which is the same length as the hash output or message digest. If the packet is transported upon IPv6, the first 16 octets contain the IPv6 source address followed by the hexadecimal value 0x878FE1F3 repeated (L-16)/4 times. If the packet is transported upon IPv4, the first 4 octets contain the IPv4 source address followed by the hexadecimal value 0x878FE1F3 repeated (L-4)/4 times.

1. Preparation of the Key

   In this application, Ko is always L octets long.

   If the Authentication Key (K) is L octets long, then Ko is equal to K. If the Authentication Key (K) is more than L octets long, then Ko is set to H(K). If the Authentication Key (K) is less than L octets long, then Ko is set to the Authentication Key (K) with zeros appended to the end of the Authentication Key (K) such that Ko is L octets long.

2. First Hash

   First, the AEP packet's Authentication Data field in the AEP header is filled with the value Apad.

   Then, a First-Hash, also known as the inner hash, is computed as follows:

   If the original packet is a Register packet

   First-Hash = H(Ko XOR Ipad || (AEP Packet-Data Part))

   else

   First-Hash = H(Ko XOR Ipad || (AEP Packet))

   The digest length for SHA-1 is 20 octets; for SHA-256, 32 octets; for SHA-384, 48 octets; and for SHA-512, 64 octets.

3. Second Hash

   Then a second hash, also known as the outer hash, is computed as follows:

   Second-Hash = H(Ko XOR Opad || First-Hash)

4. Result

   The resulting Second-Hash becomes the authentication data that is

sent in the AEP header. The length of the authentication data is always identical to the message digest size of the specific hash function H that is being used.

4.2. Outbounding Packet Processing

First of all, a sender needs to find a proper PIM SA and generate a PIM header. The checksum field of the AEP header is set as zero. The length of the Authentication Data field is determined according the algorithm specified in the SA. The sequence number for this SA is increased, and the new value is inserted into the Sequence Number field. The Authentication Data field is set as Apad. After these, the sender appends the encapsulated PIM packet (without the redundant fields) at the end of the AEP header and generates the authentication data as illustrated in Section 4.1. After inserting the calculated authentication data into the Authentication Data field, the sender delivers the packet.

4.3. Inbounding Packet Processing

A router identifies a received PIM packet is an AEP by examining the Type field in PIM packet header. If the cryptographic sequence number of the packet is less than or equal to the last sequence number received from the PIM router, the AEP packet MUST be dropped. If the Checksum fields in the AEP header and in the PIM header of the encapsulated PIM packet are not zero, the AEP packet MUST be dropped.

According to the key ID in the packet header, the receiver tries to find the associated PIM SA. If no valid PIM SA exists for this packet or the key is not in its valid period, the receiver MUST discard the packet. If the appropriate PIM SA for the received packet is found, the receiver starts performing the authentication algorithm dependent processing, using the algorithm specified in the SA.

In the first step, the receiver derives the cryptographic algorithm from the PIM SA and identify the length of the Authentication Data field. Then the receiver fills the Authentication Data field with Apad . After this, the receiver calculate the authentication data for the AEP as described in Section 4.1. The calculated data is compared with the received authentication data in AEP header. If the two do not match, the packet MUST be discarded. In such a case, an error event SHOULD be logged.

5. Security Considerations

5.1. Register Packet Processing

The solution proposed in this draft only intends to secure PIM signaling packets. The efforts of protecting data packets transported among PIM routers are out of scope. Therefore, for a register packet, only the Type field, the B field, and the N field are secured while the Multicast data packet part is not protected by the authentication data.

5.2. New Packet Type Versus Authentication Trailer

Both PIM and OSPFv3 rely on IPsec to secure packet transmission, and they meet similar security issues, such as the vulnerability to the replay attacks and lack of support to priority packets. [I-D.ietf-ospf-auth-trailer-ospfv3] proposes an authentication trailer which is appended at the end of an OSPFv3 packet and provides IPsec independent authentication for the packet. This idea can also be adopted into PIM. However, compared with the OSPFv3 packet header, the PIM header lacks a field to point out the length the PIM packet. The length of the PIM packet is actually indicated by the length of the IP payload and can be variable. This raises a issue. If an authentication trailer is attached at the end of a PIM packet, it will be difficult to locate. This issue can be addressed by extending the PIM headers with an Length field.

5.3. Inter-Session Replay Attack Issue

When a router is rebooted , the sequence number will be re-initialzed. This will cause a problem. When a PIM router received a hello message with a changed GenID and an re-inialized sequence number, it is difficult for the receiver to distinguish this message from a replay attack. The soltuion proposed in this document is subject to this problem. However, the experience in [I-D.ietf-ospf-security-extension-manual-keying] can be used to address this problem. In the solution proposed in [I-D.ietf-ospf-security-extension-manual-keying], there is a reboot counter maintained in non-violate memory which is increased by 1 after every reboot. The count value is set into the first 32 bits of the sequence number. Therefore, even after a restart, the sequence number will still be increased.

6. Acknowledgements

We would like to thank Stig Venaas for his kindly review work and comments on this document.

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.

7.2. Informative References

[I-D.bhatia-karp-pim-gap-analysis]
Bhatia, M., "Analysis of Protocol Independent Multicast Sparse Mode (PIM-SM) Security According to KARP Design Guide", draft-bhatia-karp-pim-gap-analysis-00 (work in progress), April 2011.

[I-D.ietf-ospf-auth-trailer-ospfv3]
Bhatia, M., Manral, V., and A. Lindem, "Supporting Authentication Trailer for OSPFv3", draft-ietf-ospf-auth-trailer-ospfv3-11 (work in progress), November 2011.

[I-D.ietf-ospf-security-extension-manual-keying]
Bhatia, M., Hartman, S., Zhang, D., and A. Lindem, "Security Extension for OSPFv2 when using Manual Key Management", draft-ietf-ospf-security-extension-manual-keying-01 (work in progress), October 2011.

[RFC3973] Adams, A., Nicholas, J., and W. Siadak, "Protocol Independent Multicast - Dense Mode (PIM-DM): Protocol Specification (Revised)", RFC 3973, January 2005.

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

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

[RFC4601] Fenner, B., Handley, M., Holbrook, H., and I. Kouvelas,

"Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)", RFC 4601, August 2006.

[RFC5796] Atwood, W., Islam, S., and M. Siami, "Authentication and Confidentiality in Protocol Independent Multicast Sparse Mode (PIM-SM) Link-Local Messages", RFC 5796, March 2010.

Authors' Addresses

Manav Bhatia
Alcatel-Lucent

Email: manav.bhatia@alcatel-lucent.com

Dacheng Zhang
Huawei

Email: zhangdacheng@huawei.com