

Network Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: June 19, 2014

M. Bhatia  
Alcatel-Lucent  
M. Jethanandani  
Ciena Corporation  
D. Zhang  
Huawei Technologies Co. LTD.  
December 16, 2013

Analysis of Protocol Independent Multicast Sparse Mode (PIM-SM) Security  
According to KARP Design Guide  
[draft-bhatia-karp-pim-gap-analysis-01](#)

## Abstract

This document analyzes the Protocol Independent Multicast Sparse Mode (PIM-SM) according to the guidelines set forth in the KARP Design Guide.

## 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 June 19, 2014.

## Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in [Section 4.e](#) of

Internet-Draft

PIM-SM Gap Analysis

December 2013

the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## 1. Introduction

This document performs the initial analysis of the current state of Protocol Independent Multicast Sparse Mode (PIM-SM) [[RFC4601](#)] according to the requirements of KARP Design Guidelines [[RFC6518](#)]

The base PIM-SM specification [[RFC4601](#)] introduces the use non-cryptographic authentication approaches to protect PIM-SM packets and recommends the use of transport mode of IPsec AH [[RFC4302](#)] to protect PIM-SM unicast and multicast packets. The memo assumes that the SAs are manually deployed.

Authentication and Confidentiality in PIM-SM Link-Local Messages [[RFC5796](#)] proposes the mechanisms to authenticate the PIM-SM multicast messages using the IP security (IPsec) Encapsulating Security Payload (ESP) [[RFC4303](#)] or (optionally) the IP Authentication Header (AH) [[RFC4302](#)] .

The document specifies manual key management as mandatory to implement and provides the necessary structure for an automated key management protocol that the PIM routers may use.

However, some gaps remain between the current state and the requirements for manually keyed routing security expressed in the [[RFC6862](#)] document. This document explores these gaps and proposes directions for addressing the gaps.

## 2. Current State

Unlike OSPFv2 [[RFC2328](#)], PIM-SM does not propose any in-band security solution. Instead, IPsec is used to protect both unicast and multicast control packets.

Authentication and Confidentiality in PIM-SM Link-Local Messages [[RFC5796](#)] describes how IPsec can be used to secure and authenticate PIM-SM protocol packets. It mandates the use of manual keying and optionally provides support for an automated group key management mechanism. However, it leaves the procedures for implementing automated group key management to other documents and does not discuss how this can be done.

The mechanism proposed in Authentication and Confidentiality in PIM-SM Link-Local Messages [[RFC5796](#)] supports packet level integrity protection using a wide variety of cryptographic algorithms. In addition, the Security Parameter Index (SPI) [[RFC4301](#)] provides an

identifier for the security association. Along with other IPsec facilities, SPI provides a mechanism for moving from one key to another, meeting the key rollover requirements. Because the algorithm can be changed as part of rekeying, algorithm agility is provided.

Authentication and Confidentiality in PIM-SM Link-Local Messages [[RFC5796](#)] uses manually configured keys, rather than some automated key management protocol, since no suitable key management mechanism was available at this time. This is because PIM-SM adjacencies are formed on a one-to-many basis and most key management mechanisms are designed for a one-to-one communication model. Since authentication and confidentiality in PIM-SM Link-Local Messages [[RFC5796](#)] uses manual keying it clearly states that it provides no protection against both inter-session and intra-session replay attacks. This can be exploited in various ways. For instance, by replaying the Join message sent by a legitimate requester, an attacker can direct multicast traffic to be delivered to links where it is not required. Similarly, replaying a Prune Message can deprive the receivers from that multicast traffic.

### [3.](#) Deployment Issues Imposed by IPsec and Manual Keying

Since multiple PIM-SM routers can exist on a single link, it would be worth noting that setting up IPsec Security Associations (SAs) manually can be a very tedious process. The routers might not even support IPsec, rendering automatic key negotiation either impractical (in those platforms where an extra license has to be obtained for using IPsec) or infeasible (in those platforms where IPsec support is not available at all).

PIM-SM [[RFC4601](#)] requires all PIM-SM routers to configure an IPsec Security Association (SA) when sending PIM Register packets to each Rendezvous Point (RP). This can become highly unscalable as the number of RPs increase or in case of Anycast-RP [[RFC4610](#)] deployment where each PIM-SM router close to the source will need to establish

IPsec tunnels to all PIM-SM routers in the Anycast-RP set.

Similarly, the Security Policy Database at each Rendezvous Point should be configured to choose an SA to use when sending Register-Stop messages. Because Register-Stop messages are unicast to the destination DR, a different SA and a potentially unique SPI are required for each DR.

In order to simplify the management problem, PIM-SM [[RFC4601](#)] suggests using the same authentication algorithm and authentication parameters, regardless of the sending RP and regardless of the destination DR. While this alleviates the management problem by some

extent it still requires a unique SA on each DR which can result in a significant scaling issue as the size of the PIM-SM network grows.

#### [4.](#) Gap Analysis

In PIM-SM, multiple types of PIM messages (Hello, Join/Prune, Bootstrap, Assert) are delivered with multicast. As it exists today, PIM-SM supports only manual key management. When using manual keying, the replay protection mechanism (replay protection window) of IPsec will be switched off. That is why IPsec cannot protect against any replay protection in this case. In addition, the PIM messages do not have any replay protection mechanism, e.g. nonce or sequence numbers. Therefore, PIM-SM is subject to both inter- and intra-connection replay attacks. From the aspect of meeting the requirements for replay protection, a significant gap exists between the optimal state and where PIM-SM is today.

In order to encourage deployment of PIM-SM security, an authentication option is required that does not have the deployment challenges of IPsec. We therefore need an alternate authentication mechanism to IPsec as suggested by the first phase of the KARP design guide, where the guide suggests securing the routing protocols using manual keying.

The new mechanism should work for both the unicast and multicast PIM-SM routing exchanges. It should also provide both inter-session and intra-session replay protection that has been spelled out in the [[RFC6862](#)] document.

## [5.](#) Security Considerations

TBD

## [6.](#) IANA Considerations

This document places no new request to IANA

## [7.](#) Acknowledgements

We would like to thank Stig Venaas and Bill Atwood for reviewing and providing feedback on this draft.

## [8.](#) References

### [8.1.](#) Normative References

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

Bhatia, et al.

Expires June 19, 2014

[Page 4]

---

Internet-Draft

PIM-SM Gap Analysis

December 2013

- [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.

### [8.2.](#) Informative References

- [RFC2328] Moy, J., "OSPF Version 2", STD 54, [RFC 2328](#), April 1998.
- [RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", [RFC 4301](#), December 2005.
- [RFC4302] Kent, S., "IP Authentication Header", [RFC 4302](#), December 2005.
- [RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", [RFC 4303](#), December 2005.
- [RFC4306] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", [RFC](#)

[4306](#), December 2005.

- [RFC4610] Farinacci, D. and Y. Cai, "Anycast-RP Using Protocol Independent Multicast (PIM)", [RFC 4610](#), August 2006.
- [RFC6518] Lebovitz, G. and M. Bhatia, "Keying and Authentication for Routing Protocols (KARP) Design Guidelines", [RFC 6518](#), February 2012.
- [RFC6862] Lebovitz, G., Bhatia, M., and B. Weis, "Keying and Authentication for Routing Protocols (KARP) Overview, Threats, and Requirements", [RFC 6862](#), March 2013.

#### Authors' Addresses

Manav Bhatia  
Alcatel-Lucent  
India

Email: [manav.bhatia@alcatel-lucent.com](mailto:manav.bhatia@alcatel-lucent.com)

Bhatia, et al.

Expires June 19, 2014

[Page 5]

---

Internet-Draft

PIM-SM Gap Analysis

December 2013

Mahesh Jethanandani  
Ciena Corporation  
3939 North 1st Street  
San Jose, CA 95134  
USA

Phone: +1 (408) 904-2160  
Email: [mjethanandani@gmail.com](mailto:mjethanandani@gmail.com)

Dacheng Zhang  
Huawei Technologies Co. LTD.  
Beijing  
China

Email: zhangdacheng@huawei.com