Network Working Group
Internet Draft
Intended status: Proposed Standard
Expiration Date: June 2009

David J. Smith
John Mullooly
Cisco Systems, Inc.

William Jaeger
AT&T

Tom Scholl
AT&T Labs

December 7, 2008

Requirements for Label Edge Router Forwarding of IPv4 Option Packets

draft-ietf-mpls-ip-options-00.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

Abstract

This document imposes a new requirement on Label Edge Routers (LER) specifying that when determining whether to MPLS encapsulate an IP packet, the determination is made independent of any IP options that may be carried in the IP packet header. Lack of a formal standard has resulted in different LER forwarding behaviors for IP packets with header options despite being associated with a prefix-based Forwarding Equivalence Class (FEC). IP option packets that belong to a prefix-based FEC but fail to be MPLS encapsulated simply due to their header options present a security risk against the MPLS infrastructure. Further, LERs that are unable to MPLS encapsulate IP packets with header options cannot operate in certain MPLS environments. This new requirement will reduce the risk of IP options-based security attacks against LSRs as well as assist LER operation across MPLS networks which minimize the IP routing information carried by LSRs.

Table of Contents

1 Specification of Requirements 2
2 Motivation 3
3 Introduction 3
4 Ingress Label Edge Router Requirement 4
5 Security Considerations 5
5.1 IP Option Packets that Bypass MPLS Encapsulation ... 5
5.2 Router Alert Label Imposition 7
6 IANA Considerations 7
7 Conclusion 7
8 Acknowledgements 8
9 Normative References 8
10 Informational References 8
11 Authors' Addresses 9
12 Full Copyright Statement 10
13 Intellectual Property 10

1. Specification of Requirements

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 [RFC2119].

2. Motivation

This document is motivated by the need to formalize MPLS encapsulation processing of IPv4 packets with header options in order to mitigate the existing risks of IP options-based security attacks against MPLS infrastructures. We believe that this document adds details that have not been fully addressed in [RFC3031] and [RFC3032], and that the methods presented in this document update [RFC3031] as well as complement [RFC3270], [RFC3443] and [RFC4950].

3. Introduction

The IP packet header provides for various IP options as originally specified in [RFC791]. IP header options are used to enable control functions within the IP data forwarding plane that are required in some specific situations but not necessary for most common IP communications. Typical IP header options include provisions for timestamps, security, and special routing. Example IP header options & applications include but are not limited to:

- o Strict & Loose Source Route Options: Used to IP route the IP packet based on information supplied by the source.
- o Record Route Option: Used to trace the route an IP packet takes.
- o Router Alert Option: Indicates to downstream IP routers to examine these IP packets more closely.

The list of current IP header options can be accessed at [IANA].

IP packets may or may not use IP header options (they are optional) but IP header option handling mechanisms must be implemented by all IP protocol stacks (hosts and routers). Each IP header option has distinct header fields and lengths. IP options extend the IP packet header length beyond the minimum of 20 octets. As a result, IP packets received with header options are typically handled as exceptions and in a less efficient manner due to their variable length and complex processing requirements. Many router implementations, for example, punt such IP option packets from the hardware forwarding (fast) path into the software forwarding (slow) path.

Multi-Protocol Label Switching (MPLS) [RFC3031] is a technology in which packets associated with a prefix-based Forwarding Equivalence Class (FEC) are encapsulated with a label stack and then switched along a label switched path (LSP) by a sequence of label switch routers (LSRs). These intermediate LSRs do not generally perform any processing of the IP header as packets are forwarded. (There are some exceptions to this rule, such as ICMP processing and LSP ping, as described in [RFC3032] and [RFC4379], respectively.) Many MPLS deployments rely on LSRs to provide layer 3 transparency much like

ATM switches are transparent at layer 2. Such deployments often minimize the IP routing information (e.g., no BGP transit routes) carried by LSRs since not necessary for MPLS forwarding of transit packets.

Even though MPLS encapsulation seems to offer a viable solution to provide layer 3 transparency, there is currently no formal standard for MPLS encapsulation of IP packets with header options that below to a prefix-based FEC. Lack of a formal standard has resulted in inconsistent forwarding behaviors by ingress LERs. When MPLS encapsulated by an ingress LER, for example, the IP header including option fields of transit packets are transparent to downstream LSRs given MPLS forwarding. Conversely, when IP routed by an ingress LER, downstream LSRs must apply IP forwarding rules which may expose the LSRs to IP security attacks and for which they (the LSRs) may have insufficient IP routing information.

IP option packets that belong to a prefix-based FEC but fail to be MPLS encapsulated simply due to their header options present a security risk against the MPLS infrastructure. Further, LERs that are unable to MPLS encapsulate IP packets with header options cannot operate as an LER in certain MPLS environments. This new requirement will reduce the risk of IP options-based security attacks against LSRs as well as assist LER operation across MPLS networks which minimize the IP routing information (e.g., no BGP transit routes) carried by LSRs.

4. Ingress Label Edge Router Requirement

An ingress LER MUST implement the following policy:

- o When determining whether to push an MPLS label stack onto an IP packet, the determination is made without considering any IP options that may be carried in the IP packet header. Further, the label values that appear in the label stack are determined without considering any such IP options.

This policy MAY be configurable on an ingress LER, however, it SHOULD be enabled by default. When processing of signaling messages or data packets with more specific forwarding rules is enabled, this policy SHOULD NOT alter the specific processing rules. This applies to, but is not limited to, RSVP as per [RFC2205] as well as other FEC elements defined by future specifications. Further, how an ingress LER processes the IP header options of packets before MPLS encapsulation is out of scope since the IP packets are received as they enter the MPLS domain.

Implementation of the above policy prevents IP packets that belong to a prefix-based FEC from bypassing MPLS encapsulation due to header options. The policy also prevents specific option types such as Router Alert (option value 148), for example, from forcing MPLS imposition of the MPLS Router Alert Label (label value 1) at ingress LERs. Without this policy, the MPLS infrastructure is exposed to security attacks using legitimate IP packets crafted with header options. Further, LERs that are unable to MPLS encapsulate IP packets with header options cannot operate as an LER in certain MPLS environments as described above in Section 3.

5. Security Considerations

There are two potential categories of attacks using crafted IP option packets that threaten existing MPLS infrastructures. Both are described below. To mitigate the risk of these specific attacks, the ingress LER policy specified above is required.

5.1. IP Option Packets that Bypass MPLS Encapsulation

Given that a router's exception handling process (i.e., CPU, processor line-card bandwidth, etc.) used for IP header option processing is often shared with IP control and management protocol router resources, a flood of IP packets with header options may adversely affect a router's control and management protocols, thereby, triggering a denial-of-service (DoS) condition. Note, IP packets with header options may be valid transit IP packets with legitimate sources and destinations. Hence, a DoS-like condition may be triggered on downstream transit IP routers that lack protection mechanisms even in the case of legitimate IP option packets.

IP option packets that below to a prefix-based FEC yet bypass MPLS encapsulation at a ingress LER may be inadvertently IP routed downstream across the MPLS core network (not label switched). This allows an external attacker the opportunity to maliciously craft seemingly legitimate IP packets with specific IP header options in order to intentionally bypass MPLS encapsulation at the MPLS edge (i.e., ingress LER) and trigger a DoS condition on downstream LSRs. Some of the specific types of IP option-based security attacks that may be leveraged against MPLS networks include:

- o Crafted IP option packets that below to a prefix-based FEC yet bypass MPLS encapsulation at a ingress LER may allow an attacker to DoS downstream LSRs by saturating their software forwarding paths. By targeting a LSR's exception path, control and management protocols may be adversely affected and, thereby, a LSR's availability. This assumes, of course, that downstream

LSRs lack protection mechanisms.

- o Crafted IP option packets that below to a prefix-based FEC yet bypass MPLS encapsulation at a ingress LER may allow for IP TTL expiry-based DoS attacks against downstream LSRs. MPLS enables IP core hiding whereby transit IP traffic flows see the MPLS network as a single router hop [RFC3443]. However, MPLS core hiding does not apply to packets that bypass MPLS encapsulation and, therefore, IP option packets may be crafted to expire on downstream LSRs which may trigger a DoS condition. Bypassing MPLS core hiding is an additional security consideration since it exposes the network topology.
- o Crafted IP option packets that below to a prefix-based FEC yet bypass MPLS encapsulation at a ingress LER may allow for DoS attacks against downstream LSRs that do not carry the IP routing information required to forward transit IP traffic. Lack of such IP routing information may prevent legitimate IP option packets from transiting the MPLS network and, further, may trigger generation of ICMP destination unreachable messages which could lead to a DoS condition. This assumes, of course, that downstream LSRs lack protection mechanisms and do not carry the IP routing information required to forward transit traffic.
- o Crafted IP option packets that below to a prefix-based FEC yet bypass MPLS encapsulation at a ingress LER may allow an attacker to bypass LSP Diff-Serv tunnels [RFC3270] and any associated MPLS CoS field [MPLSCOS] marking policies at ingress LERs and, thereby, adversely affect (i.e., DoS) high-priority traffic classes within the MPLS core. Further, this could also lead to theft of high-priority services by unauthorized parties. This assumes, of course, that the [RFC3270] Pipe model is deployed within the MPLS core.
- o Crafted IP strict and loose source route option packets that below to a prefix-based FEC yet bypass MPLS encapsulation at a ingress LER may allow an attacker to specify explicit IP forwarding path(s) across an MPLS network and, thereby, target specific LSRs with any of the DoS attacks outlined above. This assumes, of course, that the MPLS network is enabled to process IP strict and loose source route options.
- o Crafted RSVP packets that below to a prefix-based FEC yet bypass MPLS encapsulation at a ingress LER may allow an attacker to build RSVP soft-states [RFC2205] on downstream LSRs which could lead to theft of service by unauthorized parties or to a DoS condition caused by locking up LSR resources. This assumes, of course, that the MPLS network is enabled to process RSVP packets.

The security attacks outlined above specifically apply to IP option packets that below to a prefix-based FEC yet bypass ingress LER label stack imposition. Additionally, these attacks only apply to IP option packets forwarded using the global routing table (i.e., IPv4

address family) of a ingress LER. IP option packets associated with a BGP/MPLS IP VPN service are always MPLS encapsulated by the ingress LER per [RFC4364] given that packet forwarding uses a Virtual Forwarding/Routing (VRF) instance. Therefore, BGP/MPLS IP VPN services are not subject to the threats outlined above [RFC4381]. Further, IPv6 [RFC2460] makes use of extension headers not header options and is therefore outside the scope of this document. A separate security threat that does apply to both BGP/MPLS IP VPNs and the IPv4 address family makes use of the Router Alert Label. This is described directly below.

5.2. Router Alert Label Imposition

[RFC3032] defines a "Router Alert Label" (label value of 1) which is analogous to the "Router Alert" IP header option (option value of 148). The MPLS Router Alert Label (when exposed and processed only) indicates to downstream LSRs to examine these MPLS packets more closely. MPLS packets with the MPLS Router Alert Label are also handled as an exception by LSRs and, again, in a less efficient manner. At the time of this writing, the only legitimate use of the Router Alert Label is for LSP ping/trace [RFC4379]. Since there is also no formal standard for Router Alert Label imposition at ingress LERs:

- Crafted IP packets with specific IP header options (e.g., Router Alert) and that below to a prefix-based FEC may allow an attacker to force MPLS imposition of the Router Alert Label at ingress LERs and, thereby, trigger a DoS condition on downstream LSRs. This assumes, of course, that downstream LSRs lack protection mechanisms.

6. IANA Considerations

This document has no actions for IANA.

7. Conclusion

This document imposes a new requirement on ingress LERs in order to reduce the risk of IP options-based security attacks against LSRs as well as to assist LER operation across MPLS networks which minimize the IP routing information carried by LSRs.

8. Acknowledgements

The authors would like to thank Adrian Cepleanu, Bruce Davie, Rick Huber, Chris Metz, Pradosh Mohapatra, Ashok Narayanan, Carlos Pignataro, Eric Rosen, Mark Szczesniak and Yung Yu for their valuable comments and suggestions.

9. Normative References

[RFC791] Postel, J., "Internet Protocol Specification," RFC791, September 1981.

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

[RFC3031] Rosen, E., Viswanathan, A., and Callon, R., "MPLS Label Switching Architecture," RFC3031, January 2001.

[RFC3032] Rosen, E., Tappan, D., Fedorkow, G., Rekhter, Y., Farinacci, D., Li, T., and Conta, A., "MPLS Label Stack Encoding," RFC3032, January 2001.

10. Informational References

[RFC2205] Braden, R., Zhang, L., Berson, S., Herzog, S., Jamin, S., "Resource ReSerVation Protocol -- Version 1 Functional Specification," RFC2205, September 1997.

[RFC2460] Deering, S., Hinden, R. "Internet Protocol, Version 6 Specification," RFC2460, December 1998.

[RFC3209] Awduche, D., L. Berger, D. Gan, T. Li, V. Srinivasan, G. Swallow, "RSVP-TE: Extensions to RSVP for LSP Tunnels," RFC3209, December 2001.

[RFC3270] Le Faucheur, F., Wu, L., Davie, B., Davari, S., Vaananen, P., Krishnan, R., Cheval, P., Heinanen, J., "Multi-Protocol Label Switching Support of Differentiated Services," RFC3270, May 2002.

[RFC3443] Agarwal, P., Akyol, B., "Time To Live (TTL) Processing in Multi-Protocol Label Switching (MPLS) Networks," RFC3443, January 2003.

[RFC4364] Rosen, E. and Y. Rekhter, "BGP/MPLS IP Virtual Private Networks (VPNs)," RFC4364, February 2006.

[RFC4379] "Kompella, K., Swallow, G., "Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures," RFC4379, February 2006.

[RFC4381] Behringer, M., "Analysis of the Security of BGP/MPLS IP Virtual Private Networks (VPNs)," RFC4381, February 2006.

[RFC4950] Bonica, R., Gan, D., Tappan, D., and Pignataro, C., "ICMP Extensions for Multiprotocol Label Switching," RFC4950, August 2007.

[IANA] "IP Option Numbers," IANA, February 15, 2007, <www.iana.org/assignments/ip-parameters>.

[MPLSCOS] Andersson, L., "EXP Field renamed to Traffic Class Field," IETF draft-ietf-mpls-cosfield-def-07.txt, November 17, 2008.

11. Authors' Addresses

William Jaeger
AT&T
200 S. Laurel Avenue
Middletown, NJ 07748
Email: wjaeger@att.com

John Mullooly
Cisco Systems, Inc.
111 Wood Avenue
Iselin, NJ 08830
E-mail: jmullool@cisco.com

Tom Scholl
AT&T Labs
200 S. Laurel Avenue
Middletown, NJ 07748
Email: ts3127@att.com

David J. Smith
Cisco Systems, Inc.
111 Wood Avenue
Iselin, NJ 08830
E-mail: djsmith@cisco.com

12. Full Copyright Statement

Copyright (C) The IETF Trust (2008).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

13. Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.