Network Working Group   David J. Smith
Internet Draft   John Mullooly
Intended status: Proposed Standard   Cisco Systems, Inc.
Expiration Date: April 2009

                                              William Jaeger
                                                         AT&T

                                                   Tom Scholl
                                                    AT&T Labs

                                              October 6, 2008

      Requirements for Label Edge Router Forwarding of IPv4 Option Packets

            draft-dasmith-mpls-ip-options-01.txt

Status of this Memo

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
   may result in a different forwarding behavior for different IP

Internet Draft   draft-dasmith-mpls-ip-options-01.txt   October 2008

   packets associated with the same prefix-based Forwarding Equivalence
   Class (FEC). While an IP packet with either a specific option type
   or no header option may follow the MPLS label switched path (LSP)
   associated with a prefix-based FEC, an IP packet with a different
   option type but associated with the same prefix-based FEC may bypass
   MPLS encapsulation and instead be IP routed downstream. IP option
   packets that fail to be MPLS encapsulated simply due to their header
   options present a security risk against the MPLS infrastructure.

Table of Contents

[1](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](RFC2119)].

Internet Draft   draft-dasmith-mpls-ip-options-01.txt   October 2008

[2](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](RFC3031)] and
   [[RFC3032](RFC3032)], and that the methods presented in this document update
   [[RFC3031](RFC3031)] as well as complement [[RFC3443](RFC3443)] and [[RFC4950](RFC4950)].

[3](3). Introduction

   The IP packet header provides for various IP options as originally
   specified in [[RFC791](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 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 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, as described in
[RFC3032].) Many MPLS deployments rely on LSRs to provide layer 3
transparency much like ATM switches are transparent at layer 2.

Even though MPLS encapsulation seems to offer a viable solution to

---

protect downstream LSRs from being adversely impacted by customer
packets with IP header options, there is currently no formal standard
for encapsulation of IP packets with header options in MPLS networks.
When MPLS encapsulated, IP option packets are processed by downstream
LSRs as native MPLS packets within their forwarding paths. In this
way, the IP header options are effectively ignored by downstream LSRs
when encapsulated with a MPLS label stack. However, for many LER
implementations not all IP packets with header options are MPLS
encapsulated by the ingress LER.

Lack of a formal standard has resulted in inconsistent forwarding
behaviors by ingress LERs. Namely, IP packets with different types
of IP header options are handled differently by an ingress LER
despite being associated with the same prefix-based FEC as defined in
Section 4.1.1 of [RFC3031]. For instance, some IP header options may
fail to be MPLS encapsulated, and are instead IP routed downstream on
a per-hop basis by downstream LSRs within the MPLS core. The
different forwarding behaviors not only vary across IP option types
but also across ingress LER implementations given no formal standard
for IP header option processing in MPLS networks. 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
minimize the IP routing information carried by LSRs.

4. Ingress Label Edge Router Requirement

An ingress LER MUST implement the following policy, and the policy
MUST be enabled by default:

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.

     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]. Further, how an ingress LER processes IP
     header options before MPLS encapsulation is out of scope as it is not
     relevant to MPLS.

     Implementation of the above policy prevents IP packets from failing
     to be MPLS encapsulated due to header options. The policy also
     prevents specific option types such as Router Alert (value 148), for
     example, from forcing MPLS imposition of the MPLS Router Alert Label
     (value 1) at ingress LERs. Without this policy, the MPLS

Smith, et al.   [Page 4]

     infrastructure is exposed to security attacks using legitimate IP
     packets crafted with header options.

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 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 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 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
     customers 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

Smith, et al.   [Page 5]

     consideration since it exposes the network topology.
   o Crafted IP option packets that 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 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
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 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 bypass ingress LER label stack imposition.
Additionally, these attacks 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 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 an 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" (value of 1) which is
analogous to the "Router Alert" IP header option. 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:
    o Crafted IP packets with specific IP header options (e.g., Router
       Alert) 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 that helps to
    mitigate the risk of crafted security attacks using IP option packets
    against MPLS infrastructures. The security threats were described
    and exist as a result of no formal ingress LER specification for MPLS
    encapsulation of IP packets with header options. Adoption of this
    requirement will also eliminate the variability among ingress LER
    implementations.

8. Acknowledgements

    The authors would like to thank Adrian Cepleanu, Bruce Davie, Rick
    Huber, 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.

   [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.

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

   [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 CoS Field," IETF
draft-ietf-mpls-cosfield-def-02.txt, June 11, 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).

13. Intellectual Property

ipr@ietf.org.