       The Generalized TTL Security Mechanism (GTSM) for Label Distribution
                                Protocol (LDP)
                        draft-ietf-mpls-ldp-gtsm-09

Abstract

   The Generalized TTL Security Mechanism (GTSM) describes a generalized
   use of a packet's Time to Live (TTL) (IPv4) or Hop Limit (IPv6) to
   verify that the packet was sourced by a node on a connected link,
   thereby protecting the router's IP control-plane from CPU utilization
   based attacks. This technique improves security and is used by many
   protocols. This document defines the GTSM use for the Label
   Distribution Protocol (LDP).

   This specification uses a bit reserved in RFC 5036 and therefore
   updates RFC 5036.

Table of Contents

1. Introduction

   LDP [RFC5036] specifies two peer discovery mechanisms, a Basic one
   and an Extended one, both using UDP transport. The Basic Discovery
   mechanism is used to discover LDP peers that are directly connected
   at the link level, whereas the Extended Discovery mechanism is used
   to locate Label Switching Router (LSR) neighbors that are not
   directly connected at the link level. Once discovered, the LSR
   neighbors can establish the LDP peering session, using the TCP
   transport connection.

   The Generalized TTL Security Mechanism (GTSM) [RFC5082] is a
   mechanism based on IPv4 Time To Live (TTL) or (IPv6) Hop Limit value
   verification so as to provide a simple and reasonably robust defense
   from infrastructure attacks using forged protocol packets from
   outside the network. GTSM can be applied to any protocol peering
   session that is established between routers that are adjacent.
   Therefore, GTSM can protect an LDP protocol peering session
   established using Basic Discovery.

   This document specifies LDP enhancements to accommodate GTSM. In
   particular, this document specifies the enhancements in the following
   areas:

   1. Common Hello Parameter TLV of LDP Link Hello message

   2. Sending and Receiving procedures for LDP Link Hello message

   3. Sending and Receiving procedures for LDP Initilization message

   GTSM specifies that "it SHOULD NOT be enabled by default in order to
   remain backward-compatible with the unmodified protocol" (see Section
   3 of [RFC5082]). This document specifies a "built-in dynamic GTSM
   capability negotiation" for LDP to suggest the use of GTSM. GTSM
   will be used as specified in this document provided both peers on an
   LDP session can detect each others' support for GTSM procedures and

agree to use it. That is, the desire to use GTSM (i.e., its
negotiation mechanics) is enabled by default without any
configuration.

This specification uses a bit reserved in Section 3.5.2 of [RFC5036]
and therefore updates [RFC5036].

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].

1.2. Scope

This document defines procedures for LDP using IPv4 routing, but not
for LDP using IPv6 routing, since the latter has GTSM built into the
protocol definition [I-D.ietf-mpls-ldp-ipv6].

Additionally, the GTSM for LDP specified in this document applies
only to single-hop LDP peering sessions, and not to multi-hop LDP
peering sessions, in line with Section 5.5 of [RFC5082].
Consequently, any LDP method or feature (such as LDP IGP
Synchronization [RFC5443], or LDP Session Protection [LDP-SPROT])
that relies on multi-hop LDP peering sessions would not work with
GTSM and will require (statically or dynamically) disabling the GTSM
capability. See Section 3.

2. GTSM Procedures for LDP

2.1. GTSM Flag in Common Hello Parameter TLV

A new flag in Common Hello Parameter TLV, named G flag (for GTSM), is
defined by this document in a previously reserved bit. An LSR
indicates that it is capable of applying GTSM procedures, as defined
in this document, to the subsequent LDP peering session, by setting
the GTSM flag to 1. The Common Hello Parameters TLV, defined in
Section 3.5.2 of [RFC5036], is updated as shown in Figure 1.

```
    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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |0|0| Common Hello Parms(0x0400)|       Length                  |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |      Hold Time                |T|R|G|    Reserved              |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

   T, Targeted Hello
      As specified in [RFC5036].

   R, Request Send Targeted Hellos
      As specified in [RFC5036].

   G, GTSM
      A value of 1 specifies that this LSR supports GTSM procedures,
      where a value of 0 specifies that this LSR does not support GTSM.

   Reserved
      This field is reserved. It MUST be set to zero on transmission
      and ignored on receipt.

Figure 1: GTSM Flag in Common Hello Parameter TLV

The G flag is meaningful only if the T flag is set to 0 (which must
be the case for Basic Discovery), otherwise, the value of G flag is
ignored on receipt.

Any LSR not supporting GTSM for LDP as defined in this document
(i.e., an LSR that does not recognize the G flag), would continue to
ignore the G flag, independent of T and R flags' value, as per
Section 3.5.2 of [RFC5036]. Similarly, an LSR that does recognize
the G flag but that does not support GTSM (either because it is not
implemented, or because it is so configured), would not set the G
flag (i.e., G=0) when sending LDP Link hellos and would effectively
ignore the G flag when receiving LDP Link hello messages.

2.2. GTSM Sending and Receiving Procedures for LDP Link Hello

Firstly, LSRs using LDP Basic Discovery [RFC5036] send LDP Hello
messages to link-level multicast address (224.0.0.2 or "all
routers"). Such messages are never forwarded beyond one hop and are
RECOMMENDED to have their IP TTL or Hop Count = 1.

Unless configured otherwise, an LSR that supports GTSM procedures
MUST set the G flag (for GTSM) to 1 in Common Hello Parameter TLV in
the LDP Link Hello message [RFC5036].

If an LSR that supports GTSM and is configured to use it recognizes
the presence of G flag (in Common Hello Parameter TLV) with the value
=1 in the received LDP Link Hello message, then it MUST enforce GTSM
for LDP in the subsequent TCP/LDP peering session with the neighbor
that sent the Hello message, as specified in Section 2.3 of this
document.

If an LSR does not recognize the presence of G flag (in Common Hello
Parameter TLV of Link Hello message), or recognizes the presence of G
flag with the value = 0, then the LSR MUST NOT enforce GTSM for LDP
in the subsequent TCP/LDP peering session with the neighbor that sent
the Hello message. This ensures backward compatibility as well as
automatic GTSM de-activation.

2.3. GTSM Sending and Receiving Procedures for LDP Initialization

If an LSR that has sent and received LDP Link Hello with G flag = 1
from the directly-connected neighbor, then the LSR MUST enforce GTSM
procedures, as defined in Section 3 of [RFC5082], in the forthcoming
TCP Transport Connection with that neighbor. This means that the LSR
MUST check for the incoming unicast packets' TTL or Hop Count to be
255 for the particular LDP/TCP peering session and decide the further
processing as per the [RFC5082].

If an LSR that has sent LDP Link Hello with G flag = 1, but received
LDP Link Hello with G flag = 0 from the directly-connected neighbor,
then the LSR MUST NOT enforce GTSM procedures, as defined in Section
3 of [RFC5082], in the forthcoming TCP Transport Connection with that
neighbor.

3. LDP Peering Scenarios and GTSM Considerations

   This section discusses GTSM considerations arising from the LDP
   peering scenarios used, including single-hop versus multi-hop LDP
   neighbors, as well as the use of LDP basic discovery versus extended
   discovery.

   The reason that the GTSM capability negotiation is enabled for Basic
   Discovery by default (i.e., G=1), but not for Extended Discovery is
   that the usage of Basic Discovery typically relates to a single-hop
   LDP peering session, whereas the usage of Extended Discovery
   typically relates to a multi-hop LDP peering session. GTSM
   protection for multi-hop LDP sessions is outside the scope of this
   specification (see Section 1.2). However, it is worth clarifying the
   following exceptions that may occur with Basic or Extended Discovery
   usage:

   a. Two adjacent LSRs (i.e., back-to-back PE routers) forming a
       single-hop LDP peering session after doing an Extended Discovery
       (e.g., for Pseudowire signaling)

   b. Two adjacent LSRs forming a multi-hop LDP peering session after
       doing a Basic Discovery, due to the way IP routing is setup
       between them (either temporarily or permanently)

c. Two adjacent LSRs (i.e. back-to-back PE routers) forming a
       single-hop LDP peering session after doing both Basic and
       Extended Discovery.

   In the first case (a), GTSM is not enabled for the LDP peering
   session by default. In the second case (b), GTSM is actually enabled
   by default and enforced for the LDP peering session, and hence, it
   would prohibit the LDP peering session from getting established (note
   that this may impact features such as LDP IGP Synchronization
   [RFC5443], or LDP Session Protection [LDP-SPROT]). In the third case
   (c), GTSM is enabled by default for Basic Discovery and enforced on
   the subsequent LDP peering, and not for Extended Discovery. However,
   if each LSR uses the same IPv4 transport address object value in both
   Basic and Extended discoveries, then it would result in a single LDP
   peering session and that would be enabled with GTSM. Otherwise, GTSM
   would not be enforced on the second LDP peering session corresponding
   to the Extended Discovery.

   This document allows for the implementation to provide an option to
   statically (e.g., via configuration) and/or dynamically override the
   default behavior and enable/disable GTSM on a per-peer basis. This
   would address all the exceptions listed above.

4. IANA Considerations

   This document has no IANA actions.

5. Security Considerations

   This document increases the security for LDP, making it more
   resilient to off-link attacks. Security considerations for GTSM are
   detailed in Section 5 of [RFC5082].

   As discussed in Section 3, it is possible that

   o GTSM for LDP may not always be enforced on a single-hop LDP
      peering session and LDP may still be susceptible to forged/spoofed
      protocol packets, if a single-hop LDP peering session is set up

      using Extended Discovery.

o GTSM for LDP may cause the LDP peering session to not get
      established (or may be torn down), if IP routing ever declares
      that the directly connected peer is more than one IP hop away.
      Suffice to say, use of cryptographic integrity (e.g., [RFC5925])
      is recommended as an alternate solution for detecting forged
      protocol packets (especially for the multi-hop case).

   The GTSM specification [RFC5082] says that protocol messages used for
   dynamic negotiation of GTSM support MUST be authenticated. However,
   LDP discovery [RFC5036] uses UDP transport and does not have an
   authentication mechanism. The GTSM specification further elaborates
   by saying that GTSM is not substitute for authentication and it does
   not secure against insider on-the-wire attacks. LDP Basic Discovery
   uses link-level multicast address (224.0.0.2 or "all routers") that
   are never forwarded beyond the link, and this acts as a basic
   protection against off-the-wire attacks.

6. Acknowledgments

   The authors of this document do not make any claims on the
   originality of the ideas described. The concept of GTSM for LDP has
   been proposed a number of times, and is documented in both the
   Experimental and Standards Track specifications of GTSM. Among other
   people, we would like to acknowledge Enke Chen and Albert Tian for
   their document "TTL-Based Security Option for the LDP Hello Message".

   The authors would like to thank Loa Andersson, Bin Mo, Mach Chen,
   Vero Zheng, Adrian Farrel, Eric Rosen, Eric Gray, and Brian Weis for
   a thorough review and most useful comments and suggestions.

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.

   [RFC5036] Andersson, L., Minei, I., and B. Thomas, "LDP
              Specification", RFC 5036, October 2007.

   [RFC5082] Gill, V., Heasley, J., Meyer, D., Savola, P., and C.
              Pignataro, "The Generalized TTL Security Mechanism
              (GTSM)", RFC 5082, October 2007.

7.2. Informative References

   [I-D.ietf-mpls-ldp-ipv6]
              Asati, R., Manral, V., Papneja, R., and C. Pignataro,
              "Updates to LDP for IPv6", draft-ietf-mpls-ldp-ipv6-07
              (work in progress), June 2012.

   [LDP-SPROT]
              Cisco Systems, Inc., "MPLS LDP Session Protection", <http:
              //www.cisco.com/en/US/docs/ios-xml/ios/mp_ldp/
              configuration/12-4m/mp-ldp-sessn-prot.html>.

   [RFC5443] Jork, M., Atlas, A., and L. Fang, "LDP IGP
              Synchronization", RFC 5443, March 2009.

   [RFC5925] Touch, J., Mankin, A., and R. Bonica, "The TCP
              Authentication Option", RFC 5925, June 2010.

Authors' Addresses

   Carlos Pignataro
   Cisco Systems
   7200-12 Kit Creek Road
   Research Triangle Park, NC 27709
   US

   Email: cpignata@cisco.com

   Rajiv Asati
   Cisco Systems
   7025-6 Kit Creek Road
   Research Triangle Park, NC 27709
   US

   Email: rajiva@cisco.com