               Analysis of LMP Security According to KARP Design Guide
                       draft-mahesh-karp-lmp-analysis-01.txt

Abstract

   This document analyzes Link Management Protocol (LMP) according to
   guidelines set forth in section 4.2 of KARP Design Guidelines (RFC
   6518).

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

   In March 2006, the Internet Architecture Board (IAB) described an
   attack on core routing infrastructure as an ideal attack that would
   inflict the greatest amount of damage, in their Report from the IAB
   workshop on Unwanted Traffic March 9-10, 2006 [RFC4948], and
   suggested steps to tighten the infrastructure against the attack.
   Four main steps were identified for that tightening:

   1. Create secure mechanisms and practices for operating routers.

   2. Clean up the Internet Routing Registry (IRR) repository, and
       securing both the database and the access, so that it can be used
       for routing verifications.

   3. Create specifications for cryptographic validation of routing
       message content.

   4. Secure the routing protocols' packets on the wire.

   In order to secure the routing protocols this document performs an
   initial analysis of the current state of LMP according to the
   requirements of KARP Design Guidelines [RFC6518]. This draft builds
   on several previous analysis efforts into routing security:

   o Issues with existing Cryptographic Protection Methods for Routing
      Protocols [RFC6039] an analysis of cryptographic issues with
      routing protocols.

   o Analysis of OSPF Security According to KARP Design Guide
      [RFC6863].

   o Analysis of BGP, LDP, PCEP, and MSDP Issues According to KARP
      Design Guide [RFC6952] which is a analysis of the four routing
      protocols.

   Link Management Protocol (LMP) [RFC4204] is used to manage Traffic
   Engineering (TE) links. According to the document, LMP can be
   subject to a number of attacks. Some examples include:

   o an adversary may spoof control packets

   o an adversary may modify the control packet in transit

   o an adversary may replay control packets

   o an adversary may study a number of control packets and try to
      break the key using cryptographic tools.

   Section 2 looks at the current security state of LMP. Section 3
   suggest an optimal security state and section 4 does an analysis of
   the gap between the existing and the optimal security state of the
   protocol and suggest some areas where we need to improve.

1.1. Abbreviations

   LMP - Link Management Protocol

   TE - Traffic Engineering

2. Current Assessment of LMP

   This section looks at LMP procedure, the underlying transport layer
   and security assessment associated with LMP.

2.1. LMP Procedure

   The two core procedures of LMP procedure are control channel
   management and link property correlation. Control channel management
   is used to establish and maintain control channels between adjacent
   nodes. This is done using a Config message exchange and a fast keep-
   alive mechanism between the nodes. Link property correlation is used

to synchronize the TE link properties and verify the TE link
configuration.

Two additional procedures include link connectivity verification and
fault management. Link connectivity verification is used for data
plane discovery, Interface_Id exchange, and physical connectivity
verification. This is done by sending Test messages over the data
channel and the TestStatus messages coming back over the control
plane. The LMP link connectivity verification procedure is
coordinated using the BeginVerify message exchanged over the control
channel.

The LMP fault management procedure is based on a ChannelStatus
message exchange. The ChannelStatus message is sent unsolicited and
is used to notify an LMP neighbor about the status of one or more
data channels. ChannelStatusAck is used to acknowledge receipt of
the ChannelStatus message. Similarly, a ChannelStatusResponse
message is used to acknowledge receipt of a ChannelStatusRequest
message.

2.2. Transport Layer

Except for Test messages, all LMP packets use UDP to communicate with
its piers over a LMP port number. Multiple "LMP adjacencies" may be
formed and be active between two nodes. LMP messages are transmitted
reliably using Message_Ids and retransmissions.

Unlike TCP which can use TCP-AO [RFC5925] for message authentication,
UDP does not have any of authenticating packets.

2.3. Message Integrity and Node Authentication

LMP [RFC4204] recommends the use of IPSec for authentication. That
document also states that there is currently no requirement that LMP
headers or payload be encrypted. It also states that LMP endpoint
identity does not need to be protected.

To authenticate LMP, the document further states that manual keying
mode be supported. However, it notes that manual keying cannot
effectively support replay protection and automatic re-keying. It
therefore recommends that manual keying should only be used for
diagnostic purposes and only use automatic re-keying for replay
protection and automatic re-keying.

2.4. Replay Attack

   MESSAGE_ID and MESSAGE_ID_ACK objects are included in the LMP
   messages to support reliable message delivery. The Message_Id field
   of the MESSAGE_ID object contains a generator selected value. This
   value is supposed to be monotonically increasing. A value is
   considered to be used when it has been sent in an LMP message with
   the same CC_Id or LMP adjacency. The Message_Id field of the
   MESSAGE_ID_ACK contains the Message_Id field of the message being
   acknowledged.

   Unacknowledged messages sent with the MESSAGE_ID object are to be
   retransmitted until the message is acknowledged or until a retry
   limit is reached. The Message_Id field is 32 bit wide and may wrap.

   The 32-bit Message_Id number space is not large enough to guarantee
   that the Message_Id number will not wrap around within a reasonable
   long period. Therefore, the system is susceptible to a replay
   attack.

   In addition, LMP does not provide for a generation of a unique
   monotonically increasing sequence numbers across a failure or a
   restart.

2.5. Out-of-order Protection

   LMP states that nodes processing incoming messages are supposed to
   check to see if the newly received message is out of order messages,
   and if so, they are to be ignored and dropped silently.

   Specifically, if the message is a Config message, and the Message_Id
   value is less than the largest Message_Id value previously received
   from the sender for the CC_Id, then the message is supposed to be
   treated as being out-of-order. If the message is a LinkSummary
   message and the Message_Id value is less than the largest Message_Id
   value previously received from the sender of the TE link, then the
   message is supposed to be treated as being out-of-order. Similarly,
   if the message is a ChannelStatus message and the Message_Id value is
   less than the largest Message_id value previously received from he
   sender of the specific TE link, then the receiver is supposed to
   check for the Message_Id value previously received from the state of
   each data channel included in the ChannelStatus message. If the
   Message_Id value associated with at least one of the data channels
   included in the message, the message is not supposed to be treated as
   out-of-order. All other messages are not supposed to be treated as
   out-of-order.

3. Security Requirements for LMP

   LMP [RFC4204] states that the following requirements should be
   applied to secure the protocol.

   o LMP security must be able to provide authentication, integrity and
      replay protection.

   o Confidentiality is not needed for LMP traffic.

   o The protection of identity of the LMP end-points is not commonly
      required.

   o The security mechanism should provide for a well defined key
      management scheme. The key management scheme should be scalable
      and should provide for automatic key rollover.

   o The algorithm used for authentication must be cryptographically
      sound and it should provide for algorithm agility.

4. Gap Analysis for LMP

   This section outlines the differences between the current state of
   LMP and the desired state as outlined in sections 4.1 and 4.2 of KARP
   Design Guidelines [RFC6518].

4.1. Replay Protection

   As outlined above, LMP protocol is subject to replay attacks.
   Solutions to replay protection include:

   1. Maintaining Message_Id numbers in stable memory

   2. Introducing the data from a local time clock into the generation
       of Message_Id numbers after a restart

   3. Introducing the timing information from a Network Recovered Clock
       into the generation of Message_Id numbers after a restart.

   In addition, a handshake is defined for a receiver to get the latest
   value of a Message_Id number. Therefore, this solution is effective
   in addressing the issues caused by the rollback of Message_Id numbers
   across a system restart or failure. However, when a router uses the
   approach to generating Message_Id numbers with the time information
   from NTP, an attacker may try to deceive the router to generate a
   Message_Id number which is less than the Message_Id numbers it used
   to have, by sending replayed or foiled NTP information.

5. IANA Requirements

This document makes no IANA requests, and the RFC Editor may consider deleting this section on publication of this document as a RFC.

6. Security Consideration

This document is all about security considerations for LMP.

7. Acknowledgements

8. References

8.1. Normative References

[RFC4204] Lang, J., "Link Management Protocol (LMP)", RFC 4204,
           October 2005.

[RFC6518] Lebovitz, G. and M. Bhatia, "Keying and Authentication for
           Routing Protocols (KARP) Design Guidelines", RFC 6518,
           February 2012.

8.2. Informative References

[RFC4948] Andersson, L., Davies, E., and L. Zhang, "Report from the
           IAB workshop on Unwanted Traffic March 9-10, 2006", RFC
           4948, August 2007.

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

[RFC6039] Manral, V., Bhatia, M., Jaeggli, J., and R. White, "Issues
           with Existing Cryptographic Protection Methods for Routing
           Protocols", RFC 6039, October 2010.

[RFC6863] Hartman, S. and D. Zhang, "Analysis of OSPF Security
           According to the Keying and Authentication for Routing
           Protocols (KARP) Design Guide", RFC 6863, March 2013.

[RFC6952] Jethanandani, M., Patel, K., and L. Zheng, "Analysis of
           BGP, LDP, PCEP, and MSDP Issues According to the Keying
           and Authentication for Routing Protocols (KARP) Design
           Guide", RFC 6952, May 2013.

Author's Address

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

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