Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: February 2, 2013

L. Zheng
M. Chen
Huawei Technologies
M. Bhatia
Alcatel-Lucent

August 1, 2012

LDP Hello Cryptographic Authentication
draft-ietf-mpls-ldp-hello-crypto-auth-00.txt

Abstract

This document introduces a new optional Cryptographic Authentication TLV that LDP can use to secure its Hello messages. It secures the Hello messages against spoofing attacks and some well known attacks against the IP header. This document describes a mechanism to secure the LDP Hello messages using National Institute of Standards and Technology (NIST) Secure Hash Standard family of algorithms.

Requirements Language

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 RFC 2119 [RFC2119].

Status of this Memo

This Internet-Draft will expire on February 2, 2013.

Copyright Notice

Table of Contents

1. Introduction

The Label Distribution Protocol (LDP) [RFC5036] sets up LDP sessions that runs between LDP peers. The peers could either be directly connected at the link level or could be multiple hops away. An LDP Label Switching Router (LSR) could either be configured with the identity of its peers or could discover them using LDP Hello messages. These messages are sent encapsulated in UDP addressed to "all routers on this subnet" or to a specific IP address. Periodic Hello messages are also used to maintain the relationship between LDP peers necessary to keep the LDP session active.

Unlike other LDP messages, the Hello messages are sent using UDP and not TCP. This implies that these messages cannot use the security mechanisms defined for TCP [RFC5926]. Besides a note that some configuration may help protect against bogus discovery messages, [RFC5036] does not really provide any security mechanism to protect the Hello messages.

Spoofing a Hello packet for an existing adjacency can cause the valid adjacency to time out and in turn can result in termination of the associated session. This can occur when the spoofed Hello specifies a smaller Hold Time, causing the receiver to expect Hellos within this smaller interval, while the true neighbor continues sending Hellos at the previously agreed lower frequency. Spoofing a Hello packet can also cause the LDP session to be terminated directly, which can occur when the spoofed Hello specifies a different Transport Address, other than the previously agreed one between neighbors. Spoofed Hello messages have been observed and reported as a real problem in production networks [I-D.ietf-karp-routing-tcp-analysis].

[RFC5036] describes that the threat of spoofed Basic Hellos can be reduced by accepting Basic Hellos only on interfaces to which LSRs that can be trusted are directly connected, and ignoring Basic Hellos not addressed to the "all routers on this subnet" multicast group. Spoofing attacks via Extended Hellos are a potentially more serious threat. An LSR can reduce the threat of spoofed Extended Hellos by filtering them and accepting only those originating at sources permitted by an access list. However, filtering using access lists requires LSR resource, and does not prevent IP-address spoofing.

This document introduces a new Cryptographic Authentication TLV which is used in LDP Hello message as an optional parameter. It enhances the authentication mechanism for LDP by securing the Hello message against spoofing attack. It also introduces a cryptographic sequence number carried in the Hello messages that can be used to protect against replay attacks. The LSRs could be configured to only accept

Hello messages from specific peers when authentication is in use.

Using this Cryptographic Authentication TLV, one or more secret keys (with corresponding key IDs) are configured in each system. For each LDP Hello packet, the key is used to generate and verify a HMAC Hash that is stored in the LDP Hello packet. For cryptographic hash function, this document proposes to use SHA-1, SHA-256, SHA-384, and SHA-512 defined in US NIST Secure Hash Standard (SHS) [FIPS-180-3]. The HMAC authentication mode defined in NIST FIPS 198 is used [FIPS-198]. Of the above, implementations MUST include support for at least HMAC-SHA-256 and SHOULD include support for HMAC-SHA-1 and MAY include support for either of HMAC-SHA-384 or HMAC-SHA-512.

2. Cryptographic Authentication TLV

2.1. Optional Parameter for Hello Message

[RFC5036] defines the encoding for the Hello message. Each Hello message contains zero or more Optional Parameters, each encoded as a TLV. Three Optional Parameters are defined by [RFC5036]. This document defines a new Optional Parameter: the Cryptographic Authentication parameter.

```
Optional Parameter               Type
------------------------------   --------
IPv4 Transport Address           0x0401 (RFC5036)
Configuration Sequence Number    0x0402 (RFC5036)
IPv6 Transport Address           0x0403 (RFC5036)
Cryptographic Authentication     0x0404 (this document, TBD by IANA)
```

The Cryptographic Authentication TLV Encoding is described in section 2.2.

2.2. Cryptographic Authentication TLV Encoding

```
    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|        Auth (TBD)         |             Length            |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                     Authentication Key ID                     |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |       Cryptographic Sequence Number (High Order 32 Bits)      |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |       Cryptographic Sequence Number (Low Order 32 Bits)       |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                                                               |
   |                Authentication Data (Variable)                 |
   ~                                                               ~
   |                                                               |
   |                                                               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

- Type: TBD, Cryptographic Authentication

- Length: Specifying the length in octets of the value field.

- Auth Key ID: 32 bit field that identifies the algorithm and the secret key used to create the message digest carried in LDP payload.

- Cryptographic Sequence Number: 64-bit strictly increasing sequence number that is used to guard against replay attacks. The 64-bit sequence number MUST be incremented for every LDP Hello packet sent by the LDP router. Upon reception, the sequence number MUST be greater than the sequence number in the last LDP Hello packet accepted from the sending LDP neighbor. Otherwise, the LDP packet is considered a replayed packet and dropped.

LDP routers implementing this specification SHOULD use available mechanisms to preserve the sequence number's strictly increasing property for the deployed life of the LDP router (including cold restarts). One mechanism for accomplishing this could be to use the high-order 32 bits of the sequence number as a wrap/boot count that is incremented anytime the LDP router loses its sequence number state. Techniques such as sequence number space partitioning described above or non-volatile storage preservation can be used but are really beyond the scope of this specification.

- Authentication Data:

This field carries the digest computed by the Cryptographic Authentication algorithm in use. The length of the Authentication Data varies based on the cryptographic algorithm in use, which is shown as below:

Auth type	Length
HMAC-SHA1	20 bytes
HMAC-SHA-256	32 bytes
HMAC-SHA-384	48 bytes
HMAC-SHA-512	64 bytes

3. Cryptographic Aspects

In the algorithm description below, the following nomenclature, which is consistent with [FIPS-198], is used:

- H is the specific hashing algorithm specified by Auth Type (e.g. SHA-256).

- K is the Authentication Key for the Hello packet.

- Ko is the cryptographic key used with the hash algorithm.

- B is the block size of H, in octets.

    For SHA-1 and SHA-256: B == 64
    For SHA-384 and SHA-512: B == 128

- L is the length of the hash outputs, in octets.

- XOR is the exclusive-or operation.

- Ipad is the byte 0x36 repeated B times.

- Opad is the byte 0x5c repeated B times.

- Apad is source IP address that the would be used when sending out the LDP packet, repeated L/4 times, where L is the length of the hash, measured in octets.

3.1. Cryptographic Key

As described in [RFC2104], the authentication key K can be of any length up to B. Applications that use keys longer than B bytes will first hash the key using H and then use the resultant L byte string as the actual key to HMAC.

In this application, Ko is always L octets long. If the Authentication Key (K) is L octets long, then Ko is equal to K. If the Authentication Key (K) is more than L octets long, then Ko is set to H(K). If the Authentication Key (K) is less than L octets long, then Ko is set to the Authentication Key (K) with trailing zeros such that Ko is L octets long.

3.2. Hash

First, the Authentication Data field in the Cryptographic Authentication TLV is filled with the value Apad. Then, to compute HMAC over the Hello packet it performs:

H(Ko XOR Opad || H(Ko XOR Ipad || (Hello Packet)))

Hello Packet refers to the LDP Hello packet excluding the IP header.

3.3. Result

The resultant Hash becomes the Authentication Data that is sent in the Authentication Data field of the Cryptographic Authentication TLV. The length of the Authentication Data field is always identical to the message digest size of the specific hash function H that is being used.

4. Processing Hello Message Using Cryptographic Authentication

4.1. Transmission Using Cryptographic Authentication

Prior to transmitting Hello message, the Length in the Cryptographic Authentication TLV header is set as per the authentication algorithm that is being used. It is set to 24 for HMAC-SHA-1, 36 for HMAC-SHA-256, 52 for HMAC-SHA-384 and 68 for HMAC-SHA-512.

The Auth Key ID field is set to the ID of the current authentication key. The HMAC Hash is computed as explained in Section 3. The resulting Hash is stored in the Authentication Data field prior to transmission. The authentication key MUST NOT be carried in the packet.

4.2. Receipt Using Cryptographic Authentication

The receiving LSR applies acceptability criteria for received Hellos using cryptographic authentication. If the Cryptographic Authentication TLV is unknown to the receiving LSR, the received packet MUST be discarded according to Section 3.5.1.2.2 of [RFC5036].

If the Auth Key ID field does not match the ID of a configured authentication key, the received packet MUST be discarded.

If the cryptographic sequence number in the LDP packet is less than or equal to the last sequence number received from the same neighbor, the LDP packet MUST be discarded.

Before the receiving LSR performs any processing, it needs to save the values of the Authentication Data field. The receiving LSR then replaces the contents of the Authentication Data field with Apad, computes the Hash, using the authentication key specified by the received Auth Key ID field, as explained in Section 3. If the locally computed Hash is equal to the received value of the Authentication Data field, the received packet is accepted for other normal checks and processing as described in [RFC5036]. Otherwise, if the locally computed Hash is not equal to the received value of the Authentication Data field, the received packet MUST be discarded.

5. Security Considerations

Section 1 of this document describes the security issues arising from the use of unauthenticated LDP Hello messages. In order to address those issues, it is RECOMMENDED that all deployments use the Cryptographic Authentication TLV to authenticate the Hello messages.

The quality of the security provided by the Cryptographic Authentication TLV depends completely on the strength of the cryptographic algorithm in use, the strength of the key being used, and the correct implementation of the security mechanism in communicating LDP implementations. Also, the level of security provided by the Cryptographic Authentication TLV varies based on the authentication type used.

It should be noted that the authentication method described in this document is not being used to authenticate the specific originator of a packet but is rather being used to confirm that the packet has indeed been issued by a router that has access to the Authentication Key.

Deployments SHOULD use sufficiently long and random values for the Authentication Key so that guessing and other cryptographic attacks on the key are not feasible in their environments. Furthermore, it is RECOMMENDED that Authentication Keys incorporate at least 128 pseudo-random bits to minimize the risk of such attacks. In support of these recommendations, management systems SHOULD support hexadecimal input of Authentication Keys.

The mechanism described herein is not perfect and does not need to be perfect. Instead, this mechanism represents a significant increase in the effort required for an adversary to successfully attack the LDP Hello protocol while not causing undue implementation, deployment, or operational complexity.

6. IANA Considerations

The IANA is requested to as assign a new TLV from the "Multiprotocol Label Switching Architecture (MPLS) Label Switched Paths (LSPs) Parameters - TLVs" registry, "TLVs and sub-TLVs" sub- registry.

Value	Meaning	Reference
TBD	Cryptographic Authentication TLV	this document (sect 3.2)

7. Acknowledgements

The authors would like to thank Liu Xuehu for his work on background and motivation for LDP Hello authentication. The authors also would like to thank Adrian Farrel, Eric Rosen, Sam Hartman, Eric Gray, Kamran Raza and Acee Lindem for their valuable comments.

We would also like to thank the authors of RFC 5709 from where we have taken most of the cryptographic computation procedures from.

8. References

8.1. Normative References

[FIPS-180-3]
"Secure Hash Standard (SHS), FIPS PUB 180-3", October 2008.

[FIPS-198]
"The Keyed-Hash Message Authentication Code (HMAC), FIPS PUB 198", March 2002.

[RFC2104] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.

[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.

8.2. References

8.3. Informative References

[I-D.ietf-karp-routing-tcp-analysis]
Jethanandani, M., Patel, K., and L. Zheng, "Analysis of BGP, LDP, PCEP and MSDP Issues According to KARP Design Guide", draft-ietf-karp-routing-tcp-analysis-04 (work in progress), July 2012.

[RFC5926] Lebovitz, G. and E. Rescorla, "Cryptographic Algorithms for the TCP Authentication Option (TCP-AO)", RFC 5926, June 2010.

Authors' Addresses

Lianshu Zheng
Huawei Technologies
China

Email: vero.zheng@huawei.com

Mach(Guoyi) Chen
Huawei Technologies
China

Email: mach.chen@huawei.com

Manav Bhatia
Alcatel-Lucent
India

Email: manav.bhatia@alcatel-lucent.com