OSPF Working Group
Internet-Draft
Intended status: Standards Track
Expires: August 23, 2011

M. Bhatia
Alcatel-Lucent
V. Manral
IP Infusion
A. Lindem
Ericsson

February 19, 2011

Supporting Authentication Trailer for OSPFv3
draft-ietf-ospf-auth-trailer-ospfv3-03

Abstract

Currently OSPFv3 uses IPsec for authenticating protocol packets. However, there are some environments, e.g., Mobile Ad-hoc Networks (MANETs), where IPsec is difficult to configure and maintain, and this mechanism cannot be used. This draft proposes an alternative mechanism that can be used so that OSPFv3 does not depend upon IPsec for authentication.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on August 23, 2011.

Copyright Notice

Table of Contents

1. Introduction

Unlike Open Shortest Path First version 2 (OSPFv2) [RFC2328], OSPF for IPv6 (OSPFv3) [RFC5340], does not include the AuType and Authentication fields in its headers for authenticating protocol packets. Instead, OSPFv3 relies on the IPv6 Authentication Header (AH)[RFC4302] and IPv6 Encapsulating Security Payload (ESP) [RFC4303] to provide integrity, authentication, and/or confidentiality.

[RFC4552] describes how IPv6 AH and ESP extension headers can be used to provide authentication and/or confidentiality to OSPFv3.

However, there are some environments, e.g., Mobile Ad-hoc Networks (MANETs), where IPsec is difficult to configure and maintain, and this mechanism cannot be used. There is also an issue with IPsec not being available on some platforms or it requiring an additional license.

[RFC4552] discusses, at length, the reasoning behind using manually configured keys, rather than some automated key management protocol such as IKEv2 [RFC5996]. The primary problem is the lack of suitable key management mechanism, as OSPF adjacencies are formed on a one-to-many basis and most key management mechanisms are designed for a one-to-one communication model. This forces the system administrator to use manually configured security associations (SAs) and cryptographic keys to provide the authentication and, if desired, confidentiality services.

Regarding replay protection [RFC4552] states that:

"As it is not possible as per the current standards to provide complete replay protection while using manual keying, the proposed solution will not provide protection against replay attacks."

Since there is no replay protection provided there are a number of vulnerabilities in OSPFv3 which have been discussed in [RFC6039].

Since there is no deterministic way to differentiate between encrypted and unencrypted ESP packets by simply examining the packet, it could become tricky for some implementations to prioritize certain OSPFv3 packets (Hellos for example) over the others.

This draft proposes a new mechanism that works similar to OSPFv2 [RFC5709]for providing authentication to the OSPFv3 packets and attempts to solve the problems described above for OSPFv3.

Additionally this document describes how HMAC-SHA authentication can be used for OSPFv3.

By definition, HMAC ([RFC2104] , [FIPS-198]) requires a cryptographic hash function. This document proposes to use any one of SHA-1, SHA-256, SHA-384, or SHA-512 [FIPS-180-3] to authenticate the OSPFv3 packets.

It is believed that [RFC2104] is mathematically identical to [FIPS-198] and it is also believed that algorithms in [RFC4634] are mathematically identical to [FIPS-180-3].

1.1. Requirements Section

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].

When used in lowercase, these words convey their typical use in common language, and are not to be interpreted as described in RFC2119 [RFC2119].

2. Proposed Solution

To perform non-IPsec cryptographic authentication, OSPFv3 routers append a special data block, henceforth referred to as, the authentication trailer to the end of the OSPFv3 packets. The length of the authentication trailer is not included into the length of the OSPFv3 packet, but is included in the IPv6 payload length.

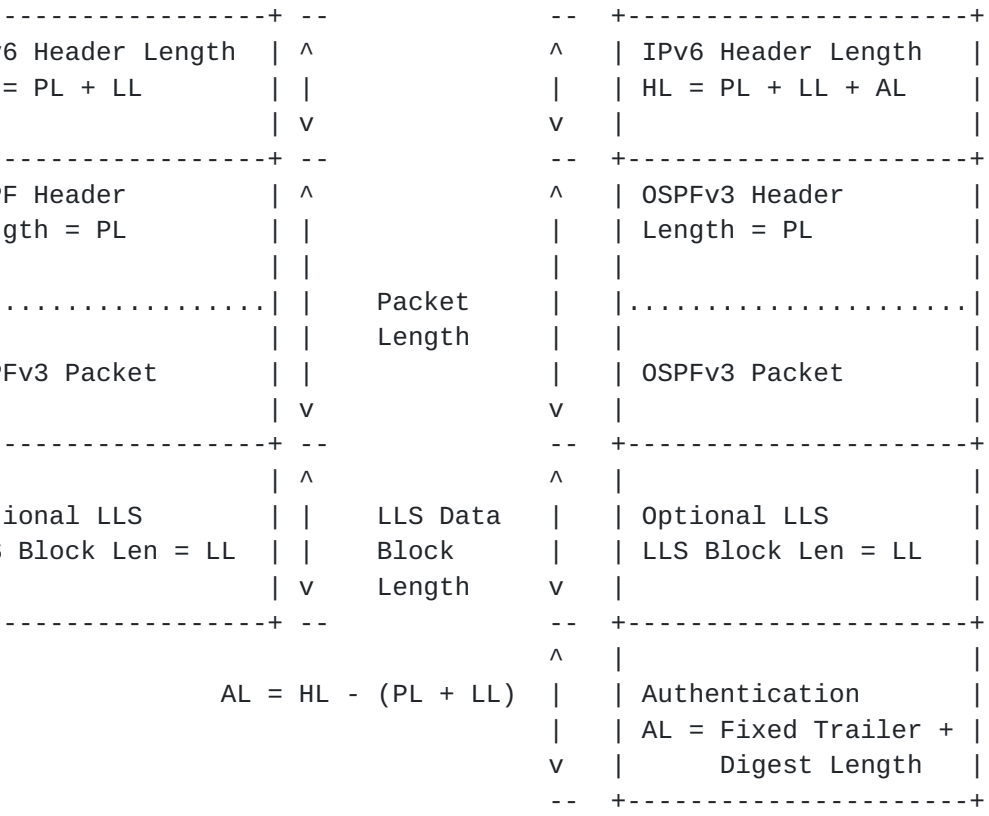

Figure 1: Authentication Trailer in OSPFv3

The presence of the Link Local Signaling (LLS) [RFC5613] block, is determined by the L-bit setting in OSPFv3 options field in OSPFv3 Hello and Database Description packets. If present, the LLS block is included along with the OSPFv3 packet in the cryptographic authentication computation.

2.1. AT-Bit in Options Field

A new AT-bit (AT stands for Authentication Trailer) is introduced into the OSPFv3 Options field. OSPFv3 routers MUST set the AT-bit in OSPFv3 Hello and Database Description packets to indicate that the OSPFv3 router will include the authentication trailer in all OSPFv3 packets on the link. For OSPFv3 Hello and Database Description packets, the AT-bit indicates the AT is present. For other OSPFv3

packet types, the OSPFv3 AT bit setting is preserved from the OSPFv3 Hello/Database Description setting.

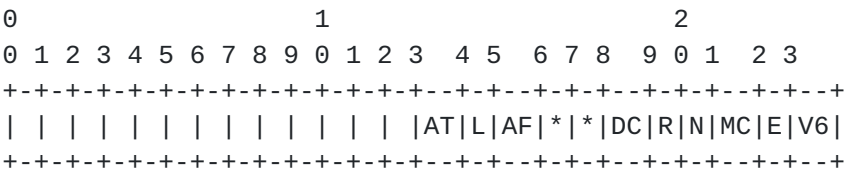

Figure 2: OSPFv3 Options Field

The AT-bit must be set in all OSPFv3 Hello and Database Description packets that contain an authentication trailer.

2.2. Basic Operation

The procedure followed for computing the Authentication Trailer is much same as described in [RFC5709] and [RFC2328]. One difference is that the LLS block, if present, is included in the cryptographic authentication computation.

The way the authentication data is carried in the Authentication Trailer is very similar to how it is done in case of [RFC2328]. The only difference between the OSPFv2 authentication trailer and the OSPFv3 authentication trailer is that information in addition to the message digest is included.

Consistent with OSPFv2 cryptographic authentication [RFC2328], both OSPFv3 header checksum calculation and verification are omitted when the OSPFv3 authentication mechanisms described in this specification are used.

3. OSPFv3 Security Association

An OSPFv3 Security Association (SA) contains a set of parameters shared between any two legitimate OSPFv3 speakers.

Parameters associated with an OSPFv3 SA:

- Security Association Identifier (SA ID)

  This is a 32-bit unsigned integer used to uniquely identify an OSPFv3 SA, as manually configured by the network operator.

  The receiver determines the active SA by looking at the SA ID field in the incoming protocol packet.

  The sender based on the active configuration, selects an SA to use and puts the correct Key ID value associated with the SA in the OSPFV3 protocol packet. If multiple valid and active OSPFv3 SAs exist for a given interface, the sender may use any of those SAs to protect the packet.

  Using SA IDs makes changing keys while maintaining protocol operation convenient. Each SA ID specifies two independent parts, the authentication protocol and the authentication key, as explained below.

  Normally, an implementation would allow the network operator to configure a set of keys in a key chain, with each key in the chain having fixed lifetime. The actual operation of these mechanisms is outside the scope of this document.

  Note that each SA ID can indicate a key with a different authentication protocol. This allows the introduction of new authentication mechanisms without disrupting existing OSPFv3 adjacencies.

- Authentication Algorithm

  This signifies the authentication algorithm to be used with the OSPFv3 SA. This information is never sent in clear text over the wire. Because this information is not sent on the wire, the implementer chooses an implementation specific representation for this information.

  Currently, the following algorithms are supported:

  HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512.

- Authentication Key

  This value denotes the cryptographic authentication key associated with the OSPFv3 SA. The length of this key is variable and depends upon the authentication algorithm specified by the OSPFv3 SA.

4. Authentication Procedure

4.1. Authentication Trailer

The authentication trailer that is appended to the OSPFv3 protocol packet is described below:

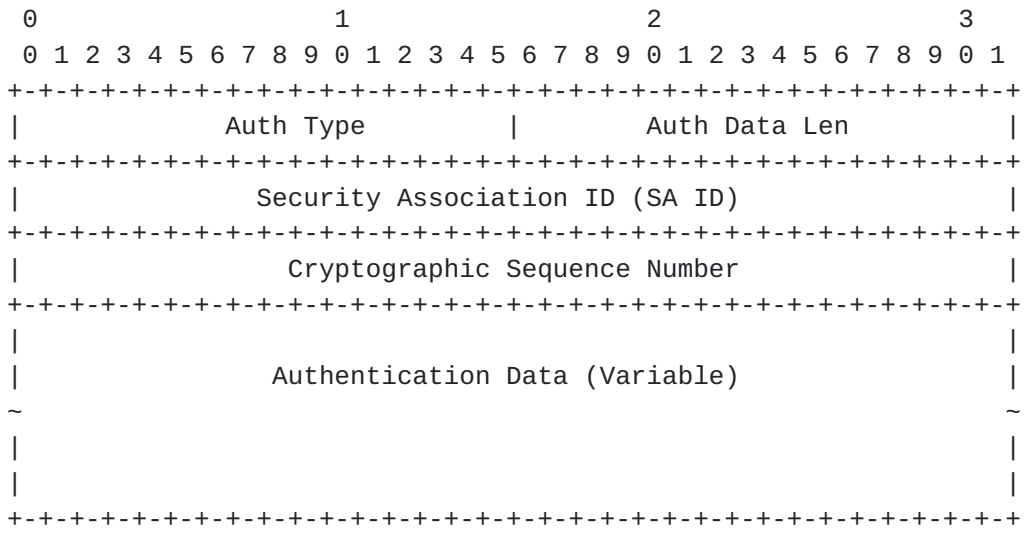

Figure 3: Authentication Trailer Format

The various fields in the Authentication trailer are:

o Auth Type

  16-bit field identifying the type of authentication. The following values are defined in this specification:

    0 - Reserved.
    1 - Cryptographic Authentication as described herein.

o Auth Data Len

  The length in bytes of the message digest appended to the OSPF packet.

o Security Association Identifier (SA ID)

  32-bit field that identifies the algorithm and the secret key used to create the message digest appended to the OSPFv3 protocol packet. Key Identifiers are unique per-interface.

- Cryptographic Sequence Number

  32-bit non-decreasing sequence number that is used to guard against replay attacks.

- Authentication Data

  Variable data that is carrying the digest for the protocol packet and optional LLS block.

4.2. OSPFv3 Header Checksum

Both OSPFv3 header checksum calculation and verification are omitted when the OSPFv3 authentication mechanisms described in this specification are used. This implies:

- For OSPFv3 packets to be transmitted, the OSPFv3 header checksum computation is omitted and the OSPFv3 header checksum SHOULD be set to 0 prior to computation of the OSPFv3 Authentication Trailer message digest.

- For received OSPFv3 packets including an OSPFv3 Authentication Trailer, OSPFv3 header checksum verification MUST be omitted.

4.3. Cryptographic Authentication Procedure

As noted earlier, the SA ID implicitly specifies the algorithms used to generate and verify the message digest. This specification discusses the computation of OSPFv3 Cryptographic Authentication data when any of the NIST SHS family of algorithms is used in the Hashed Message Authentication Code (HMAC) mode.

The currently valid algorithms (including mode) for OSPFv3 Cryptographic Authentication include:

HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384 and HMAC-SHA-512

Of the above, implementations of this specification MUST include support for at least HMAC-SHA-1 and SHOULD include support for HMAC-SHA-256 and MAY also include support for HMAC-SHA-384 and HMAC-SHA-512.

4.4. Cryptographic Aspects

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

H is the specific hashing algorithm (e.g. SHA-256).

K is the Authentication Key for the OSPFv3 security association.

Ko is the cryptographic key used with the hash algorithm.

B is the block size of H, measured in octets rather than bits.

Note that B is the internal block size, not the hash size.

For SHA-1 and SHA-256: B == 64

For SHA-384 and SHA-512: B == 128

L is the length of the hash, measured in octets rather than bits.

XOR is the exclusive-or operation.

Opad is the hexadecimal value 0x5c repeated B times.

Ipad is the hexadecimal value 0x36 repeated B times.

Apad is the hexadecimal value 0x878FE1F3 repeated (L/4) times.

Implementation Note:

This definition of Apad means that Apad is always the same length as the hash output.

1. Preparation of the Key

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 zeros appended to the end of the Authentication Key (K) such that Ko is L octets long.

2. First Hash

First, the OSPFv3 packet's Authentication Trailer (which is very similar to the appendage described in RFC 2328, Section D.4.3, Page 233, items(6)(a) and (6)(d)) is filled with the value Apad.

Then, a First-Hash, also known as the inner hash, is computed as follows:

First-Hash = H(Ko XOR Ipad || (OSPFv3 Packet))

Implementation Notes:

Note that the First-Hash above includes the Authentication Trailer containing the Apad value, as well as the OSPFv3 packet, as per RFC 2328, Section D.4.3 and, if present, the LLS block[RFC5613].

The definition of Apad (above) ensures it is always the same length as the hash output. This is consistent with RFC 2328. The "(OSPFv3 Packet)" mentioned in the First-Hash (above) does include both the optional LLS block and the OSPF Authentication Trailer.

The digest length for SHA-1 is 20 bytes; for SHA-256, 32 bytes; for SHA-384, 48 bytes; and for SHA-512, 64 bytes.

3. Second Hash

Then a second hash, also known as the outer hash, is computed as follows:

Second-Hash = H(Ko XOR Opad || First-Hash)

4. Result

The resulting Second-Hash becomes the authentication data that is sent in the Authentication Trailer of the OSPFv3 packet. The length of the authentication data is always identical to the message digest size of the specific hash function H that is being used.

This also means that the use of hash functions with larger output sizes will also increase the size of the OSPFv3 packet as transmitted on the wire.

Implementation Note:

RFC 2328, Appendix D specifies that the Authentication Trailer is not counted in the OSPF packet's own Length field, but is included in the packet's IP Length field. Similar to this, the Authentication Trailer is not included in OSPFv3's own Length field, but is included in IPv6's payload length.

4.5. Message Verification

A router would determine that OSPFv3 is using an Authentication trailer by examining the AT-bit in the Options field in the OSPFv3 header for Hello and Database Description packets. The specification in the Hello and Database description options indicates that other OSPFv3 packets will include the authentication trailer.

The Authentication Trailer (AT) is accessed using the OSPFv3 packet header length to access the data after the OSPFv3 packet and, if an LLS Data Block [RFC5613] is present, using the LLS Data Block Length to access the data after the LLS Data Block. The L-bit in the OSPFv3 options in Hello and Database Description packets is examined to determine if an LLS Data Block is present. If an LLS block is present (as specified by the L-bit), it is included along with the OSPFv3 Hello or Database Description packet in the cryptographic authentication computation.

Due to the placement of the AT following the LLS block and the fact that the LLS block is included in the cryptographic authentication computation, OSPFv3 routers supporting this specification MUST minimally support examining the L-bit in the OSPFv3 options and using the length in the LLS block to access the AT. It is RECOMMENDED that OSPFv3 routers supporting this specification fully support OSPFv3 Link Local Signaling, [RFC5613].

If usage of the Authentication Trailer (AT), as specified herein, is configured for an OSPFv3 link, OSPFv3 Hello and Database Description packets with the AT-bit clear in the options will be dropped. All OSPFv3 packet types will be dropped if AT is configured for the link and the IPv6 header length is less than the amount necessary to include an authentication trailer.

Authentication algorithm dependent processing needs to be performed, using the algorithm specified by the appropriate OSPFv3 SA for the received packet.

Before an implementation performs any processing it needs to save the values of the Authentication data field from the Authentication Trailer appended to the OSPFv3 packet.

It should then set the Authentication data field with Apad before the authentication data is computed. The calculated data is compared with the received authentication data in the Authentication trailer and the packet MUST be discarded if the two do not match. In such a case, an error event SHOULD be logged.

5. Migration and Backward Compatibility

In general, all OSPFv3 routers participating on a link should be migrated to OSPFv3 Authentication at the same time. As with OSPFv2 authentication, a mismatch in the SA ID, Authentication Type, or message digest will result in failure to form an adjacency. For multi-access links, communities of OSPFv3 routers could be migrated using different interface instance IDs. However, at least one router would need to form adjacencies between both the OSPFv3 routers including and not including the authentication trailer. This would result in sub-optimal routing, as well as, added complexity and is only recommended in cases where authentication is desired on the link and it isn't feasible to migrate all the routers on the link at the same time.

An implementation MAY have a transition mode where it includes the Authentication Trailer in the packets but does not verify this information. This is provided as a transition aid for networks in the process of migrating to the mechanism described in this draft.

6. Security Considerations

The document proposes extensions to OSPFv3 which would make it more secure than [RFC5340]. It does not provide confidentiality as a routing protocol contains information that does not need to be kept secret. It does, however, provide means to authenticate the sender of the packets which is of interest to us.

It should be noted that 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 which had access to the password.

The mechanism described here is not perfect and does not need to be perfect. Instead, this mechanism represents a significant increase in the work function of an adversary attacking the OSPFv3 protocol, while not causing undue implementation, deployment, or operational complexity.

7. IANA Considerations

IANA is requested to allocate AT-bit in the OSPFv3 "Options Registry"

IANA is also requested to create new OSPFv3 "Authentication Trailer Types Registry"

Value/Range	Designation	Assignment Policy
0	Reserved	Reserved
1	Cryptographic Authentication	Already assigned
2-65535	Unassigned	Standards Action

OSPFv3 Authentication Types

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2328] Moy, J., "OSPF Version 2", STD 54, RFC 2328, April 1998.

[RFC5709] Bhatia, M., Manral, V., Fanto, M., White, R., Barnes, M., Li, T., and R. Atkinson, "OSPFv2 HMAC-SHA Cryptographic Authentication", RFC 5709, October 2009.

8.2. Informative References

[FIPS-180-3] US National Institute of Standards & Technology, "Secure Hash Standard (SHS)", FIPS PUB 180-3 , October 2008.

[FIPS-198] US National Institute of Standards & Technology, "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.

[RFC4302] Kent, S., "IP Authentication Header", RFC 4302, December 2005.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.

[RFC4552] Gupta, M. and N. Melam, "Authentication/Confidentiality for OSPFv3", RFC 4552, June 2006.

[RFC4634] Eastlake, D. and T. Hansen, "US Secure Hash Algorithms (SHA and HMAC-SHA)", RFC 4634, July 2006.

[RFC5340] Coltun, R., Ferguson, D., Moy, J., and A. Lindem, "OSPF for IPv6", RFC 5340, July 2008.

[RFC5613] Zinin, A., Roy, A., Nguyen, L., Friedman, B., and D. Yeung, "OSPF Link-Local Signaling", RFC 5613, August 2009.

[RFC5996] Kaufman, C., Hoffman, P., Nir, Y., and P. Eronen, "Internet Key Exchange Protocol Version 2 (IKEv2)",

RFC 5996, September 2010.

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

Appendix A. Acknowledgments

First and foremost, thanks to the authors of RFC5709[RFC5709] from which this work was derived.

Thanks to Michael Barnes for numerous comments and strong input on the coverage of LLS by the Authentication Trailer (AT).

Thanks to Rajesh Shetty for numerous comments including the suggestion to include an Authentication Type field in the Authentication Trailer for extendibility.

Thanks to Srinivasan K L, Shraddha H, Alan Davey, and Glen Kent for their review comments.

Thanks to Alan Davey, Russ White, Stan Ratliff, and others for their support of the draft.

The RFC text was produced using Marshall Rose's xml2rfc tool.

Authors' Addresses

Manav Bhatia
Alcatel-Lucent
Bangalore,
India

Phone:
Email: manav.bhatia@alcatel-lucent.com

Vishwas
IP Infusion
USA

Phone:
Email: vishwas@ipinfusion.com

Acee Lindem
Ericsson
102 Carric Bend Court
Cary, NC 27519
USA

Phone:
Email: acee.lindem@ericsson.com