OSPF Working Group	M. Bhatia
Internet-Draft	Alcatel-Lucent
Intended status: Standards Track	V. Manral
Expires: April 18, 2011	IP Infusion
	A. Lindem
	Ericsson
	October 15, 2010

TOC

Supporting Authentication Trailer for OSPFv3
draft-bhatia-manral-auth-trailer-ospfv3-01

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 April 18, 2011.

Copyright Notice

from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

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] (Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” March 1997.).
When used in lowercase, these words convey their typical use in common language, and are not to be interpreted as described in RFC2119 [RFC2119] (Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” March 1997.).

---

1. Introduction

TOC

Unlike Open Shortest Path First version 2 (OSPFv2) [RFC2328] (Moy, J., “OSPF Version 2,” April 1998.), OSPF for IPv6 (OSPFv3) [RFC5340] (Coltun, R., Ferguson, D., Moy, J., and A. Lindem, “OSPF for IPv6,” July 2008.), 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] (Kent, S., “IP Authentication Header,” December 2005.) and IPv6 Encapsulating Security Payload (ESP) [RFC4303] (Kent, S., “IP Encapsulating Security Payload (ESP),” December 2005.) to provide integrity, authentication, and/or confidentiality.

[RFC4522] (Legg, S., “Lightweight Directory Access Protocol (LDAP): The Binary Encoding Option,” June 2006.) 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.

[RFC4522] (Legg, S., “Lightweight Directory Access Protocol (LDAP): The Binary Encoding Option,” June 2006.) discusses, at length, the reasoning behind using manually configured keys, rather than some automated key management protocol such as IKEv2 [RFC5996] (Kaufman, C., Hoffman, P., Nir, Y., and P. Eronen, “Internet Key Exchange Protocol Version 2 (IKEv2),” September 2010.) . 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 [RFC4522] (Legg, S., “Lightweight Directory Access Protocol (LDAP): The Binary Encoding Option,” June 2006.) 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 [I-D.ietf-opsec-routing-protocols-crypto-issues] (Jaeggli, J., Hares, S., Bhatia, M., Manral, V., and R. White, “Issues with existing Cryptographic Protection Methods for Routing Protocols,” August 2010.).

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] (Bhatia, M., Manral, V., Fanto, M., White, R., Barnes, M., Li, T., and R. Atkinson, “OSPFv2 HMAC-SHA Cryptographic Authentication,” October 2009.)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] (Krawczyk, H., Bellare, M., and R. Canetti, “HMAC: Keyed-Hashing for Message Authentication,” February 1997.) , [FIPS-198] (US National Institute of Standards & Technology, “The Keyed-Hash Message Authentication Code (HMAC),” March 2002.)) 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] (US National Institute of Standards & Technology, “Secure Hash Standard (SHS),” October 2008.) to authenticate the OSPFv3 packets.
It is believed that [RFC2104] (Krawczyk, H., Bellare, M., and R. Canetti, “HMAC: Keyed-Hashing for Message Authentication,” February 1997.) is mathematically identical to [FIPS-198] (US National Institute of Standards & Technology, “The Keyed-Hash Message Authentication Code (HMAC),” March 2002.) and it is also believed that algorithms in [RFC4634] (Eastlake, D. and T. Hansen, “US Secure Hash Algorithms (SHA and HMAC-SHA),” July 2006.) are mathematically identical to [FIPS-180-3] (US National Institute of Standards & Technology, “Secure Hash Standard (SHS),” October 2008.).

---

2. Proposed Solution

TOC

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.

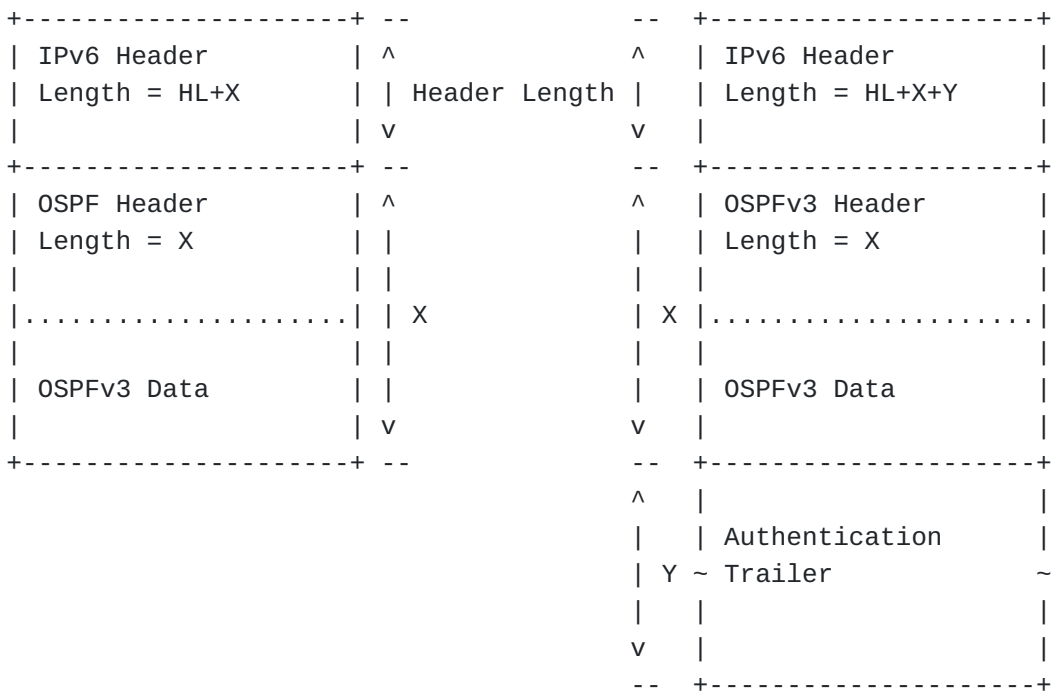

Figure 1: Authentication Trailer in OSPFv3

For the sake of consistency and simplicity the authentication trailer in the OSPFv3 packets MUST be inserted before the link local signalling (LLS) [RFC5613] (Zinin, A., Roy, A., Nguyen, L., Friedman, B., and D. Yeung, "OSPF Link-Local Signaling," August 2009.) block, if it exists. This is inline with the authentication mechanism that currently exists for OSPFv2.

2.1. AT-Bit in Options Field

TOC

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. In other words, the authentication trailer is only examined if the AT-bit is set.

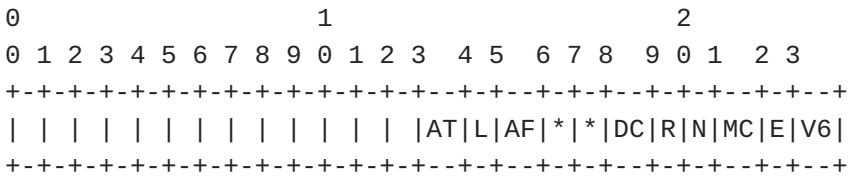

Figure 2: OSPFv3 Options Field

The AT-bit must be set in all OSPFv3 protocol packets that contain an authentication trailer.

2.2. Basic Operation

TOC

The procedure followed for computing the Authentication Trailer is exactly the same as described in [RFC5709] (Bhatia, M., Manral, V., Fanto, M., White, R., Barnes, M., Li, T., and R. Atkinson, "OSPFv2 HMAC-SHA Cryptographic Authentication," October 2009.) and [RFC2328] (Moy, J., "OSPF Version 2," April 1998.).
The way the authentication data is carried in the Authentication Trailer is very similar to how its done in case of [RFC2328] (Moy, J., "OSPF Version 2," April 1998.). The only difference between this

mechanism and OSPFv2's authentication mechanism is that for OSPFv3 some additional authentication information in addition to the message digest, is appended to the protocol packet.

---

3. OSPFv3 Security Association

TOC

An OSPFv3 Security Association (SA) contains a set of parameters shared between any two legitimate OSPFv3 speakers.
Parameters associated with an OSPFv3 SA:

*Key Identifier (Key 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 Key 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 Key IDs makes changing keys while maintaining protocol operation convenient. Each key 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 key 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 cleartext over the wire. Because this information is not sent on the wire, the implementer chooses an implementation specific representation for this information.

At present, the following values are possible:

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

TOC

4.1. Authentication Trailer

TOC

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

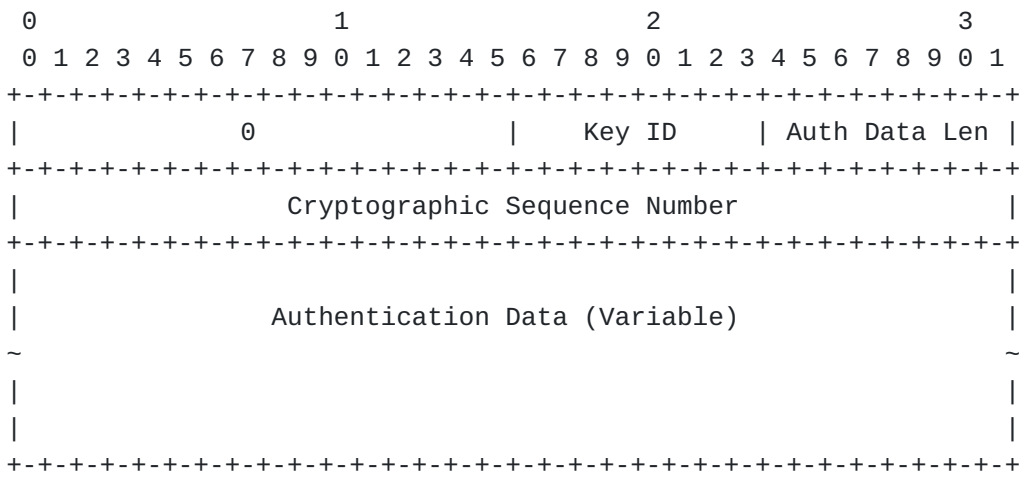

Figure 3: Authentication Trailer Format

The idea is to keep the fields as similar as possible with OSPFv2 so that most of the source code can be reused for authenticating the

OSPFv3 protocol packets.

The various fields in the Authentication trailer are:

*Reserved

16-bit reserved field. The value MUST be initialized to zero by the sender, and MUST be ignored by the receiver.

*Key ID (Identifier)

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 of the protocol packet.

4.2. Cryptographic Authentication Procedure

TOC

As noted earlier the algorithms used to generate and verify the message digest are specified implicitly by the secret key. 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.

TOC

4.3. Cryptographic Aspects

In the algorithm description below, the following nomenclature, which is consistent with [FIPS-198] (US National Institute of Standards & Technology, "The Keyed-Hash Message Authentication Code (HMAC)," March 2002.), 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.

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 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.

4.4. Message Verification

TOC

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.

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.

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.

5. Security Considerations

TOC

The document proposes extensions to OSPFv3 which would make it more secure than what it is today. 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.

6. IANA Considerations

TOC

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

7. References

TOC

7.1. Normative References

TOC

[RFC2119]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).
[RFC2328]	Moy, J., "OSPF Version 2," STD 54, RFC 2328, April 1998 (TXT, HTML, XML).
[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 (TXT).

7.2. Informative References

TOC

[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.
[I-D.hartman-ospf-analysis]	Hartman, S. and D. Zhang, "Analysis of OSPF Security According to KARP Design Guide," draft-hartman-ospf-analysis-01 (work in progress), June 2010 (TXT).
[I-D.ietf-opsec-routing-protocols-crypto-issues]	Jaeggli, J., Hares, S., Bhatia, M., Manral, V., and R. White, "Issues with existing Cryptographic Protection Methods for Routing Protocols," draft-ietf-opsec-routing-protocols-crypto-issues-07 (work in progress), August 2010 (TXT).
[RFC2104]	

	Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication," RFC 2104, February 1997 (TXT).
[RFC4302]	Kent, S., "IP Authentication Header," RFC 4302, December 2005 (TXT).
[RFC4303]	Kent, S., "IP Encapsulating Security Payload (ESP)," RFC 4303, December 2005 (TXT).
[RFC4522]	Legg, S., "Lightweight Directory Access Protocol (LDAP): The Binary Encoding Option," RFC 4522, June 2006 (TXT).
[RFC4634]	Eastlake, D. and T. Hansen, "US Secure Hash Algorithms (SHA and HMAC-SHA)," RFC 4634, July 2006 (TXT).
[RFC5340]	Coltun, R., Ferguson, D., Moy, J., and A. Lindem, "OSPF for IPv6," RFC 5340, July 2008 (TXT).
[RFC5613]	Zinin, A., Roy, A., Nguyen, L., Friedman, B., and D. Yeung, "OSPF Link-Local Signaling," RFC 5613, August 2009 (TXT).
[RFC5996]	Kaufman, C., Hoffman, P., Nir, Y., and P. Eronen, "Internet Key Exchange Protocol Version 2 (IKEv2)," RFC 5996, September 2010 (TXT).

Authors' Addresses

TOC

	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