OSPF Working Group M. Bhatia
Internet-Draft Alcatel-Lucent
Intended status: Standards Track V. Manral
Expires: May 24, 2012 Hewlett Packard
A. Lindem
Ericsson
Nov 21, 2011

Supporting Authentication Trailer for OSPFv3
draft-ietf-ospf-auth-trailer-ospfv3-11

Abstract

Currently OSPFv3 uses IPsec as the only mechanism for authenticating protocol packets. This behavior is different from authentication mechanisms present in other routing protocols (OSPFv2, IS-IS, RIPng). In some environments, it has been found that IPsec is difficult to configure and maintain, and cannot be used. This document proposes an alternative mechanism to authenticate OSPFv3 protocol packets so that OSPFv3 does not depend upon only IPsec for authentication.

Status of this Memo

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 IPsec protocols Authentication Header (AH)[RFC4302] and 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.

[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 OSPFv3 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 that 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 document proposes a new mechanism that works similar to OSPFv2 [RFC5709]for providing authentication to the OSPFv3 packets and attempts to solve the problems related to replay protection and deterministically disambiguating different OSPFv3 packets as described above.

This document adds support for Secure Hash Algorithms (SHA) defined

in the US NIST Secure Hash Standard (SHS), which is defined by NIST FIPS 180-3. [FIPS-180-3] includes SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512. The Hashed Message Authentication Code (HMAC) authentication mode defined in NIST FIPS 198 is used [FIPS-198].

It is believed that HMAC defined in [RFC2104] is mathematically identical to [FIPS-198] and it is also believed that algorithms in [RFC6234] are mathematically identical to [FIPS-198].

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].

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, as shown in the figure below .

```
 +---------------------+ --              --  +---------------------+
 | IPv6 Header Length  | ^               ^   | IPv6 Header Length  |
 | HL = PL + LL        | |               |   | HL = PL + LL + AL   |
 |                     | v               v   |                     |
 +---------------------+ --              --  +---------------------+
 | OSPFv3 Header       | ^               ^   | OSPFv3 Header       |
 | Length = PL         | |               |   | Length = PL         |
 |                     | |               |   |                     |
 |.....................| |   Packet      |   |.....................|
 |                     | |   Length      |   |                     |
 | OSPFv3 Packet       | |               |   | OSPFv3 Packet       |
 |                     | v               v   |                     |
 +---------------------+ --              --  +---------------------+
```

```
   |                      | ^               ^  |                       |
   | Optional LLS         | |    LLS Data   |  | Optional LLS          |
   | LLS Block Len = LL   | |    Block      |  | LLS Block Len = LL    |
   |                      | v    Length     v  |                       |
   +----------------------+ --              --  +-----------------------+
                                            ^  |                       |
                     AL = HL - (PL + LL)    |  | Authentication        |
                                            |  | AL = Fixed Trailer +  |
                                            v  |      Digest 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 all the packets on this link will include an authentication trailer. 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 from the OSPFv3 Hello/Database Description setting is preserved in the OSPFv3 neighbor data structure. OSPFv3 packet types that don't include an OSPFv3 options field will use the setting from the neighbor data structure to determine whether or not the AT is expected.

```
           0                   1                      2
           0 1 2 3 4 5 6 7 8 9 0 1 2 3  4 5  6 7 8  9 0 1  2 3
           +-+-+-+-+-+-+-+-+-+-+-+-+-+--+-+--+-+-+--+-+-+--+--+
           | | | | | | | | | | | | |  |AT|L|AF|*|*|DC|R|N|MC|E|V6|
           +-+-+-+-+-+-+-+-+-+-+-+-+-+--+-+--+-+-+--+-+-+--+--+
```

Figure 2: OSPFv3 Options Field

The AT-bit MUST be set in all OSPFv3 Hello and Database Description packets that contain an authentication trailer as shown in the figure above.

2.2. Basic Operation

The procedure followed for computing the Authentication Trailer is much the 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. The additional information in the OSPFv3 Authentication Trailer is included in the message digest computation and, therefore, protected by OSPFv3 cryptographic authentication as described herein.

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.

2.3. IPv6 Source Address Protection

While OSPFv3 always uses the Router ID to identify OSPFv3 neighbors, the IPv6 source address is learned from OSPFv3 hello packets and copied into the neighbor data structure [RFC5340]. Hence, OSPFv3 is susceptible to Man-in-the-Middle attacks where the IPv6 source

address has been modified. To thwart such attacks, the IPv6 source address will be included in the message digest calculation and protected by OSPFv3 authentication. Refer to Section 4.5 for details. This is different than the procedure specified in [RFC5709] but consistent with [I-D.ietf-ospf-security-extension-manual-keying].

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:

o 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 algorithm 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 algorithm. This allows the introduction of new authentication mechanisms without disrupting existing OSPFv3 adjacencies.

o 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.

- o 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.

- o KeyStartAccept

  The time that this OSPFv3 router will accept packets that have been created with this OSPFv3 Security Association.

- o KeyStartGenerate

  The time that this OSPFv3 router will begin using this OSPFv3 Security Association for OSPFv3 packet generation.

- o KeyStopGenerate

  The time that this OSPFv3 router will stop using this OSPFv3 Security Association for OSPFv3 packet generation.

- o KeyStopAccept

  The time that this OSPFv3 router will stop accepting packets generated with this OSPFv3 Security Association.

In order to achieve smooth key transition, KeyStartAccept SHOULD be less than KeyStartGenerate and KeyStopGenerate SHOULD be less than KeyStopAccept. If KeyStartGenerate or KeyStartAccept are left unspecified, the time will default to 0 and the key will be used immediately. If KeyStopGenerate or KeyStopAccept are left unspecified, the time will default to infinity and the key's lifetime will be infinite. When a new key replaces an old, the KeyStartGenerate time for the new key MUST be less than or equal to the KeyStopGenerate time of the old key.

Key storage SHOULD persist across a system restart, warm or cold, to avoid operational issues. In the event that the last key associated with an interface expires, it is unacceptable to revert to an unauthenticated condition, and not advisable to disrupt routing. Therefore, the router SHOULD send a "last Authentication Key expiration" notification to the network manager and treat the key as having an infinite lifetime until the lifetime is extended, the key is deleted by network management, or a new key is configured

4. Authentication Procedure

4.1. Authentication Trailer

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

```
     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
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |              Auth Type         |         Auth Data Len        |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                Security Association ID (SA ID)                |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |           Cryptographic Sequence Number (High Order 32 Bits)  |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |           Cryptographic Sequence Number (Low Order 32 Bits)   |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                                                               |
    |                Authentication Data (Variable)                 |
    ~                                                               ~
    |                                                               |
    |                                                               |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

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 - HMAC Cryptographic Authentication as described herein.

o Auth Data Len

The length in octets of the Authentication Trailer (AT) including both the 16 octet fixed header and the variable length message digest.

o Security Association Identifier (SA ID)

32-bit field that maps to the authentication algorithm and the

secret key used to create the message digest appended to the OSPFv3 protocol packet.

Though the SA ID implicitly implies the algorithm, the HMAC output size should not be used by implementers as an implicit hint because additional algorithms may be defined in the future that have the same output size.

o 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 OSPFv3 packet sent by the OSPFv3 router. Upon reception, the sequence number MUST be greater than the sequence number in the last OSPFv3 packet accepted from the sending OSPFv3 neighbor. Otherwise, the OSPFv3 packet is considered a replayed packet and dropped.

OSPFv3 routers implementing this specification MUST use available mechanisms to preserve the sequence number's strictly increasing property for the deployed life of the OSPFv3 router (including cold restarts). One mechanism for accomplishing this would be to use the high order 32 bits of the sequence number as a wrap/boot count that is incremented anytime the OSPFv3 router loses its sequence number state. Sequence number wrap is described in Section 4.1.1.

o Authentication Data

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

4.1.1. Sequence Number Wrap

When incrementing the sequence number for each transmitted OSPFv3 packet, the sequence number should be treated as an unsigned 64-bit value. If the lower order 32-bit value wraps, the higher order 32-bit value should be incremented and saved in non-volatile storage. If by some chance the OSPFv3 router is deployed long enough that there is a possibility that the 64-bit sequence number may wrap, all keys, independent of key distribution mechanism, MUST be reset to avoid the possibility of replay attacks. Once the keys have been changed, the higher order sequence number can be reset to 0 and saved to non-volatile storage.

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:

- o 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.

- o For received OSPFv3 packets including an OSPFv3 Authentication Trailer, OSPFv3 header checksum verification MUST be omitted. However, if the OSPFv3 packet does include a non-zero OSPFv3 header checksum, it will not be modified by the receiver and will simply be included in the OSPFv3 Authentication Trailer message digest verification.

4.3. Cryptographic Authentication Procedure

As noted earlier, the SA ID maps to the authentication algorithm and > the secret key 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-256 and SHOULD include support for HMAC-SHA-1 and MAY also include support for HMAC-SHA-384 and HMAC-SHA-512.

Implementations of this standard MUST use HMAC-SHA-256 as the default authentication algorithm.

4.4. Cross Protocol Attack Mitigation

In order to prevent cross protocol replay attacks for protocols sharing common keys, the two octet OSPFv3 Cryptographic Protocol ID is appended to the authentication key prior to use. Other protocols using cryptographic authentication as specified herein MUST similarly append their respective Cryptographic Protocol IDs to their keys in this step. Refer to IANA Considerations (Section 7).

4.5. 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 from the OSPFv3 security association.

Ks is a Protocol Specific Authentication Key obtained by appending Authentication Key (K) with the two-octet OSPFv3 Cryptographic Protocol ID appended.

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 a value which is the same length as the hash output or message digest. The first 16 octets contain the IPv6 source address followed by the hexadecimal value 0x878FE1F3 repeated (L-16)/4 times. This implies that hash output is always a length of at least 16 octets.

1. Preparation of the Key

   The OSPFv3 Cryptographic Protocol ID is appended to the Authentication Key (K) yielding a Protocol Specific Authentication Key (Ks). In this application, Ko is always L octets long, and is computed as follows:

   If the Protocol Specific Authentication Key (Ks) is L octets long, then Ko is equal to K. If the Protocol Specific Authentication Key (Ks) is more than L octets long, then Ko is

   set to H(Ks). If the Protocol Specific Authentication Key (Ks) is less than L octets long, then Ko is set to the Protocol Specific Authentication Key (Ks) with zeros appended to the end of the Protocol Specific Authentication Key (Ks) such that Ko is L octets long.

2. First Hash

   First, the OSPFv3 packet's Authentication Data field in the 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, 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 OSPFv3 Authentication Trailer.

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

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.

4.6. 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.

If the cryptographic sequence number in the AT is less than or equal to the last sequence number successfully received from the neighbor, the OSPFv3 packet MUST be dropped and an error event SHOULD be

logged.

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 (as described in Section 4.5). 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.

After the OSPFv3 packet has been successfully authenticated, implementations MUST store the 64-bit cryptographic sequence number for future replay checks.

5. Migration and Backward Compatibility

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.

In support of uninterrupted deployment, an OSPFv3 router implementing this standard MAY implement 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 document.

6. Security Considerations

The document proposes extensions to OSPFv3 that 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 addresses all the security issues that have been identified in [RFC6039].

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 that had 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 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.

Refer to [RFC4552] for additional considerations on manual keying.

7. IANA Considerations

IANA is requested to allocate an AT-bit in the "OSPFv3 Options Registry" as described in Section 2.1.

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

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

OSPFv3 Authentication Types

Finally, IANA is requested to create new general registry "Cryptographic Protocol ID". This new registry will provide unique protocol specific values for cryptographic applications, such as but not limited to, prevention of cross protocol replay attacks. Values can be assigned for both native IPv4/IPv6 protocols and UDP/TCP

protocols.

Value/Range	Designation	Assignment Policy
0	Reserved	Reserved
1	OSPFv3	Already assigned
2-65535	Unassigned	Standards Action

Cryptographic Protocol ID

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.

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

[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.

[I-D.ietf-ospf-security-extension-manual-keying]
Bhatia, M., Hartman, S., Zhang, D., and A. Lindem, "Security Extension for OSPFv2 when using Manual Key Management", draft-ietf-ospf-security-extension-manual-keying-01 (work in progress), October 2011.

[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.

[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.

[RFC6234] Eastlake, D. and T. Hansen, "US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)", RFC 6234, May 2011.

Appendix A. Acknowledgments

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

Thanks to Sam Hartman for discussions on replay mitigation and the use of a 64-bit strictly increasing sequence number. Also, thanks to Sam for comments during IETF last call with respect to the OSPFv3 SA and sharing of key between protocols.

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 Uma Chunduri for suggesting that we may want to protect the IPv6 source address even though OSPFv3 uses the Router ID for neighbor identification.

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. Also, thanks to Alan for WG last call comments.

Thanks to Alia Atlas for comments made under the purview of the Routing Directorate review.

Thanks to Stephen Farrell for comments during the IESG review. Stephen was also involved in the discussion of cross protocol attacks.

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 Manral
Hewlett Packard
USA

Phone:
Email: vishwas.manral@hp.com

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

Phone:
Email: acee.lindem@ericsson.com