Network Working Group **Manav Bhatia**
Internet Draft **Alcatel-Lucent**
Intended Status: Proposed Standard **Vishwas Manral**
Expires: April 2009 IP Infusion
Tony Li
Redback Networks Inc.
Randall J. Atkinson
Extreme Networks
Russ White
Cisco Systems
Matthew J. Fanto
Ciber Inc.

IS-IS Generic Cryptographic Authentication

draft-ietf-isis-hmac-sha-07.txt

Status of this Memo

Abstract

This document proposes an extension to Intermediate System to Intermediate System (IS-IS) to allow the use of any cryptographic authentication algorithm in addition to the already documented authentication schemes, described in the base specification and RFC 5304. IS-IS is specified in International Standards Organization

(ISO) 10589, with extensions to support Internet Protocol version 4 (IPv4) described in RFC 1195.

Although this document has been written specifically for using the Hashed Message Authentication Code (HMAC) construct along with the Secure Hash Algorithm (SHA) family of cryptographic hash functions, the method described in this document is generic and can be used to extend IS-IS to support any cryptographic hash function in the future.

Conventions used in this document

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]

Contents

1. Introduction

Intermediate System to Intermediate System (IS-IS) specification [ISO] [RFC1195] allows for authentication of its Protocol Data Units (PDUs) via the authentication TLV 10 that is carried as a part of the PDU. The base specification has provision for only clear text passwords and RFC 5304 [RFC5304] augments this to provide the capability to use Hashed Message Authentication Code - Message Digest 5 (HMAC-MD5) authentication for its PDUs.

The first octet of the value field of TLV 10 specifies the type of authentication to be carried out. Type 0 is reserved, Type 1 indicates a cleartext password, Type 54 indicates HMAC MD5 and Type

255 is used for routing domain private authentication methods. The remainder of the value field contains the actual authentication data determined by the value of the authentication type.

This document proposes a new authentication type to be carried in TLV 10, called the generic cryptographic authentication (CRYPTO_AUTH). This can be used to specify any authentication algorithm for authenticating and verifying IS-IS PDUs.

This document also explains how HMAC-SHA authentication can be used in IS-IS.

By definition, HMAC [RFC2104] requires a cryptographic hash function. We propose to use any one of SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512 [FIPS-180-3] for this purpose to authenticate the IS-IS PDUs.

We propose to do away with the per interface keys and instead have key IDs that map to unique IS-IS Security Associations (SA).

While at the time of this writing there are no openly published attacks on the HMAC-MD5 mechanism, some reports [Dobb96a, Dobb96b] create concern about the ultimate strength of the MD5 cryptographic hash function.

The mechanism described in this document does not provide confidentiality, since PDUs are sent in the clear. However, the objective of a routing protocol is to advertise the routing topology, and confidentiality is not normally required for routing protocols.

2. IS-IS Security Association

An IS-IS Security Association contains a set of parameters shared between any two legitimate IS-IS speakers.

Parameters associated with an IS-IS SA:

O Key Identifier (Key ID) : This is a two octet unsigned integer used to uniquely identify an IS-IS SA, as manually configured by the network operator.

The receiver determines the active SA by looking at the Key ID field in the incoming PDU.

The sender based on the active configuration, selects the Security Association to use and puts the correct Key ID value associated with the Security Association in the IS-IS PDU. If multiple valid and active IS-IS Security Associations exist for a given outbound interface at the time an IS-IS PDU is sent, the sender may use any of those security associations 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 multiple authentication mechanisms to be used at various times without disrupting an IS-IS peering, including the introduction of new authentication mechanisms.

o Authentication Algorithm : This signifies the authentication algorithm to be used with the IS-IS 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-224, HMAC-SHA-256, HMAC-SHA-384 and HMAC-SHA-512.

o Authentication Key : This value denotes the cryptographic authentication key associated with the IS-IS SA. The length of this key is variable and depends upon the authentication algorithm specified by the IS-IS SA.

3. Authentication Procedures

3.1 Authentication TLV

A new authentication code, 3, indicates the CRYPTO_AUTH mechanism described in this document is in use, is inserted in the first octet of the existing IS-IS Authentication TLV (10).

```
  0                   1
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |     Type 10   |     Length    |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |   Auth Type   |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |            Key ID             |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |                               |
  +                               +
  | Authentication Data (Variable)|
  +                               +
  |                               |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 1

3.2 Authentication Process

When calculating the CRYPTO_AUTH result for Sequence Number PDUs, Level 1 Sequence Number PDUs SHALL use the Area Authentication string as in Level 1 Link State PDUs. Level 2 Sequence Number PDUs shall use the domain authentication string as in Level 2 Link State PDUs.

IS-IS HELLO PDUs SHALL use the Link Level Authentication String, which MAY be different from that of Link State PDUs. The CRYPTO_AUTH result for the IS-IS HELLO PDUs SHALL be calculated after the PDU is padded to the MTU size, if padding is not disabled. Implementations that support the optional checksum for the Sequence Number PDUs and IS-IS HELLO PDUs MUST NOT include the Checksum TLV.

3.3 Cryptographic Aspects

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

H   is the specific hashing algorithm (e.g. SHA-256).
K   is the password for the PDU type as per the International Standard ISO/IEC 10589 [ISO].
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.

(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 IS-IS packet's Authentication Data field is filled with the value Apad and the Authentication Type field is set to 0x3.

Then, a first hash, also known as the inner hash, is computed as follows:

```
        First-Hash = H(Ko XOR Ipad || (IS-IS PDU))
```

(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 result Second-Hash becomes the Authentication Data that is sent in the Authentication Data field of the IS-IS PDU. 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.

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

3.4 Procedures at the Sending Side

An appropriate IS-IS SA is selected for use with an outgoing IS-IS PDU. This is done based on the active key at that instant. If IS-IS is unable to find an active key, then the PDU is discarded.

If IS-IS is able to find the active key, then the key gives the authentication algorithm (HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384 or HMAC-SHA-512) that needs to be applied on the PDU.

An implementation MUST fill the authentication type and the length before the authentication data is computed. The authentication data is computed as explained in the previous section. The length of the TLV is set as per the authentication algorithm that is being used.

The length is set to 23 for HMAC-SHA-1, 31 for HMAC-SHA-224, 35 for HMAC-SHA-256, 51 for HMAC-SHA-384 and 67 for HMAC-SHA-512. Note that two octets have been added to account for the Key ID and one octet for the authentication type.

The key ID is filled.

The Checksum and Remaining Life time fields are set to Zero for the LSPs before authentication is calculated.

The result of the authentication algorithm is placed in the Authentication data, following the key ID.

The authentication data for the IS-IS IIH PDUs MUST be computed after the IIH has been padded to the MTU size, if padding is not explicitly disabled.

3.5 Procedure at the Receiving Side

The appropriate IS-IS SA is identified by looking at the Key ID from the Authentication TLV 10 from the incoming IS-IS PDU.

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

Before an implementation performs any processing it needs to save the values of the Authentication Value field, the Checksum and the Remaining Life time.

It should then set the Authentication Value field with Apad and zero the Checksum and Remaining Life time fields before the authentication data is computed. The calculated data is compared with the received authentication data in the PDU and the PDU is 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 CRYPTO_AUTH information in the PDUs but does not verify this information. This is provided as a transition aid for networks in the

process of migrating to the new CRYPTO_AUTH based authentication schemes.

4. Security Considerations

The document proposes extensions to IS-IS 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 PDUs 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 PDU, but is rather being used to confirm that the PDU has indeed been issued by an intermediate system which had access to the area or the domain password, depending upon the kind of PDU it is.

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 IS-IS protocol, while not causing undue implementation, deployment, or operational complexity.

The mechanism detailed in this document does not protect IS-IS against replay attacks. An adversary could in theory replay old IIHs and bring down the adjacency [CRYPTO] or replay old CSNPs and PSNPs that would cause a flood of LSPs in the network. Using some sort of crypto sequence numbers in IS-IS IIHs and CSNP/PSNPs is an option to solve this problem. Discussing this is beyond the scope of this document.

This document states that the remaining lifetime of the LSP MUST be set to zero before computing the authentication, thus this field is not authenticated. This field is excluded so that the LSPs may be aged by the ISes in between without requiring to recompute the authentication data. This can be exploited by an attacker.

There is a transition mode suggested where routers can ignore the CRYPTO_AUTH information carried in the PDUs. The operator must ensure that this mode is only used when migrating to the new CRYPTO_AUTH based authentication scheme as this leaves the router vulnerable to an attack.

To ensure greater security, the keys used should be changed periodically and implementations MUST be able to store and use more than one key at the same time. Operators should ensure that the authentication key is never sent over the network in clear-text via any protocol. Care should also be taken to ensure that the selected key is unpredictable, avoiding any keys known to be weak for the

algorithm in use. [RFC4086] contains helpful information on both key generation techniques and cryptographic randomness.

It should be noted that the cryptographic strength of the HMAC depends upon the cryptographic strength of the underlying hash function and on the size and quality of the key.

If a stronger authentication were believed to be required, then the use of a full digital signature [RFC2154] would be an approach that should be seriously considered. It was rejected for this purpose at this time because the computational burden of full digital signatures is believed to be much higher than is reasonable given the current threat environment in operational commercial networks.

5. Acknowledgements

The authors would like to thank Hugo Krawczyk, Arjen K. Lenstra (Bell Labs) and Eric Grosse (Bell Labs) for educating us on some of the finer points related to Crypto Mathematics.

We would also like to thank Bill Burr, Tim Polk, John Kelsey, and Morris Dworkin of (US) NIST for review of portions of this document that are directly derived from the closely related work on RIPv2 Cryptographic Authentication [RFC-4822].

We would also like to mention Alfred Hoenes for his careful and detailed review during the last call.

6. IANA Considerations

Upon publication of this RFC, IANA shall register the pre-allocated value for the CRYPTO_AUTH method in the "IS-IS Authentication Type Codes for TLV 10" subregistry established by [RFC5304].

This document currently defines the value 3 to be used to denote the CRYPTO_AUTH mechanism for authenticating IS-IS PDUs.

Authentication Type Code	Value	Reference
Cryptographic Authentication (CRYPTO_AUTH)	3	RFC {this}

7. References

7.1 Normative References

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

[ISO] "Intermediate system to Intermediate system routeing information exchange protocol for use in conjunction with the Protocol for providing the Connectionless-mode Network Service (ISO 8473)", ISO/IEC 10589:1992

[RFC1195] Callon, R., "Use of OSI IS-IS for routing in TCP/IP and dual environments", RFC 1195, December 1990.

[RFC5304] Li, T. and Atkinson, R. "Intermediate System to Intermediate System (IS-IS) Cryptographic Authentication", RFC 5304, October 2008.

[RFC2104] Krawczyk, H. et al., "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997

[FIPS-180-3] National Institute of Standards and 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.

7.2 Informative References

[Dobb96a] Dobbertin, H, "Cryptanalysis of MD5 Compress", Technical Report, 2 May 1996. (Presented at the Rump Session of EuroCrypt 1996.)

[Dobb96b] Dobbertin, H, "The Status of MD5 After a Recent Attack", CryptoBytes, Vol. 2, No. 2, Summer 1996.

[CRYPTO] Manral, V. et al., "Issues with existing Cryptographic Protection Methods for Routing Protocols", Work in Progress, February 2006

[RFC2154] S. Murphy, M. Badger, and B. Wellington, "OSPF with Digital Signatures", RFC 2154, June 1997.

[RFC4822] R. Atkinson, M. Fanto, "RIPv2 Cryptographic Authentication", RFC 4822, February 2007.

8. Author's Addresses

Manav Bhatia
Alcatel-Lucent
Bangalore, India
Email: manav@alcatel-lucent.com

Tony Li
Redback Networks Inc.
300 Holger Way
San Jose CA 95134
USA
EMail: tony.li@tony.li

Vishwas Manral
IP Infusion
Almora, Uttarakhand
India
Email: vishwas@ipinfusion.com

Russ White
Cisco Systems
RTP North Carolina
USA
Email: riw@cisco.com

Randall J. Atkinson
Extreme Networks
3585 Monroe Street
Santa Clara, CA 95051
USA
Email: rja@extremenetworks.com

Matthew J. Fanto
Ciber Inc.
Dearborn, Mi
USA
Email: mfanto@ciber.com

Full Copyright Statement

Intellectual Property