Network Working Group
INTERNET DRAFT

Tony Li
Juniper Networks
January 1999

IS-IS HMAC-MD5 Authentication

<draft-ietf-isis-hmac-00.txt>

Status

1.0 Abstract

This document describes the authentication of IS-IS PDUs using the HMAC-MD5 algorithm [1]. IS-IS is specified in [2], with extensions to support IPv4 described in [3]. The base specification includes an authentication mechanism that allows for multiple authentication algorithms. The base specification only specifies the algorithm for cleartext passwords.

This document proposes an extension to that specification that allows the use of the HMAC-MD5 authentication algorithm to be used in conjunction with the existing authentication mechanisms.

2.0 Introduction

The IS-IS protocol, as specified in ISO 10589, provides for the authentication of Link State PDUs (LSPs) through the inclusion of authentication information as part of the LSP. This authentication information is encoded as a Type-Length-Value (TLV) tuple. The type of the TLV is specified as 10. The length of the TLV is variable. The value of the TLV depends on the authentication algorithm and

related secrets being used. The first octet of the value is used to specify the authentication type. Type 0 is reserved, type 1 indicates a cleartext password, and type 255 is used for routing domain private authentication methods. The remainder of the TLV value is known as the Authentication Value.

This document extends the above situation by allocating a new authentication type for HMAC-MD5 and specifying the algorithms for the computation of the Authentication Value. This document also describes modifications to the base protocol to insure that the authentication mechanisms described in this document are effective.

This document is a publication of the IS-IS Working Group within the IETF, and is a contribution to ISO IEC JTC1/SC6, for eventual inclusion with ISO 10589.

3.0 Authentication Procedures

The authentication type used for HMAC-MD5 is 54 (0x36). The length of the Authentication Value for HMAC-MD5 is 16, and the length field in the TLV is 17.

The HMAC-MD5 algorithm requires a key K and text T as input. The key K is the password for the PDU type, as specified in ISO 10589. The text T is the PDU to be authenticated with the Authentication Value field inside of the Authentication Information TLV set to zero. Note that the Authentication Type is set to 54 and the length of the TLV is set to 17 before authentication is computed. When LSPs are authenticated, the Checksum and Remaining Lifetime fields are set to zero (0) before authentication is computed. The result of the algorithm is placed in the Authentication Value field.

An implementations that implements HMAC-MD5 authentication and receives HMAC-MD5 Authentication Information MUST discard the PDU if the Authentication Value is incorrect.

An implementation MAY include HMAC-MD5 Authentication Information in PDUs even if it does not fully implement HMAC-MD5 authentication. This allows an implementation to generate authentication information without verifying the authentication information. This is a transition aid for networks in the process of deploying authentication.

An implementation MAY check a set of passwords when verifying the Authentication Value. This provides a mechanism for incrementally changing passwords in a network.

An implementation that does not implement HMAC-MD5 authentication MAY accept a PDU that contains the HMAC-MD5 Authentication Type.

ISes (routers) that implement HMAC-MD5 authentication and initiating LSP purges MUST remove the body of the LSP and add the authentication TLV. ISes MUST NOT accept unauthenticated purges. ISes MUST NOT accept purges that contain TLVs other than the authentication TLV. These restrictions are necessary to prevent a hostile system from receiving an LSP, setting the Remaining Lifetime field to zero, and flooding it, thereby initiating a purge without knowing the authentication password.

4.0 Security Considerations

This document enhances the security of the IS-IS routing protocol. Because a routing protocol contains information that is not of significant value, privacy is not a requirement. However, authentication of the messages within the protocol is of interest.

The technology in this document provides an authentication mechanism for IS-IS. This mechanism does not prevent replay attacks, however such attacks would trigger mechanisms in the protocol that would effectively reject old information. This document does not address denial-of-service attacks.

5.0 Acknowledgments

The author would like to thank Henk Smit, Dave Katz and Tony Przygienda for their comments on this work.

6.0 References

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

[2] ISO 10589, "Intermediate System to Intermediate System Intra-Domain Routeing Exchange Protocol for use in Conjunction with the Protocol for Providing the Connectionless-mode Network Service (ISO 8473)" [Also republished as RFC 1142]

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

10.0 Author's Address

Tony Li
Juniper Networks, Inc.
385 Ravendale Dr.
Mountain View, CA 94043

Email: tli@juniper.net
Fax: +1 650 526 8001
Voice: +1 650 526 8006