Network Working Group
Request for Comments: 3567
Category: Informational

T. Li
Procket Networks
R. Atkinson
Extreme Networks

July 2003

Intermediate System to Intermediate System (IS-IS) Cryptographic Authentication

Status of this Memo

Copyright Notice

Abstract

This document describes the authentication of Intermediate System to Intermediate System (IS-IS) Protocol Data Units (PDUs) using the Hashed Message Authentication Codes - Message Digest 5 (HMAC-MD5) algorithm as found in RFC 2104. IS-IS is specified in International Standards Organization (ISO) 10589, with extensions to support Internet Protocol version 4 (IPv4) described in RFC 1195. 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.

1. Introduction

The IS-IS protocol, as specified in ISO 10589 [1], 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 use of IS-IS for IPv4 networks is described in [3].

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 ensure 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.

2. 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 [2]. The key K is the password for the PDU type, as specified in ISO 10589. The text T is the IS-IS 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.

When calculating the HMAC-MD5 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 HMAC-MD5 result for the IS-IS HELLO PDUs SHALL be calculated after the Packet 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.

To authenticate an incoming PDU, a system should save the values of the Authentication Value field, the Checksum and the Remaining Lifetime field, set these fields to zero, compute authentication, and then restore the values of these fields.

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

An implementation MAY have a transition mode where it includes HMAC-MD5 Authentication Information in PDUs but does not verify the HMAC-MD5 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 initiate LSP purges MUST remove the body of the LSP and add the authentication TLV. ISes implementing HMAC-MD5 authentication 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.

2.1 Implementation Considerations

There is an implementation issue just after password rollover on an IS-IS router that might benefit from additional commentary. Immediately after password rollover on the router, the router or IS-IS process may restart. If this happens, this causes the LSP Sequence Number restarts from the value 1 using the new password. However, neighbors will reject those new LSPs because the Sequence Number is smaller. The router can not increase its own LSP Sequence Number because it fails to authenticate its own old LSP that neighbors keep sending to it. So the router can not update its LSP Sequence Number to its neighbors until all the neighbors time out all of the original LSPs. One possible solution to this problem is for the IS-IS process to detect if any inbound LSP with an authentication failure has the local System ID and also has a higher Sequence Number than the IS-IS process has. In this event, the IS-IS process SHOULD increase its own LSP Sequence Number accordingly and re-flood the LSPs. However, as this scenario could also be triggered by an active attack by an adversary, it is recommended that a counter also be kept on this case to mitigate the risk from such an active attack.

3. Security Considerations

This document enhances the security of the IS-IS routing protocol. Because a routing protocol contains information that need not be kept secret, privacy is not a requirement. However, authentication of the messages within the protocol is of interest, to reduce the risk of an adversary compromising the routing system by deliberately injecting false information into the routing system.

The technology in this document provides an authentication mechanism for IS-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.

This mechanism does not prevent replay attacks, however, in most cases, such attacks would trigger existing mechanisms in the IS-IS protocol that would effectively reject old information. Denial of service attacks are not generally preventable in a useful networking protocol [4].

Changes to the authentication mechanism described here (primarily: to add a Key-ID field such as OSPFv2 and RIPv2 have) were considered at some length, but ultimately were rejected. The mechanism here was already widely implemented in 1999. As of this writing, this mechanism is fairly widely deployed within the users interested in cryptographic authentication of IS-IS. The improvement provided by the proposed revised mechanism was not large enough to justify the change, given the installed base and lack of operator interest in deploying a revised mechanism.

If and when a key management protocol appears that is both widely implemented and easily deployed to secure routing protocols such as IS-IS, a different authentication mechanism that is designed for use with that key management schema could be added if desired.

If a stronger authentication were believed to be required, then the use of a full digital signature [5] 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.

Acknowledgements

The authors would like to thank (in alphabetical order) Dave Katz, Steven Luong, Tony Przygienda, Nai-Ming Shen, and Henk Smit for their comments and suggestions on this document.

Normative References

[1] ISO, "Intermediate System to Intermediate System Routing Information Exchange Protocol for use in Conjunction with the Protocol for Providing the Connectionless-mode Network Service (ISO 8473)", ISO/IEC 10589:2002, Second Edition.

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

Informative References

[3] Callon, R., "Use of OSI IS-IS for Routing in TCP/IP and Dual environments", RFC 1195, December 1990.

[4] Voydock, V. and S. Kent, "Security Mechanisms in High-level Networks", ACM Computing Surveys, Vol. 15, No. 2, June 1983.

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

Authors' Addresses

Tony Li
Procket Networks
1100 Cadillac Ct.
Milpitas, CA 95035 USA

Phone: +1 (408) 635-7903
EMail: tli@procket.net

Ran J. Atkinson
Extreme Networks
3585 Monroe Street
Santa Clara, CA 95051 USA

Phone: +1 (408) 579-2800
EMail: rja@extremenetworks.com

Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.