Network Working Group
Request for Comments: 5304
Obsoletes: 3567
Updates: 1195
Category: Standards Track

T. Li
Redback Networks, Inc.
R. Atkinson
Extreme Networks, Inc.

October 2008

IS-IS Cryptographic Authentication

Status of This Memo

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 replaces RFC 3567.

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.

Table of Contents

1. Introduction 3
2. Authentication Procedures 3
2.1. Implementation Considerations 5
3. Security Considerations 5
3.1. Security Limitations 5
3.2. Assurance 6
3.3. Key Configuration 6
3.4. Other Considerations 7
3.5. Future Directions 7
4. IANA Considerations 7
5. Acknowledgements 8
6. References 8
6.1. Normative References 8
6.2. Informative References 9

1. Introduction

The IS-IS protocol, as specified in [ISO-10589], provides for the authentication of Link State Protocol Data Units (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 [RFC1195].

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. This document replaces [RFC3567], which is an Informational RFC. This document is on the Standards Track. This document has revised Section 3, with the significant addition of a discussion of recent attacks on MD5 in Section 3.2. This document has also added a substantive "IANA Considerations" section to create a missing codepoint registry.

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].

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 [RFC2104]. 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 field, 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 that occurs just after password rollover on an IS-IS router and 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 to restart from the value 1 using the new password. However, neighbors will reject those new LSPs because the Sequence Number is smaller. The router cannot increase its own LSP Sequence Number because it fails to authenticate its own old LSP that neighbors keep sending to it. So the router cannot 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 be kept on this case to mitigate the risk from such an 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 in order to reduce the risk of an adversary compromising the routing system by deliberately injecting false information into that system.

3.1. Security Limitations

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. It provides improved security against passive attacks, as defined in [RFC1704], when compared to cleartext password authentication.

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 [DoS].

The mechanisms in this document do not provide protection against compromised, malfunctioning, or misconfigured routers. Such routers can, either accidentally or deliberately, cause malfunctions that affect the whole routing domain. The reader is encouraged to consult [RFC4593] for a more comprehensive description of threats to routing protocols.

3.2. Assurance

Users need to understand that the quality of the security provided by this mechanism depends completely on the strength of the implemented authentication algorithms, the strength of the key being used, and the correct implementation of the security mechanism in all communicating IS-IS implementations. This mechanism also depends on the IS-IS Authentication Key being kept confidential by all parties. If any of these are incorrect or insufficiently secure, then no real security will be provided to the users of this mechanism.

Since Dobbertin's attacks on MD5 [Dobb96a] [Dobb96b] [Dobb98] were first published a dozen years ago, there have been growing concerns about the effectiveness of the compression function within MD5. More recent work by Wang and Yu [WY05] accentuates these concerns. However, despite these research results, there are no published attacks at present on either Keyed-MD5 or HMAC-MD5. A recent paper by Bellare [Bell06a] [Bell06b] provides new proofs for the security of HMAC that require fewer assumptions than previous published proofs for HMAC. Those proofs indicate that the published issues with MD5 (and separately with SHA-1) do not create an attack on HMAC-MD5 (or HMAC SHA-1). Most recently, Fouque and others [FLN07] have published new attacks on NMAC-MD4, HMAC-MD4, and NMAC-MD5. However, their attacks are non-trivial computationally, and they have not found an equivalent attack on HMAC-MD5. So, despite the published issues with the MD5 algorithm, there is currently no published attack that applies to HMAC-MD5 as used in this IS-IS specification. As with any cryptographic technique, there is the possibility of the discovery of future attacks against this mechanism.

3.3. Key Configuration

It should be noted that the key configuration mechanism of routers may restrict the possible keys that may be used between peers. It is strongly recommended that an implementation be able to support, at minimum, a key composed of a string of printable ASCII of 80 bytes or less, as this is current practice.

3.4. Other Considerations

Changes to the authentication mechanism described here (primarily: to add a Key-ID field such as that of OSPFv2 and RIPv2) 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.

3.5. Future Directions

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.

If and when additional authentication mechanisms are defined (for example, to provide a cryptographically stronger hash function), it will also be necessary to define mechanisms that allow graceful transition from the existing mechanisms (as defined in this document) to any future mechanism.

4. IANA Considerations

IANA has created a new codepoint registry to administer the Authentication Type codepoints for TLV 10. This registry is part of the existing IS-IS codepoints registry as established by [RFC3563] and [RFC3359]. This registry is managed using the Designated Expert policy as described in [RFC5226] and is called "IS-IS Authentication Type Codes for TLV 10".

The values in the "IS-IS Authentication Type Codes for TLV 10" registry should be recorded in decimal and should only be approved after a designated expert, appointed by the IESG area director, has been consulted. The intention is that any allocation will be accompanied by a published RFC. However, the designated expert can approve allocations once it seems clear that an RFC will be published, allowing for the allocation of values prior to the

document being approved for publication as an RFC. New items should be documented in a publicly and freely available specification. We should also allow external specifications to allocate and use the IS-IS Authentication Type Codes maintained by this registry.

Initial values for the "IS-IS Authentication Type Codes for TLV 10" registry are given below; future assignments are to be made through Expert Review. Assignments consist of an authentication type name and its associated value.

Authentication Type Code	Value	Reference
Reserved	0	[ISO-10589]
Cleartext Password	1	[ISO-10589]
ISO 10589 Reserved	2	[ISO-10589]
HMAC-MD5 Authentication	54	RFC 5304
Routeing Domain private authentication method	255	[ISO-10589]

5. Acknowledgements

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

6. References

6.1. Normative References

[ISO-10589] ISO, "Intermediate System to Intermediate System intra-domain routeing information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode network service (ISO 8473)", International Standard 10589:2002, Second Edition, 2002.

[RFC2104] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

6.2. Informative References

[Bell06a] Bellare, M., "New Proofs for NMAC and HMAC: Security without Collision-Resistance", Preliminary Version, in Proceedings of Crypto 2006, Lecture Notes in Computer Science, Vol. 4117, August 2006.

[Bell06b] Bellare, M., "New Proofs for NMAC and HMAC: Security without Collision-Resistance", August 2006, <http://www-cse.ucsd.edu/users/mihir/papers/hmac-new.html>.

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

[Dobb96a] Dobbertin, H., "Cryptanalysis of MD5 Compress", EuroCrypt Rump Session 1996, May 1996.

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

[Dobb98] Dobbertin, H., "Cryptanalysis of MD4", Journal of Cryptology, Vol. 11, No. 4, 1998.

[FLN07] Fouque, P., Leurent, G., and P. Nguyen, "Full Key-Recovery Attacks on HMAC/NMAC-MD5 and NMAC-MD5", Proceedings of Crypto 2007, August 2007.

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

[RFC1704] Haller, N. and R. Atkinson, "On Internet Authentication", RFC 1704, October 1994.

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

[RFC3359] Przygienda, T., "Reserved Type, Length and Value (TLV) Codepoints in Intermediate System to Intermediate System", RFC 3359, August 2002.

[RFC3563] Zinin, A., "Cooperative Agreement Between the ISOC/IETF and ISO/IEC Joint Technical Committee 1/Sub Committee 6 (JTC1/SC6) on IS-IS Routing Protocol Development", RFC 3563, July 2003.

[RFC3567] Li, T. and R. Atkinson, "Intermediate System to Intermediate System (IS-IS) Cryptographic Authentication", RFC 3567, July 2003.

[RFC4593] Barbir, A., Murphy, S., and Y. Yang, "Generic Threats to Routing Protocols", RFC 4593, October 2006.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

[WY05] Wang, X. and H. Yu, "How to Break MD5 and Other Hash Functions", Proceedings of EuroCrypt 2005, Lecture Notes in Computer Science, Vol. 3494, 2005.

Authors' Addresses

Tony Li
Redback Networks, Inc.
300 Holger Way
San Jose, CA 95134
USA

Phone: +1 408 750 5160
EMail: tony.li@tony.li

R. Atkinson
Extreme Networks, Inc.
3585 Monroe St.
Santa Clara, CA 95051
USA

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

Full Copyright Statement

Intellectual Property