Network Working Group **Manav Bhatia**
Internet Draft **Alcatel-Lucent**
Expires: September 2007 **Vishwas Manral**
IP Infusion

Cryptographic Algorithm Implementation Requirements for IS-IS

draft-bhatia-manral-crypto-req-isis-01.txt

Status of this Memo

Abstract

IS-IS currently defines two different kinds of authentication schemes: Clear Text password and HMAC-MD5. There has been recently a new draft submitted that adds support for a generic cryptographic authentication scheme, which can make use of different cryptographic algorithms in order to authenticate the IS-IS PDUs.

To ensure interoperability between disparate implementations, it is imperative that we specify a set of mandatory-to-implement algorithms to ensure that there is at least one algorithm that all implementations will have available.

This document defines the current set of mandatory-to-implement algorithms to be used for the cryptographic authentication for IS-IS

as well as specifying the algorithms that should be implemented because they may be promoted to mandatory at some future time.

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 [KEYWORDS]

1. Introduction

IS-IS [ISO] [RFC1195] specification allows for authentication of its PDUs via the authentication TLV 10 that is carried as the part of the PDU. The base spec has provision for only clear text passwords and RFC 3567 [RFC3567] augments this to provide the capability to use HMAC-MD5 authentication for its PDUs.

In the clear text password scheme of authentication, the passwords are exchanged in the clear text on the network and anyone with physical access to the network can learn the password and compromise the security of the IS-IS domain.

The HMAC-MD5 scheme is also not good enough as there have recently been reports about attacks on the collision resistance properties of MD5 [MD5-attack]. MD5CRK, was a distributed computing project to break the MD5 hash algorithm in a short period of time. The project closed down with the publication of the paper [MD5-attack].

It was discovered that collisions can be found in MD5 algorithm in less than 24 hours, making MD5 very insecure. Further research has verified this result and shown other ways to find collisions in MD5 hashes. We thus need to move away from MD5 towards more complex and difficult to break hash algorithms.

The [ISIS-HMAC] document recently submitted in the IETF addresses this. It is imperative that we move away from using MD5 to something that s cryptographically more stronger (like HMAC-SHA-1).

However, the nature of cryptography is that new algorithms surface continuously and existing algorithms are continuously attacked. An algorithm believed to be strong today may be demonstrated to be weak tomorrow. Given this, the choice of mandatory-to-implement algorithm should be conservative so as to minimize the likelihood of it being compromised quickly.

Also, we need to recognize that the mandatory-to-implement algorithm(s) may need to change over time to adapt to the changing world. For this reason, the selection of mandatory-to-implement algorithms should not be included in the base IS-IS specification.

This way it is only this document that needs to get updated, whenever there is a need to update the status of mandatory-to-implement authentication algorithms.

2. Requirements Terminology

Keywords "MUST", "MUST NOT", "REQUIRED", "SHOULD", "SHOULD NOT" and "MAY" that appear in this document are to be interpreted as described in [RFC2119].

We define some additional terms here:

SHOULD+	This term means the same as SHOULD. However, it is likely that an algorithm marked as SHOULD+ will be promoted at some future time to be a MUST.
SHOULD-	This term means the same as SHOULD. However, it is likely that an algorithm marked as SHOULD- will be deprecated to a MAY or worse in a future version of this document.
MUST-	This term means the same as MUST. However, we expect that at some point in the future this algorithm will no longer be a MUST.

3. Authentication Scheme Selection

For IS-IS implementations to interoperate, they must support one or more authentication schemes in common. This section specifies the requirements for standards conformant IS-IS implementations, which desire to utilize the security feature.

Old Req.	Old RFC	New Requirement	Authentication Scheme
MUST	ISO-10589/ RFC 1195	SHOULD NOT	Clear Text Password (1)
MUST	3567	MUST-	HMAC-MD5
-	-	SHOULD+	Cryptographic Auth [ISIS-HMAC]

The above is only true in case security is required, if there is no requirement of security from an implementation, the above requirements need not be followed

Notes:

(1)This is used when all the routers can "trust" one another but the operator does not want an accidental introduction of a router in the domain. This scheme of authentication is useful, but not when the operator wants to "cryptographically" authenticate the OSPF packets.

4. Authentication Algorithm Selection

For IS-IS implementations to interoperate, they must support one or more authentication algorithms in common that can be used in the cryptographic scheme of authentication.

This section details the authentication algorithm requirements for standards conformant IS-IS implementations.

Old Req.	Old RFC	New Requirement	Authentication Algorithm
MUST	3567	MUST-	HMAC-MD5
-	-	SHOULD+	HMAC-SHA-1 [ISIS-HMAC]
-	-	MAY+	HMAC-SHA-256/HMAC-SHA-384/HMAC-SHA-512

5. Security Considerations

The cryptographic mechanisms defined in this document define only authentication algorithms, and do not provide any confidentiality. However encrypting the content of the packet (providing confidentiality) is not of as great a value to routing protocols as authenticating the source of the packet.

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.

To ensure greater security, the keys used must be changed periodically and implementations MUST be able to store and use more than one key at the same time.

This document concerns itself with the selection of cryptographic algorithms for the use of IS-IS, specifically with the selection of "mandatory-to-implement" algorithms. The algorithms identified in this document as "MUST implement" or "SHOULD implement" are not known to be broken at the current time, and cryptographic research so far leads us to believe that they will likely remain secure into the foreseeable future. However, this isn't necessarily forever. We would therefore expect that new revisions of this document will be issued from time to time that reflect the current best practice in this area.

6. Acknowledgements

Much of the wording herein was adapted from RFC 4307, "Cryptographic Algorithms for Use in the Internet Key Exchange Version 2", by Jeffrey I. Schiller.

7. IANA Considerations

This document places no requests to IANA.

8. References

8.1 Normative References

[KEYWORDS] 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.

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

[ISIS-HMAC] Bhatia, M., Manral, V. and White, R.,"ISIS HMAC Cryptographic Authentication", Work in Progress

8.2 Informative References

[MD5-attack] Wang, X. et al., "Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD", August 2004, http://eprint.iacr.org/2004/199

9. Author's Addresses

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

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

Full Copyright Statement

Intellectual Property