Internet Engineering Task Force (IETF)
Request for Comments: 6094
Category: Informational
ISSN: 2070-1721

M. Bhatia
Alcatel-Lucent
V. Manral
IP Infusion

February 2011

Summary of Cryptographic Authentication Algorithm Implementation Requirements for Routing Protocols

Abstract

The routing protocols Open Shortest Path First version 2 (OSPFv2), Intermediate System to Intermediate System (IS-IS), and Routing Information Protocol (RIP) currently define cleartext and MD5 (Message Digest 5) methods for authenticating protocol packets. Recently, effort has been made to add support for the SHA (Secure Hash Algorithm) family of hash functions for the purpose of authenticating routing protocol packets for RIP, IS-IS, and OSPF.

To encourage interoperability between disparate implementations, it is imperative that we specify the expected minimal set of algorithms, thereby ensuring that there is at least one algorithm that all implementations will have in common.

Similarly, RIP for IPv6 (RIPng) and OSPFv3 support IPsec algorithms for authenticating their protocol packets.

This document examines the current set of available algorithms, with interoperability and effective cryptographic authentication protection being the principal considerations. Cryptographic authentication of these routing protocols requires the availability of the same algorithms in disparate implementations. It is desirable that newly specified algorithms should be implemented and available in routing protocol implementations because they may be promoted to requirements at some future time.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6094.

Copyright Notice

Table of Contents

1. Introduction

Most routing protocols include three different types of authentication schemes: Null authentication, cleartext password, and cryptographic authentication. Null authentication is equivalent to having no authentication scheme at all.

In a cleartext scheme, also known as a "simple password" scheme, the password is exchanged completely unprotected, and anyone with physical access to the network can learn the password and compromise the integrity of the routing domain. The simple password scheme protects against accidental establishment of routing sessions in a given domain, but beyond that it offers no additional protection.

In a cryptographic authentication scheme, routers share a secret key that is used to generate a message authentication code for each of the protocol packets. Today, routing protocols that implement message authentication codes often use a Keyed-MD5 [RFC1321] digest. The recent escalating series of attacks on MD5 raise concerns about its remaining useful lifetime.

These attacks may not necessarily result in direct vulnerabilities for Keyed-MD5 digests as message authentication codes because the colliding message may not correspond to a syntactically correct protocol packet. The known collision, pre-image, and second pre-image attacks [RFC4270] on MD5 may not increase the effectiveness of the key recovery attacks on HMAC-MD5. Regardless, there is a need felt to deprecate MD5 [RFC1321] as the basis for the Hashed Message Authentication Code (HMAC) algorithm in favor of stronger digest algorithms.

In light of these considerations, there are proposals to replace HMAC-MD5 with keyed HMAC-SHA [SHS] digests where HMAC-MD5 is currently mandated in RIPv2 [RFC2453] IS-IS [ISO] [RFC1195], and Keyed-MD5 in OSPFv2 [RFC2328].

OSPFv3 [RFC5340] and RIPng [RFC2080] rely on the IPv6 Authentication Header (AH) [RFC4302] and IPv6 Encapsulating Security Payload (ESP) [RFC4303] in order to provide integrity, authentication, and/or confidentiality.

However, the nature of cryptography is that algorithmic improvement is an ongoing process, as is the exploration and refinement of attack vectors. An algorithm believed to be strong today may be demonstrated to be weak tomorrow. Given this, the choice of preferred algorithm should favor the minimization of the likelihood of it being compromised quickly.

It should be recognized that preferred algorithm(s) will change over time to adapt to the evolving threats. At any particular time, the mandatory-to-implement algorithm(s) might not be specified in the base protocol specification. As protocols are extended, the preference for presently stronger algorithms presents a problem regarding the question of interoperability of existing and future implementations with respect to standards, and also regarding operational preference for the configuration as deployed.

It is expected that an implementation should support the changing of security (authentication) keys. Changing the symmetric key used in any HMAC algorithm on a periodic basis is good security practice. Operators need to plan for this.

Implementations can support in-service key change so that no control packets are lost. During an in-service/in-band key change, more than one key can be active for receiving packets for a session. Some protocols support a key identifier that allows the two peers of a session to have multiple keys simultaneously for a session.

However, these protocols currently manage keys manually (i.e., via operator intervention) or dynamically based on some timer or security protocol.

2. Intermediate System to Intermediate System (IS-IS)

The IS-IS specification allows for authentication of its Protocol Data Units (PDUs) via the authentication TLV (TLV 10) in the PDU. The base specification [ISO] had provisions only for cleartext passwords. [RFC5304] extends the authentication capabilities by providing cryptographic authentication for IS-IS PDUs. It mandates support for HMAC-MD5.

[RFC5310] adds support for the use of any cryptographic hash function for authenticating IS-IS PDUs. In addition to this, [RFC5310] also details how IS-IS can use the HMAC construct along with the Secure Hash Algorithm (SHA) family of cryptographic hash functions to secure IS-IS PDUs.

2.1. Authentication Scheme Selection

In order for IS-IS implementations to securely interoperate, they must support one or more authentication schemes in common. This section specifies the preference for standards-conformant IS-IS implementations that use accepted authentication schemes.

The earliest interoperability requirement for authentication as stated by [ISO] [RFC1195] required all implementations to support a cleartext password. This authentication scheme's utility is limited to precluding the accidental introduction of a new IS into a broadcast domain. Operators should not use this scheme, as it provides no protection against an attacker with access to the broadcast domain: anyone can determine the secret password through inspection of the PDU. This mechanism does not provide any significant level of security and should be avoided.

[RFC5304] defined the cryptographic authentication scheme for IS-IS. HMAC-MD5 was the only algorithm specified; hence, it is mandated. [RFC5310] defined a generic cryptographic scheme and added support for additional algorithms. Implementations should support [RFC5310], as it defines the generic cryptographic authentication scheme.

2.2. Authentication Algorithm Selection

For IS-IS implementations to securely interoperate, they must have support for one or more authentication algorithms in common.

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

The following are the available options for authentication algorithms:

- [RFC5304] mandates the use of HMAC-MD5.

- [RFC5310] does not require a particular algorithm but instead supports any digest algorithm (i.e., cryptographic hash functions).

As noted earlier, there is a desire to deprecate MD5. IS-IS implementations will likely migrate to an authentication scheme supported by [RFC5310], because it is algorithm agnostic. Possible digest algorithms include SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512. Picking at least one mandatory-to-implement algorithm is imperative to ensuring interoperability.

3. Open Shortest Path First Version 2 (OSPFv2)

[RFC2328] includes three different types of authentication schemes: Null authentication, cleartext password (defined as "simple password" in [RFC2328]), and cryptographic authentication. Null authentication is semantically equivalent to no authentication.

In the cryptographic authentication scheme, the OSPFv2 routers on a common network/subnet are configured with a shared secret that is used to generate a Keyed-MD5 digest for each packet. A monotonically increasing sequence number scheme is used to protect against replay attacks.

[RFC5709] adds support for the use of the SHA family of hash algorithms for authentication of OSPFv2 packets.

3.1. Authentication Scheme Selection

For OSPF implementations to securely interoperate, they must have one or more authentication schemes in common.

While all implementations will have Null authentication since it's mandated by [RFC2328], its use is not appropriate in any context where the operator wishes to authenticate OSPFv2 packets in their network.

While all implementations will also support a cleartext password since it's mandated by [RFC2328], its use is only appropriate when the operator wants to preclude the accidental introduction of a router into the domain. This scheme is patently not useful when an operator wants to authenticate the OSPFv2 packets.

Cryptographic authentication is a mandatory scheme defined in [RFC2328], and all conformant implementations must support this.

3.2. Authentication Algorithm Selection

For OSPFv2 implementations to securely interoperate, they must support one or more cryptographic authentication algorithms in common.

The following are the available options for authentication algorithms:

- [RFC2328] specifies the use of Keyed-MD5.

- [RFC5709] specifies the use of HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512, and also mandates support for HMAC-SHA-256 (HMAC-SHA-1 is optional).

As noted earlier, there is a desire to deprecate MD5. Some alternatives for MD5 are listed in [RFC5709].

Possible digest algorithms include SHA-1, SHA-256, SHA-384, and SHA-512. Picking one mandatory-to-implement algorithm is imperative to ensuring interoperability.

4. Open Shortest Path First Version 3 (OSPFv3)

OSPFv3 [RFC5340] relies on the IPv6 Authentication Header (AH) [RFC4302] and IPv6 Encapsulating Security Payload (ESP) [RFC4303] in order to provide integrity, authentication, and/or confidentiality.

[RFC4552] mandates the use of ESP for authenticating OSPFv3 packets. The implementations could also provide support for using AH to protect these packets.

The algorithm requirements for AH and ESP are described in [RFC4835] as follows:

- o [RFC2404] mandates HMAC-SHA-1-96.
- o [RFC3566] indicates AES-XCBC-MAC-96 as a "should", but it's likely that this will be mandated at some future time.

5. Routing Information Protocol Version 2 (RIPv2)

RIPv2, originally specified in [RFC1388] and then in [RFC1723], has been updated and published as STD 56, [RFC2453]. If the Address Family Identifier of the first (and only the first) entry in the RIPv2 message is 0xFFFF, then the remainder of the entry contains the authentication information. The [RFC2453] version of the protocol provides for authenticating packets using a cleartext password (defined as "simple password" in [RFC2453]) not more than 16 octets in length.

[RFC2082] added support for Keyed-MD5 authentication, where a digest is appended to the end of the RIP packet. [RFC4822] obsoleted [RFC2082] and added the SHA family of hash algorithms to the list of cryptographic authentications that can be used to protect RIPv2, whereas [RFC2082] previously specified only the use of Keyed-MD5.

5.1. Authentication Scheme Selection

For RIPv2 implementations to securely interoperate, they must support one or more authentication schemes in common.

While all implementations will support a cleartext password since it's mandated by [RFC2453], its use is only appropriate when the operator wants to preclude the accidental introduction of a router into the domain. This scheme is patently not useful when an operator wants to authenticate the RIPv2 packets.

[RFC2082] mandates the use of an authentication scheme that uses Keyed-MD5. However, [RFC2082] has been obsoleted by [RFC4822]. Compliant implementations must provide support for an authentication scheme that uses Keyed-MD5 but should recognize that this is superseded by cryptographic authentication as defined in [RFC4822].

Implementations should provide support for [RFC4822], as it specifies the RIPv2 cryptographic authentication schemes.

5.2. Authentication Algorithm Selection

For RIPv2 implementations to securely interoperate, they must support one or more authentication algorithms in common.

The following are the available options for authentication algorithms:

- o [RFC2082] specifies the use of Keyed-MD5.

- o [RFC4822] specifies the use of Keyed-MD5, HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512.

As noted earlier, there is a desire to deprecate MD5. Some alternatives for MD5 are listed in [RFC4822]. Possible digest algorithms include SHA-1, SHA-256, SHA-384, and SHA-512. Picking one mandatory-to-implement algorithm is imperative to ensuring interoperability.

6. Routing Information Protocol for IPv6 (RIPng)

RIPng [RFC2080] relies on the IPv6 Authentication Header (AH) [RFC4302] and IPv6 Encapsulating Security Payload (ESP) [RFC4303] in order to provide integrity, authentication, and/or confidentiality.

The algorithm requirements for AH and ESP are described in [RFC4835] as follows:

- o [RFC2404] mandates HMAC-SHA-1-96.

- o [RFC3566] indicates AES-XCBC-MAC-96 as a "should", but it's likely that this will be mandated at some future time.

7. Security Considerations

The cryptographic mechanisms referenced in this document provide only authentication algorithms. These algorithms do not provide confidentiality. Encrypting the content of the packet and thereby providing confidentiality is not considered in the definition of the routing protocols.

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. The feasibility of attacking the integrity of routing protocol messages protected by keyed digests may be significantly more limited than that of other data; however, preference for one family of algorithms over another may also change independently of the perceived risk to a particular protocol.

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. Operational experience suggests that the lack of periodic rekeying is a source of significant exposure and that the lifespan of shared keys in the network is frequently measured in years.

While simple password schemes are well represented in the document series and in conformant implementations of the protocols, the inability to offer either integrity or identity protection are sufficient reason to strongly discourage their use.

This document concerns itself with the selection of cryptographic algorithms for use in the authentication of routing protocol packets being exchanged between adjacent routing processes. The cryptographic algorithms identified in this document are not known to be broken at the current time, and ongoing cryptographic research so far leads us to believe that they will likely remain secure in the foreseeable future. We expect that new revisions of this document will be issued in the future to reflect current thinking on the algorithms that various routing protocols should employ to ensure interoperability between disparate implementations.

8. Acknowledgements

We would like to thank Joel Jaeggli, Sean Turner, and Adrian Farrel for their comments and feedback on this document, which resulted in significant improvement of the same.

9. References

9.1. Normative References

[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/IEC 10589:1992 (ISO 8473).

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

[RFC2080] Malkin, G. and R. Minnear, "RIPng for IPv6", RFC 2080, January 1997.

[RFC2328] Moy, J., "OSPF Version 2", STD 54, RFC 2328, April 1998.

[RFC2453] Malkin, G., "RIP Version 2", STD 56, RFC 2453, November 1998.

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

[RFC4835] Manral, V., "Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)", RFC 4835, April 2007.

[RFC5304] Li, T. and R. Atkinson, "IS-IS Cryptographic Authentication", RFC 5304, October 2008.

[RFC5310] Bhatia, M., Manral, V., Li, T., Atkinson, R., White, R., and M. Fanto, "IS-IS Generic Cryptographic Authentication", RFC 5310, February 2009.

[RFC5340] Coltun, R., Ferguson, D., Moy, J., and A. Lindem, "OSPF for IPv6", RFC 5340, July 2008.

[RFC5709] Bhatia, M., Manral, V., Fanto, M., White, R., Barnes, M., Li, T., and R. Atkinson, "OSPFv2 HMAC-SHA Cryptographic Authentication", RFC 5709, October 2009.

9.2. Informative References

[RFC1321] Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, April 1992.

[RFC1388] Malkin, G., "RIP Version 2 Carrying Additional Information", RFC 1388, January 1993.

[RFC1723] Malkin, G., "RIP Version 2 - Carrying Additional Information", RFC 1723, November 1994.

[RFC2082] Baker, F. and R. Atkinson, "RIP-2 MD5 Authentication", RFC 2082, January 1997.

[RFC2404] Madson, C. and R. Glenn, "The Use of HMAC-SHA-1-96 within ESP and AH", RFC 2404, November 1998.

[RFC3566] Frankel, S. and H. Herbert, "The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec", RFC 3566, September 2003.

[RFC4270] Hoffman, P. and B. Schneier, "Attacks on Cryptographic Hashes in Internet Protocols", RFC 4270, November 2005.

[RFC4302] Kent, S., "IP Authentication Header", RFC 4302, December 2005.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.

[RFC4552] Gupta, M. and N. Melam, "Authentication/Confidentiality for OSPFv3", RFC 4552, June 2006.

[SHS] "Secure Hash Standard (SHS)", National Institute of Standards and Technology (NIST) FIPS Publication 180-3, October 2008.

Authors' Addresses

Manav Bhatia
Alcatel-Lucent
Bangalore
India

EMail: manav.bhatia@alcatel-lucent.com

Vishwas Manral
IP Infusion
1188 E. Arques Ave.
Sunnyvale, CA 94089
USA

Phone: 408-400-1900
EMail: vishwas@ipinfusion.com