Network Working Group **Manav Bhatia**
Internet Draft **Alcatel-Lucent**
Expires: April 2011 **Vishwas Manral**
Intended Status: Informational IP Infusion
October 2010

Cryptographic Authentication Algorithm Implementation Requirements for Routing Protocols

draft-ietf-opsec-igp-crypto-requirements-02.txt

Status of this Memo

This Internet-Draft will expire on March 28, 2011.

Copyright Notice

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 Clear Text 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.

This document examines the current set of available algorithms with interoperability and effective cryptographic authentication protection being the principle 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.

Table of Contents

1. Introduction

Most routing protocols include three different types of authentication schemes: Null authentication, Clear Text Password and a Cryptographic Authentication scheme. Null authentication is equivalent to having no authentication scheme at all.

In a clear text scheme, also known as, simple password scheme, the password is exchanged in the clear on the network and anyone with physical access to the network can learn the password and compromise the integrity of the routing domain. While the Password scheme protects from accidental establishment of routing session in a given domain, it offers little additional protection.

In a cryptographic authentication scheme, routers share a secret key which is used to generate a message authentication code for each of the protocol packets. Today, message authentication codes often use a keyed MD5 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. There is a however a need felt to deprecate MD5 [RFC1321] in favor of stronger message authentication code algorithms.

In light of these considerations there have been proposals for adding support of the SHA [SHS] family of hash algorithms for authenticating routing protocol packets in RIP [RFC2453], IS-IS [ISO] [RFC1195] and OSPF [RFC2328].

However, the nature of cryptography is that algorithmic improvement is an ongoing process and 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. The selection of preferred algorithms may well not be reflected in the base protocol specification. As protocols are extended the preference for presently stronger algorithms presents a problem both on the question of interoperability of existing and future implementations with respect to standards and operational preference for the configuration as deployed. This document intends to provide guidance to implementers in anticipation of operational preference.

It is expected an implementation should support changing of Security (Authentication) Keys. Changing Keys periodically is a good security practice.

Implementations can support in-service key change so that no control packets are lost. During such Key change more than one key can be active for receiving packets for a session. Some protocols support Key ID which allows the two ends of a session to have multiple keys simultaneously for a session. Key change however is managed outside the scope of the protocols themselves and can be done manually via operator intervention, or dynamically based on some timer or a 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 had provisions only for clear text passwords. RFC 5304 [RFC5304] extends the authentication capabilities by providing HMAC-MD5 authentication for IS-IS PDUs.

RFC 5310 [RFC5310] adds support for the use of the SHA family of hash algorithms for authenticating IS-IS PDUs.

2.1 Authentication Scheme Selection

In order for IS-IS implementations to interoperate with the use of security, they must support one or more authentication schemes in common. This section specifies the preference for standards conformant IS-IS implementations, which desire to utilize the security feature.

The earliest interoperability requirement for authentication as stated by [ISO] [RFC1195] required all implementations to support Clear Text Password. This authentication scheme's utility is limited to precluding the accidental introduction of a new IS into a broadcast domain. We believe that operators should not use this scheme as it provides no protection against an attacker with access to the broadcast domain as 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] mandates the use of HMAC-MD5 for cryptographically authenticating the IS-IS PDUs. It is likely that this may get deprecated in favor of the generic cryptographic authentication scheme defined in [RFC5310] in the future deployments, so new implementations should support this scheme.

2.2 Authentication Algorithm Selection

For IS-IS implementations to interoperate with the use of security, 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.

[RFC5304] mandates the use of HMAC-MD5 for cryptographically authenticating the IS-IS PDUs. It is likely that this may get deprecated in favor of HMAC-SHA-1 as defined in [RFC5310] in the future deployments, so new implementations should support this algorithm.

Implementations may start providing support for HMAC-SHA-256/HMAC-SHA-384/HMAC-SHA-512 as these algorithms may be necessary in the future.

3. Open Shortest Path First Version 2(OSPFv2)

OSPFv2 as defined in [RFC2328] includes three different types of authentication schemes: Null authentication, simple password and cryptographic authentication. Null authentication is semantically equivalent to no authentication. In the simple password scheme of authentication, the passwords are exchanged in the clear on the network. Anyone with physical access to the network can learn the password and compromise the security of the OSPFv2 domain.

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

RFC 5709 [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 interoperate with the use of security, they must have one or more authentication schemes in common. This section specifies the preference for standards conformant OSPFv2 implementations, which desire to utilize the security feature.

While all implementations will have NULL auth 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.

Similarly Simple Password, also mandatory per [RFC2328], should be used when the operator only wants to preclude the accidental introduction of a router into the domain. This scheme is not useful when the operator wants to authenticate the OSPFv2 packets.

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

3.2 Authentication Algorithm Selection

For OSPFv2 implementations to interoperate with the use of security, they must support one or more cryptographic authentication algorithms in common.

[RFC2328] states that implementations must offer keyed MD5 authentication. It is likely that this will be deprecated in favor of HMAC-SHA-1 and HMAC-SHA-256 [RFC5709] in future deployments, so new implementations should support these algorithms.

Operators should consider migration to HMAC-SHA-256 if they desire a stronger cryptographic algorithm for authentication of OSPFv2 packets.

Implementations may start providing support for HMAC-SHA-1/HMAC-SHA-384/HMAC-SHA-512 [RFC5709] as these algorithms may be preferred in the future.

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.

[RFC4522] 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] and are not discussed here.

5. Routing Information Protocol Version 2 (RIPv2)

RIPv2, originally specified in [RFC1388], then [RFC1723], has been updated and published as STD56 [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 simple password of not more than 16 octets, in which the password is sent in clear.

"RIP-2 MD5 Authentication" [RFC2082] added support for Keyed-MD5 authentication, where a digest is appended to the end of the RIP packet. "RIPv2 Cryptographic Authentication" [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 interoperate with the use of security, one or more authentication schemes must be supported in common. This section specifies the preference for standards conformant RIPv2 implementations, which desire to utilize the security feature.

Simple Password is a mandatory to implement scheme as defined in [RFC2453] and should only be used when the operator wishes to preclude the accidental introduction of a RIP router into the domain. This authentication scheme is useful, but not when the operator wants to protect RIPv2 message exchange in a potentially hostile environment.

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

Implementations should provide support for [RFC4822] Cryptographic Authentication as it will likely be the preferred authentication method in the future.

5.2 Authentication Algorithm Selection

For RIPv2 implementations to interoperate with the use of security, one or more authentication algorithms must be supported in common that can be used for authentication.

The keyed MD5 algorithm in [RFC2082] and [RFC4822] must be implemented. It is our belief that it will be superseded by HMAC-SHA-1 also available in [RFC4822]. Keyed MD5 must be implemented for interoperability purposes, but its use may be deprecated in the future.

Implementations should provide support for HMAC-SHA-1 used in preference to keyed MD5 the future.

Operators should consider migration to HMAC-SHA-1 if they want to use stronger cryptographic algorithms for authenticating RIPv2 packets.

Implementations should consider providing support for HMAC-SHA-256/HMAC-SHA-384/HMAC-SHA-512 as these algorithms may be preferred in the future.

6. Routing Information Protocol for IPv6 (RIPng)

RIPng [RFC2080] relies on the IPv6 AH and IPv6 ESP to provide integrity, authentication, and/or confidentiality.

The algorithm requirements for AH and ESP are described in [RFC4835] and are not discussed here.

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 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 various routing protocols should employ to ensure interoperability between disparate implementations.

8.
Acknowledgements

We would like to thank Joel Jaeggli for this comments and feedback on this draft that resulted in significant improvement of the same.

9. IANA Considerations

This document places no requests to IANA.

10.
References

10.1
Normative References

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

[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.

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

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

[RFC5304] Li, T. and R. Atkinson, "Intermediate System to Intermediate System (IS-IS) Cryptographic Authentication", RFC 5304, October 2008

[RFC5340] Coltun, R., et. al, "OSPF for IPv6", RFC 5340, July 2008.

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

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

[RFC5310] Bhatia, M., et. al., "IS-IS Generic Cryptographic Authentication", RFC 5310, February 2009

[RFC5709] Bhatia, M., Manral, V., et al., "OSPF HMAC-SHA Cryptographic Authentication", RFC 5709, October 2009

10.2
Informative References

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

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

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

[RFC4522] Gupta, M. and Melam, N.,"Authentication/Confidentiality for OSPFv3", RFC 4522, June 2006

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

[RFC1723] Malkin, G., "RIP Version 2 - Carrying Additional Information", STD 56, RFC 1723, November 1994.

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

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

Author's Addresses

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

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