DNSext Working Group F. Dupont
Internet-Draft ISC
Updates: 2845,2930,4635 May 8, 2009
(if approved)
Intended status: Standards Track
Expires: November 9, 2009

Deprecation of HMAC-MD5 in DNS TSIG and TKEY Resource Records
draft-ietf-dnsext-tsig-md5-deprecated-03.txt

Status of this Memo

This Internet-Draft will expire on November 9, 2009.

Copyright Notice

Abstract

The main purpose of this document is to deprecate the use of HMAC-MD5 as an algorithm for the TSIG (secret key transaction authentication) resource record in the DNS (domain name system), and the use of MD5 in TKEY (secret key establishment for DNS).

1. Introduction

The secret key transaction authentication for DNS (TSIG, [RFC2845]) was defined with the HMAC-MD5 [RFC2104] cryptographic algorithm. When the MD5 [RFC1321] security came to be considered lower than expected, [RFC4635] standardized new TSIG algorithms based on SHA [RFC3174][RFC3874][RFC4634] digests.

But [RFC4635] did not deprecate the HMAC-MD5 algorithm. This document is targeted to complete the process, in detail:

1. Mark HMAC-MD5.SIG-ALG.REG.INT as optional in the TSIG algorithm name registry managed by the IANA under the IETF Review Policy [RFC5226]
2. Make HMAC-MD5.SIG-ALG.REG.INT support "not Mandatory" for implementations
3. Provide a keying material derivation for the secret key establishment for DNS (TKEY, [RFC2930]) using a Diffie-Hellman exchange with SHA256 [RFC4634] in place of MD5 [RFC1321]
4. Finally recommend the use of HMAC-SHA256.

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. Implementation Requirements

The table of section 3 of [RFC4635] is replaced by:

Requirement Level	Algorithm Name
Optional	HMAC-MD5.SIG-ALG.REG.INT
Optional	gss-tsig
Mandatory	hmac-sha1
Optional	hmac-sha224
Mandatory	hmac-sha256
Optional	hmac-sha384
Optional	hmac-sha512

Implementations that support TSIG MUST also implement HMAC-SHA1 and HMAC-SHA256 (i.e., algorithms at the "Mandatory" requirement level) and MAY implement GSS-TSIG and the other algorithms listed above (i.e., algorithms at a "not Mandatory" requirement level).

3. TKEY keying material derivation

When the TKEY [RFC2930] uses a Diffie-Hellman exchange, the keying material is derived from the shared secret and TKEY resource record data using MD5 [RFC1321] at the end of section 4.1 page 9.

This is amended into:

```
keying material =
     XOR ( DH value, SHA256 ( query data | DH value ) |
                     SHA256 ( server data | DH value ) )
```

using the same conventions.

4. IANA Consideration

This document extends the "TSIG Algorithm Names - per [] and [RFC2845]" located at http://www.iana.org/assignments/tsig-algorithm-names by adding a new column to the registry "Compliance Requirement".

The registry should contain the following:

Algorithm Name	Compliance Requirement	Reference
gss-tsig	Optional	[RFC3645]
HMAC-MD5.SIG-ALG.REG.INT	Optional	[][RFC2845]
hmac-sha1	Mandatory	[RFC4635]
hmac-sha224	Optional	[RFC4635]
hmac-sha256	Mandatory	[RFC4635]
hmac-sha384	Optional	[RFC4635]
hmac-sha512	Optional	[RFC4635]

where [] is this document.

5. Availability Considerations

MD5 is no longer universally available and its use may lead to increasing operation issues. SHA1 is likely to suffer from the same kind of problem. In summary MD5 has reached end-of-life and SHA1 will likely follow in the near term.

According to [RFC4635], implementations which support TSIG are REQUIRED to implement HMAC-SHA256.

6. Security Considerations

This document does not assume anything about the cryptographic security of different hash algorithms. Its purpose is a better availability of some security mechanisms in a predictable time frame.

Requirement levels are adjusted for TSIG and related specifications (i.e., TKEY):
   The support of HMAC-MD5 is changed from mandatory to optional.
   The use of MD5 and HMAC-MD5 is NOT RECOMMENDED.
   The use of HMAC-SHA256 is RECOMMENDED.

7. Acknowledgments

Olafur Gudmundsson kindly helped in the procedure to deprecate the MD5 use in TSIG, i.e., the procedure which led to this memo. Alfred Hoenes, Peter Koch, Paul Hoffman and Edward Lewis proposed some improvements.

8. References

8.1. Normative References

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

[RFC2845] Vixie, P., Gudmundsson, O., Eastlake, D., and B. Wellington, "Secret Key Transaction Authentication for DNS (TSIG)", RFC 2845, May 2000.

[RFC2930] Eastlake, D., "Secret Key Establishment for DNS (TKEY RR)", RFC 2930, September 2000.

[RFC4635] Eastlake, D., "HMAC SHA TSIG Algorithm Identifiers", RFC 4635, August 2006.

8.2. Informative References

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

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

[RFC3174] Eastlake, D. and P. Jones, "US Secure Hash Algorithm 1 (SHA1)", RFC 3174, September 2001.

[RFC3645] Kwan, S., Garg, P., Gilroy, J., Esibov, L., Westhead, J., and R. Hall, "Generic Security Service Algorithm for Secret Key Transaction Authentication for DNS (GSS-TSIG)", RFC 3645, October 2003.

[RFC3874] Housley, R., "A 224-bit One-way Hash Function: SHA-224", RFC 3874, September 2004.

[RFC4634] Eastlake, D. and T. Hansen, "US Secure Hash Algorithms (SHA and HMAC-SHA)", RFC 4634, July 2006.

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

Author's Address

Francis Dupont
ISC

Email: Francis.Dupont@fdupont.fr