Deprecation of HMAC-MD5 in DNS TSIG and TKEY Resource Records
draft-ietf-dnsext-tsig-md5-deprecated-02.txt

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79. This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on October 29, 2009.

Copyright Notice

Copyright (c) 2009 IETF Trust and the persons identified as the document authors. All rights reserved.
This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents in effect on the date of publication of this document (http://trustee.ietf.org/license-info). Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Abstract

The main goal 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).

1. Introduction

The secret key transaction authentication for DNS (TSIG, [RFC2845]) was defined with the HMAC-MD5 [RFC2104] cryptographic algorithm. As the MD5 [RFC1321] security was recognized to be 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 details:

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:
<table>
<thead>
<tr>
<th>Requirement Level</th>
<th>Algorithm Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optional</td>
<td>HMAC-MD5.SIG-ALG.REG.INT</td>
</tr>
<tr>
<td>Optional</td>
<td>gss-tsig</td>
</tr>
<tr>
<td>Mandatory</td>
<td>hmac-sha1</td>
</tr>
<tr>
<td>Optional</td>
<td>hmac-sha224</td>
</tr>
<tr>
<td>Mandatory</td>
<td>hmac-sha256</td>
</tr>
<tr>
<td>Optional</td>
<td>hmac-sha384</td>
</tr>
<tr>
<td>Optional</td>
<td>hmac-sha512</td>
</tr>
</tbody>
</table>

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   |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>gss-tsig</td>
<td>Optional</td>
<td>[RFC3645]</td>
</tr>
<tr>
<td>HMAC-MD5.SIG-ALG.REG.INT</td>
<td>Optional</td>
<td>R[FC2845]</td>
</tr>
<tr>
<td>hmac-sha1</td>
<td>Mandatory</td>
<td>[RFC4635]</td>
</tr>
<tr>
<td>hmac-sha224</td>
<td>Optional</td>
<td>[RFC4635]</td>
</tr>
<tr>
<td>hmac-sha256</td>
<td>Mandatory</td>
<td>[RFC4635]</td>
</tr>
<tr>
<td>hmac-sha384</td>
<td>Optional</td>
<td>[RFC4635]</td>
</tr>
<tr>
<td>hmac-sha512</td>
<td>Optional</td>
<td>[RFC4635]</td>
</tr>
</tbody>
</table>

where [] is this document.

5. Availability Considerations

MD5 is no more universally available and its use should lead to increasing operation issues. SHA1 is likely to suffer from the same kind of problem. To summary MD5 has reached end-of-life and SHA1 follows few years behind.

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. It is a routine maintenance, its goal is better availability of some security mechanisms in a predictable future.

Requirement levels are adjusted for TSIG and related specifications (i.e., TKEY):
- 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 and Paul Hoffman proposed some improvements.

8. References
8.1. Normative References


8.2. Informative References


Author’s Address

Francis Dupont
ISC

Email: Francis.Dupont@fdupont.fr