       Deprecating MD5 and SHA-1 Signature Hashes in TLS 1.2 and DTLS 1.2

Abstract

   The MD5 and SHA-1 hashing algorithms are increasingly vulnerable to
   attack, and this document deprecates their use in TLS 1.2 and DTLS
   1.2 digital signatures. However, this document does not deprecate
   SHA-1 with Hashed Message Authentication Code (HMAC), as used in
   record protection. This document updates RFC 5246.

Status of This Memo

   This is an Internet Standards Track document.

   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). Further information on
   Internet Standards is available in Section 2 of RFC 7841.

   Information about the current status of this document, any errata,
   and how to provide feedback on it may be obtained at
   https://www.rfc-editor.org/info/rfc9155.

Table of Contents

1. Introduction

The usage of MD5 and SHA-1 for signature hashing in (D)TLS 1.2 is
specified in [RFC5246]. MD5 and SHA-1 have been proven to be
insecure, subject to collision attacks [Wang]. In 2011, [RFC6151]
detailed the security considerations, including collision attacks for
MD5. NIST formally deprecated use of SHA-1 in 2011
[NISTSP800-131A-R2] and disallowed its use for digital signatures at
the end of 2013, based on both the attack described in [Wang] and the
potential for brute-force attack. In 2016, researchers from the
National Institute for Research in Digital Science and Technology
(INRIA) identified a new class of transcript collision attacks on TLS
(and other protocols) that relies on efficient collision-finding
algorithms on the underlying hash constructions
[Transcript-Collision]. Further, in 2017, researchers from Google
and Centrum Wiskunde & Informatica (CWI) Amsterdam [SHA-1-Collision]
proved SHA-1 collision attacks were practical. This document updates
[RFC5246] in such a way that MD5 and SHA-1 MUST NOT be used for
digital signatures. However, this document does not deprecate SHA-1
with HMAC, as used in record protection. Note that the CA/Browser
Forum (CABF) has also deprecated use of SHA-1 for use in certificate
signatures [CABF].

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
"SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and
"OPTIONAL" in this document are to be interpreted as described in
BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all
capitals, as shown here.

2. Signature Algorithms

Clients MUST include the signature_algorithms extension. Clients
MUST NOT include MD5 and SHA-1 in this extension.

3. Certificate Request

Servers SHOULD NOT include MD5 and SHA-1 in CertificateRequest
messages.

4. Server Key Exchange

Servers MUST NOT include MD5 and SHA-1 in ServerKeyExchange messages.
If the client receives a ServerKeyExchange message indicating MD5 or
SHA-1, then it MUST abort the connection with an illegal_parameter
alert.

5. Certificate Verify

Clients MUST NOT include MD5 and SHA-1 in CertificateVerify messages.
If a server receives a CertificateVerify message with MD5 or SHA-1,
it MUST abort the connection with an illegal_parameter alert.

6. IANA Considerations

IANA has updated the "TLS SignatureScheme" registry by changing the
recommended status of SHA-1-based signature schemes to "N" (not
recommended), as defined by [RFC8447]. The following entries have
been updated; other entries in the registry remain the same.

Value	Description	Recommended	Reference
========	================	=============	======================
0x0201	rsa_pkcs1_sha1	N	[RFC8446] [RFC9155]
0x0203	ecdsa_sha1	N	[RFC8446] [RFC9155]

Table 1

IANA has also updated the reference for the "TLS SignatureAlgorithm"
and "TLS HashAlgorithm" registries to refer to this document in
addition to RFCs 5246 and 8447.

7. Security Considerations

Concerns with (D)TLS 1.2 implementations falling back to SHA-1 is an
issue. This document updates the TLS 1.2 specification [RFC5246] to
deprecate support for MD5 and SHA-1 for digital signatures. However,
this document does not deprecate SHA-1 with HMAC, as used in record
protection.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
           Requirement Levels", BCP 14, RFC 2119,
           DOI 10.17487/RFC2119, March 1997,
           <https://www.rfc-editor.org/info/rfc2119>.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security
           (TLS) Protocol Version 1.2", RFC 5246,
           DOI 10.17487/RFC5246, August 2008,
           <https://www.rfc-editor.org/info/rfc5246>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC
           2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174,
           May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol
           Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018,
           <https://www.rfc-editor.org/info/rfc8446>.

   [RFC8447]   Salowey, J. and S. Turner, "IANA Registry Updates for TLS
               and DTLS", RFC 8447, DOI 10.17487/RFC8447, August 2018,
               <https://www.rfc-editor.org/info/rfc8447>.

8.2. Informative References

   [CABF]   CA/Browser Forum, "Ballot 118 -- SHA-1 Sunset (passed)",
               October 2014, <https://cabforum.org/2014/10/16/ballot-118-
               sha-1-sunset/>.

   [NISTSP800-131A-R2]
               Barker, E. and A. Roginsky, "Transitioning the Use of
               Cryptographic Algorithms and Key Lengths", NIST Special
               Publication 800-131A, Revision 2,
               DOI 10.6028/NIST.SP.800-131Ar2, March 2019,
               <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/
               NIST.SP.800-131Ar2.pdf>.

   [RFC6151]   Turner, S. and L. Chen, "Updated Security Considerations
               for the MD5 Message-Digest and the HMAC-MD5 Algorithms",
               RFC 6151, DOI 10.17487/RFC6151, March 2011,
               <https://www.rfc-editor.org/info/rfc6151>.

   [SHA-1-Collision]
               Stevens, M., Bursztein, E., Karpman, P., Albertini, A.,
               and Y. Markov, "The First Collision for Full SHA-1", 2017,
               <https://eprint.iacr.org/2017/190>.

   [Transcript-Collision]
               Bhargavan, K. and G. Leurent, "Transcript Collision
               Attacks: Breaking Authentication in TLS, IKE, and SSH",
               DOI 10.14722/ndss.2016.23418, February 2016,
               <https://hal.inria.fr/hal-01244855/document>.

   [Wang]   Wang, X., Yin, Y., and H. Yu, "Finding Collisions in the
               Full SHA-1", DOI 10.1007/11535218_2, 2005,
               <https://www.iacr.org/archive/
               crypto2005/36210017/36210017.pdf>.

Authors' Addresses

   Loganaden Velvindron
   cyberstorm.mu
   Rose Hill
   Mauritius

   Phone: +230 59762817
   Email: logan@cyberstorm.mu

Kathleen Moriarty
Center for Internet Security
East Greenbush, NY
United States of America

Email: Kathleen.Moriarty.ietf@gmail.com

Alessandro Ghedini
Cloudflare Inc.

Email: alessandro@cloudflare.com