Abstract

The MD5 and SHA-1 hashing algorithms are steadily weakening in strength and their deprecation process should begin for their use in TLS 1.2 digital signatures. However, this document does not deprecate SHA-1 in HMAC for record protection.
1. Introduction

The usage of MD5 and SHA-1 for signature hashing in TLS 1.2 is specified in RFC 5246 [RFC5246]. MD5 and SHA-1 have been proven to be insecure, subject to collision attacks. RFC 6151 [RFC6151] details the security considerations, including collision attacks for MD5, published in 2011. 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 Wang, et. al, attack and the potential for brute-force attack. Further, in 2017, researchers from Google and CWI Amsterdam [SHA-1-Collision] proved SHA-1 collision attacks were practical. This document updates RFC 5246 [RFC5246] and RFC7525 [RFC7525] in such a way that MD5 and SHA1 MUST NOT be used for digital signatures. However, this document does not deprecate SHA-1 in HMAC for record protection.

1.1. Requirements Language

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 RFC 2119 [RFC2119].

2. Signature Algorithms

Clients SHOULD NOT include MD5 and SHA-1 in signature_algorithms extension. If a client does not send a signature_algorithms extension, then the server MUST abort the handshake and send a handshake_failure alert.
3. Certificate Request

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

4. Server Key Exchange

Servers MUST NOT include MD5 and SHA-1 in ServerKeyExchange message. If client does receive a MD5 or SHA-1 signature in the ServerKeyExchange message it MUST abort the connection with handshake_failure or insufficient_security alert.

5. Certificate Verify

Clients MUST NOT include MD5 and SHA-1 in CertificateVerify message.

6. Updates to RFC5246

OLD:

In Section 7.4.1.4.1: the text should be revised from "Note: this is a change from TLS 1.1 where there are no explicit rules, but as a practical matter one can assume that the peer supports MD5 and SHA-1."

NEW:

"Note: This is a change from TLS 1.1 where there are no explicit rules, but as a practical matter one can assume that the peer supports SHA-256."

7. Updates to RFC7525

RFC7525 [RFC7525], Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) recommends use of SHA-256 as a minimum requirement. This update moves the minimum recommendation to use stronger language deprecating use of both SHA-1 and MD5. The prior text did not explicitly include MD5 and this text adds it to ensure it is understood as having been deprecated.

Section 4.3:

OLD:

When using RSA, servers SHOULD authenticate using certificates with at least a 2048-bit modulus for the public key. In addition, the use of the SHA-256 hash algorithm is RECOMMENDED (see [CAB-Baseline] for
Clients SHOULD indicate to servers that they request SHA-256, by using the "Signature Algorithms" extension defined in TLS 1.2.

NEW:

servers SHOULD authenticate using certificates with at least a 2048-bit modulus for the public key.

In addition, the use of the SHA-256 hash algorithm is RECOMMENDED, SHA-1 or MD5 MUST not be used (see [CAB-Baseline] for more details). Clients MUST indicate to servers that they request SHA-256, by using the "Signature Algorithms" extension defined in TLS 1.2.

8. Security Considerations

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

9. Acknowledgement

The authors would like to thank Hubert Kario for his help in writing the initial draft. We are also grateful to Daniel Migault, Martin Thomson and David Cooper for their feedback.

10. References

10.1. Normative References


10.2. Informative References


Authors’ Addresses

Loganaden Velvindron
cyberstorm.mu
Rose Hill
MU

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

Kathleen Moriarty
Dell EMC

Alessandro Ghedini
Cloudflare Inc.