Internet Engineering Task Force (IETF)
Request for Comments: 9155
Updates: 5246
Category: Standards Track
ISSN: 2070-1721

L. Velvindron
cyberstorm.mu
K. Moriarty
CIS
A. Ghedini
Cloudflare Inc.

December 2021

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

Отмена хэш-подписей MD5 и SHA-1 в TLS 1.2 и DTLS 1.2

Аннотация

Алгоритмы MD5 и SHA-1 становятся все более уязвимыми для атак и этот документ отменяет их использование в цифровых подписях TLS 1.2 и DTLS 1.2. Однако документ не отменяет применение SHA-1 в хэшированных кодах аутентификации сообщений (Hashed Message Authentication Code или HMAC) для защиты записей. Данный документ обновляет RFC 5246.

Статус документа

Документ относится к категории Internet Standards Track.

Документ является результатом работы IETF[1] и представляет согласованный взгляд сообщества IETF. Документ прошёл открытое обсуждение и был одобрен для публикации IESG[2]. Дополнительную информацию о стандартах Internet можно найти в разделе 2 в RFC 7841.

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке https://www.rfc-editor.org/info/rfc9155.

Оглавление

1. Введение....1
1.1. Уровни требований....2
2. Алгоритмы подписи....2
3. Запрос сертификата....2
4. Обмен ключами с сервером....2
5. Проверка сертификата....2
6. Взаимодействие с IANA....2
7. Вопросы безопасности....2
8. Литература....2
8.1. Нормативные документы....2
8.2. Дополнительная литература....2
Благодарности....3
Адреса авторов....3

1. Введение

Использование MD5 и SHA-1 для хэширования подписей в (D)TLS 1.2 задано в [RFC5246]. За прошедшее время стало ясно, что алгоритмы MD5 и SHA-1 небезопасны и подвержены атакам с конфликтами (collision attack) [Wang]. В 2011 г. в [RFC6151] были подробно рассмотрены вопросы безопасности, включая collision-атаки на MD5. В NIST официально отказались от использования SHA-1 в 2011 г. [NISTSP800-131A-R2] и запретили использование этого алгоритма для цифровых подписей в конце 2013 г., основываясь на описании атак в [Wang] и возможности подбора (brute-force attack). В 2016 г. исследователи из INRIA[3] обнаружили новый класс атак на основе конфликтов «расшифровки» (transcript) для протокола TLS (и других) за счёт алгоритма эффективного поиска конфликтов в базовых хэш-конструкциях [Transcript-Collision]. В 2017 г. исследователи из Google и CWI (Centrum Wiskunde & Informatica, Amsterdam) [SHA-1-Collision] доказали практическую осуществимость collision-атак на SHA-1. Этот документ обновляет [RFC5246], указывая **недопустимость** использования MD5 и SHA-1 в цифровых подписях. Однако документ не отменяет использование SHA-1 с HMAC для защиты записей. Отметим, что CABF (CA/Browser Forum) также отменил SHA-1 в подписях сертификатов [CABF].

[1]Internet Engineering Task Force - комиссия по решению инженерных задач Internet.
[2]Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.
[3]National Institute for Research in Digital Science and Technology - Национальный институт исследований в сфере цифровых наук и технологий США.

1.1. Уровни требований

Ключевые слова **должно** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не следует** (SHALL NOT), **следует** (SHOULD), **не нужно** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **не рекомендуется** (NOT RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе интерпретируются в соответствии с BCP 14 [RFC2119] [RFC8174] тогда и только тогда, когда они выделены шрифтом, как показано здесь.

2. Алгоритмы подписи

Клиенты **должны** включать расширение signature_algorithms и **недопустимо** включать в него MD5 или SHA-1.

3. Запрос сертификата

Серверам **не следует** включать MD5 и SHA-1 в сообщения CertificateRequest.

4. Обмен ключами с сервером

Серверам **недопустимо** включать MD5 и SHA-1 в сообщения ServerKeyExchange. Если клиент получает сообщение ServerKeyExchange, указывающее MD5 или SHA-1, он **должен** разорвать соединение с сигналом illegal_parameter.

5. Проверка сертификата

Клиентам **недопустимо** включать MD5 или SHA-1 в сообщения CertificateVerify. Если сервер получает CertificateVerify с или SHA-1, он **должен** разорвать соединение с сигналом illegal_parameter.

6. Взаимодействие с IANA

Агентство IANA обновило реестр TLS SignatureScheme, заменив рекомендуемый статус схем подписи на основе SHA-1 на N (не рекомендуется), как указано в [RFC8447]. Обновлённые записи указаны в таблице 1.

Таблица 1.

Значение	*Описание*	*Рекомендуется*	*Ссылки*
0x0201	rsa_pkcs1_sha1	N	[RFC8446] [RFC9155]
0x0203	ecdsa_sha1	N	[RFC8446] [RFC9155]

Агентство IANA также обновило ссылки в реестрах TLS SignatureAlgorithm и TLS HashAlgorithm, указав этот документ в дополнение к RFC 5246 и RFC 8447.

7. Вопросы безопасности

Современные реализации (D)TLS 1.2 с откатом к SHA-1 создают проблемы. Этот документ обновляет спецификацию TLS 1.2 [RFC5246] для отмены поддержки алгоритмов цифровой подписи MD5 и SHA-1. Однако документ не отменяет применение SHA-1 в HMAC для защиты записей.

8. Литература

8.1. Нормативные документы

[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. Дополнительная литература

[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>.

Благодарности

Авторы благодарны Hubert Kario за помощь при подготовке предварительной версии этого документа. Спасибо также Daniel Migault, Martin Thomson, Sean Turner, Christopher Wood, David Cooper за их отклики.

Адреса авторов

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

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru