Internet Engineering Task Force (IETF)
Request for Comments: 6149
Obsoletes: 1319
Category: Informational
ISSN: 2070-1721
March 2011

S. Turner
IECA
L. Chen
NIST

MD2 to Historic Status

Abstract

This document retires MD2 and discusses the reasons for doing so. This document moves RFC 1319 to Historic status.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

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). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6149.

Copyright Notice

1. Introduction

MD2 [MD2] is a message digest algorithm that takes as input a message of arbitrary length and produces as output a 128-bit "fingerprint" or "message digest" of the input. This document retires MD2. Specifically, this document moves RFC 1319 [MD2] to Historic status. The reasons for taking this action are discussed.

[HASH-Attack] summarizes the use of hashes in many protocols and discusses how attacks against a message digest algorithm's one-way and collision-free properties affect and do not affect Internet protocols. Familiarity with [HASH-Attack] is assumed.

2. Rationale

MD2 was published in 1992 as an Informational RFC. Since its publication, MD2 has been shown to not be collision-free [ROCH1995] [KNMA2005] [ROCH1997], albeit successful collision attacks for properly implemented MD2 are not that damaging. Successful pre-image and second pre-image attacks against MD2 have been shown [KNMA2005] [MULL2004] [KMM2010].

3. Documents that Reference RFC 1319

Use of MD2 has been specified in the following RFCs:

Proposed Standard (PS):

- o [RFC3279] Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

- o [RFC4572] Connection-Oriented Media Transport over the Transport Layer Security (TLS) Protocol in the Session Description Protocol (SDP).

Informational:

- o [RFC1983] Internet Users' Glossary.

- o [RFC2315] PKCS #7: Cryptographic Message Syntax Version 1.5.

- o [RFC2898] PKCS #5: Password-Based Cryptography Specification Version 2.0.

- o [RFC3447] Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1.

Experimental:

- [RFC2660] The Secure HyperText Transfer Protocol.

There are other RFCs that refer to MD2, but they have been either moved to Historic status or obsoleted by a later RFC. References and discussions about these RFCs are omitted. The exceptions are:

- [RFC2313] PKCS #1: RSA Encryption Version 1.5.

- [RFC2437] PKCS #1: RSA Cryptography Specifications Version 2.0.

4. Impact on Moving MD2 to Historic

The impact of moving MD2 to Historic on the RFCs specified in Section 3 is minimal, as described below.

Regarding PS RFCs:

- MD2 support in TLS was dropped in TLS 1.1.

- MD2 support is optional in [RFC4572], and SHA-1 is specified as the preferred algorithm.

- MD2 is included in the original PKIX certificate profile and the PKIX algorithm document [RFC3279] for compatibility with older applications, but its use is discouraged. SHA-1 is identified as the preferred algorithm for the Internet PKI.

Regarding Informational RFCs:

- The Internet Users’ Guide [RFC1983] provided a definition for Message Digest and listed MD2 as one example.

- PKCS#1 v1.5 [RFC2313] stated that there are no known attacks against MD2. PKCS#1 v2.0 [RFC2437] updated this stance to indicate that MD2 should only be supported for backward compatibility and to mention the attacks in [ROCH1995]. PKCS#1 [RFC3447] indicates that support of MD2 is only retained for compatibility with existing applications.

- PKCS#5 [RFC2898] recommends that the Password-Based Encryption Scheme (PBES) that uses MD2 not be used for new applications.

- PKCS#7 [RFC2315] was replaced by a series of Standards Track publications, "Cryptographic Message Syntax" [RFC2630] [RFC3369] [RFC5652] and "Cryptographic Message Syntax (CMS) Algorithms" [RFC3370]. Support for MD2 was dropped in [RFC3370].

RFC 2818, "HTTP Over TLS", which does not reference MD2, largely supplanted implementation of [RFC2660]. [RFC2660] specified MD2 for use both as a digest algorithm and as a MAC (Message Authentication Code) algorithm [RFC2104]. Note that this is the only reference to HMAC-MD2 found in the RFC repository.

5. Other Considerations

MD2 has also fallen out of favor because it is slower than both MD4 [MD4] and MD5 [MD5]. This is because MD2 was optimized for 8-bit machines, while MD4 and MD5 were optimized for 32-bit machines. MD2 is also slower than the Secure Hash Standard (SHS) [SHS] algorithms: SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512.

6. Security Considerations

MD2 is different from MD4 and MD5 in that is not a straight Merkle-Damgaard design. For a padded message with t blocks, it generates a nonlinear checksum as its t+1 block. The checksum is considered as the final block input of MD2.

As confirmed in 1997 by Rogier et al. [ROCH1997], the collision resistance property of MD2 highly depends on the nonlinear checksum. Without the checksum, a collision can be found in 2^12 MD2 operations, while with the checksum, the best collision attack takes 2^63.3 operations with 2^50 memory complexity [MULL2004], which is not significantly better than the birthday attack.

Even though collision attacks on MD2 are not significantly more powerful than the birthday attack, MD2 was found not to be one-way. In [KMM2010], a pre-image can be found with 2^104 MD2 operations. In an improved attack described in [KMM2010], a pre-image can be found in 2^73 MD2 operations. Because of this "invertible" property of MD2, when using MD2 in HMAC, it may leak information of the keys.

Obviously, the pre-image attack can be used to find a second pre-image. The second pre-image attack is even more severe than a collision attack to digital signatures. Therefore, MD2 must not be used for digital signatures.

Some may find the guidance for key lengths and algorithm strengths in [SP800-57] and [SP800-131] useful.

7. Recommendation

Despite MD2 seeing some deployment on the Internet, this specification recommends obsoleting MD2. MD2 is not a reasonable candidate for further standardization and should be deprecated in favor of one or more existing hash algorithms (e.g., SHA-256 [SHS]).

RSA Security considers it appropriate to move the MD2 algorithm to Historic status.

It takes a number of years to deploy crypto and it also takes a number of years to withdraw it. Algorithms need to be withdrawn before a catastrophic break is discovered. MD2 is clearly showing signs of weakness, and implementations should strongly consider removing support and migrating to another hash algorithm.

8. Acknowledgements

We’d like to thank RSA for publishing MD2. We’d also like to thank all the cryptographers who studied the algorithm. For their contributions to this document, we’d like to thank Ran Atkinson, Alfred Hoenes, John Linn, and Martin Rex.

9. Informative References

[HASH-Attack] Hoffman, P. and B. Schneier, "Attacks on Cryptographic Hashes in Internet Protocols", RFC 4270, November 2005.

[KMM2010] Knudsen, L., Mathiassen, J., Muller, F., and Thomsen, S., "Cryptanalysis of MD2", Journal of Cryptology, 23(1):72-90, 2010.

[KNMA2005] Knudsen, L., and J. Mathiassen, "Preimage and Collision Attacks on MD2", FSE 2005.

[MD2] Kaliski, B., "The MD2 Message-Digest Algorithm", RFC 1319, April 1992.

[MD4] Rivest, R., "The MD4 Message-Digest Algorithm", RFC 1320, April 1992.

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

[MULL2004] Muller, F., "The MD2 Hash Function Is Not One-Way", ASIACRYPT, LNCS 3329, pp. 214-229, Springer, 2004.

[RFC1983] Malkin, G., Ed., "Internet Users' Glossary", FYI 18, RFC 1983, August 1996.

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

[RFC2313] Kaliski, B., "PKCS #1: RSA Encryption Version 1.5", RFC 2313, March 1998.

[RFC2315] Kaliski, B., "PKCS #7: Cryptographic Message Syntax Version 1.5", RFC 2315, March 1998.

[RFC2437] Kaliski, B. and J. Staddon, "PKCS #1: RSA Cryptography Specifications Version 2.0", RFC 2437, October 1998.

[RFC2630] Housley, R., "Cryptographic Message Syntax", RFC 2630, June 1999.

[RFC2660] Rescorla, E. and A. Schiffman, "The Secure HyperText Transfer Protocol", RFC 2660, August 1999.

[RFC2898] Kaliski, B., "PKCS #5: Password-Based Cryptography Specification Version 2.0", RFC 2898, September 2000.

[RFC3279] Bassham, L., Polk, W., and R. Housley, "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3279, April 2002.

[RFC3369] Housley, R., "Cryptographic Message Syntax (CMS)", RFC 3369, August 2002.

[RFC3370] Housley, R., "Cryptographic Message Syntax (CMS) Algorithms", RFC 3370, August 2002.

[RFC3447] Jonsson, J. and B. Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", RFC 3447, February 2003.

[RFC4572] Lennox, J., "Connection-Oriented Media Transport over the Transport Layer Security (TLS) Protocol in the Session Description Protocol (SDP)", RFC 4572, July 2006.

[RFC5652] Housley, R., "Cryptographic Message Syntax (CMS)", STD 70, RFC 5652, September 2009.

[ROCH1995] Rogier, N., and P. Chauvaud, "The compression function of MD2 is not collision free", Presented at Selected Areas in Cryptography ’95, Carleton University, Ottawa, Canada. May 18-19, 1995.

[ROCH1997] Rogier, N. and P. Chauvaud, "MD2 is not secure without the checksum byte", Des. Codes Cryptogr. 12(3), 245-251 (1997).

[SHS] National Institute of Standards and Technology (NIST), FIPS Publication 180-3: Secure Hash Standard, October 2008.

[SP800-57] National Institute of Standards and Technology (NIST), Special Publication 800-57: Recommendation for Key Management - Part 1 (Revised), March 2007.

[SP800-131] National Institute of Standards and Technology (NIST), Special Publication 800-131: DRAFT Recommendation for the Transitioning of Cryptographic Algorithms and Key Sizes, June 2010.

Authors’ Addresses

Sean Turner
IECA, Inc.
3057 Nutley Street, Suite 106
Fairfax, VA 22031
USA

EMail: turners@ieca.com

Lily Chen
National Institute of Standards and Technology
100 Bureau Drive, Mail Stop 8930
Gaithersburg, MD 20899-8930
USA

EMail: lily.chen@nist.gov