Internet Engineering Task Force (IETF)
Request for Comments: 6150
Obsoletes: 1320
Category: Informational
ISSN: 2070-1721
March 2011

S. Turner
IECA
L. Chen
NIST

MD4 to Historic Status

Abstract

This document retires RFC 1320, which documents the MD4 algorithm, and discusses the reasons for doing so. This document moves RFC 1320 to Historic status.

Status of This Memo

Copyright Notice

1. Introduction

MD4 [MD4] 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 [MD4]. Specifically, this document moves RFC 1320 [MD4] 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

MD4 was published in 1992 as an Informational RFC. Since its publication, MD4 has been under attack [denBORBOS1992] [DOBB1995] [DOBB1996] [GLRW2010] [WLDCY2005] [LUER2008]. In fact, RSA, in 1996, suggested that MD4 should not be used [RSA-AdviceOnMD4]. Microsoft also made similar statements [MS-AdviceOnMD4].

In Section 6, this document discusses attacks against MD4 that indicate use of MD4 is no longer appropriate when collision resistance is required. Section 6 also discusses attacks against MD4's pre-image and second pre-image resistance. Additionally, attacks against MD4 used in message authentication with a shared secret (i.e., HMAC-MD4) are discussed.

3. Documents that Reference RFC 1320

Use of MD4 has been specified in the following RFCs:

Internet Standard (IS):

- o [RFC2289] A One-Time Password System.

Draft Standard (DS):

- o [RFC1629] Guidelines for OSI NSAP Allocation in the Internet.

Proposed Standard (PS):

- o [RFC3961] Encryption and Checksum Specifications for Kerberos 5.

Best Current Practice (BCP):

- o [RFC4086] Randomness Requirements for Security.

Informational:

- o [RFC1760] The S/KEY One-Time Password System.
- o [RFC1983] Internet Users' Glossary.
- o [RFC2433] Microsoft PPP CHAP Extensions.
- o [RFC2759] Microsoft PPP CHAP Extensions, Version 2.
- o [RFC3174] US Secure Hash Algorithm 1 (SHA1).
- o [RFC4757] The RC4-HMAC Kerberos Encryption Types Used by Microsoft Windows.
- o [RFC5126] CMS Advanced Electronic Signatures (CAdES).

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 notable exceptions are:

- o [RFC2313] PKCS #1: RSA Encryption Version 1.5.
- o [RFC2437] PKCS #1: RSA Cryptography Specifications Version 2.0.
- o [RFC3447] Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1.

4. Impact of Moving MD4 to Historic

The impact of moving MD4 to Historic is minimal with the one exception of Microsoft's use of MD4 as part of RC4-HMAC in Windows, as described below.

Regarding DS, PS, and BCP RFCs:

- o The initial One-Time Password systems, based on [RFC2289], have ostensibly been replaced by HMAC-based mechanism, as specified in "HOTP: An HMAC-Based One-Time Password Algorithm" [RFC4226]. [RFC4226] suggests following recommendations in [RFC4086] for random input, and in [RFC4086] weaknesses of MD4 are discussed.
- o MD4 was used in the Inter-Domain Routing Protocol (IDRP); each IDRP message carries a 16-octet hash that is computed by applying the MD-4 algorithm (RFC 1320) to the context of the message itself. Over time, IDRP was replaced by BGP-4 [RFC4271], which required at least [MD5].

o Kerberos Version 5 [RFC3961] specifies the use of MD4 for DES encryption types and checksum types. They were specified, never really used, and are in the process of being deprecated by [DES-DIE]. Further, the mandatory-to-implement encrypted types and checksum types specified by Kerberos are based on AES-256 and HMAC-SHA1 [RFC3962].

Regarding Informational RFCs:

o PKCS#1 v1.5 [RFC2313] indicated that there was no reason to not use MD4. PKCS#1 v2.0 [RFC2437] and v2.1 [RFC3447] recommend against MD4 due to cryptoanalytic progress having uncovered weaknesses in the collision resistance of MD4.

o Randomness Requirements [RFC4086] does mention MD4, but not in a good way; it explains how the algorithm works and that there have been a number of attacks found against it.

o The "Internet Users' Glossary" [RFC1983] provided a definition for Message Digest and listed MD4 as one example.

o The IETF OTP specification [RFC2289] was based on S/KEY technology. So S/KEY was replaced by OTP, at least in theory. Additionally, the S/KEY implementations in the wild have started to use MD5 in lieu of MD4.

o The CAdES document [RFC5126] lists MD4 as a hash algorithm, disparages it, and then does not mention it again.

o The SHA-1 document [RFC3174] mentions MD4 in the acknowledgements section.

o The three RFCs describing Microsoft protocols, [RFC2433], [RFC2759], and [RFC4757], are very widely deployed as MS-CHAP v1, MS-CHAP v2, and RC4-HMAC, respectively.

  o MS-CHAP Version 1 is supported in Microsoft's Windows XP, 2000, 98, 95, NT 4.0, NT 3.51, and NT 3.5, but support has been dropped in Vista. MS-CHAP Version 2 is supported in Microsoft's Windows 7, Vista, XP, 2000, 98, 95, and NT 4.0. Both versions of MS-CHAP are also supported by RADIUS [RFC2548] and the Extensible Authentication Protocol (EAP) [RFC5281]. In 2007, [RFC4962] listed MS-CHAP v1 and v2 as flawed and recommended against their use; these incidents were presented as a strong indication for the necessity of built-in crypto-algorithm agility in Authentication, Authorization, and Accounting (AAA) protocols.

- The RC4-HMAC is supported in Microsoft's Windows 2000 and later versions of Windows for backwards compatibility with Windows 2000. As [RFC4757] stated, RC4-HMAC doesn't rely on the collision resistance property of MD4, but uses it to generate a key from a password, which is then used as input to HMAC-MD5. For an attacker to recover the password from RC4-HMAC, the attacker first needs to recover the key that is used with HMAC-MD5. As noted in [RFC6151], key recovery attacks on HMAC-MD5 are not yet practical.

5. Other Considerations

rsync [RSYNC], a non-IETF protocol, once specified the use of MD4, but as of version 3.0.0 published in 2008, it has adopted MD5 [MD5].

6. Security Considerations

This section addresses attacks against MD4's collisions, pre-image, and second pre-image resistance. Additionally, attacks against HMAC-MD4 are discussed.

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

6.1. Collision Resistance

A practical attack on MD4 was shown by Dobbertin in 1996 with complexity 2^20 of MD4 hash computations [DOBB1996]. In 2004, a more devastating result presented by Xiaoyun Wang showed that the complexity can be reduced to 2^8 of MD4 hash operations. At the Rump Session of Crypto 2004, Wang said that as a matter of fact, finding a collision of MD4 can be accomplished with a pen on a piece of paper. The formal result was presented at EUROCRYPT 2005 in [WLDCY2005].

6.2. Pre-Image and Second Pre-Image Resistance

The first pre-image attack on full MD4 was accomplished in [LUER2008] with complexity 2^100. Some improvements are shown on pre-image attacks and second pre-image attacks of MD4 with certain pre-computations [GLRW2010], where complexity is reduced to 2^78.4 and 2^69.4 for pre-image and second pre-image, respectively. The pre-image attacks on MD4 are practical. It cannot be used as a one-way function. For example, it must not be used to hash a cryptographic key of 80 bits or longer.

6.3. HMAC

The attacks on Hash-based Message Authentication Code (HMAC) algorithms [RFC2104] presented so far can be classified in three types: distinguishing attacks, existential forgery attacks, and key recovery attacks. Of course, among all these attacks, key recovery attacks are the most severe attacks.

The best results on key recovery attacks on HMAC-MD4 were published at EUROCRYPT 2008 with 2^72 queries and 2^77 MD4 computations [WOK2008].

7. Recommendation

Despite MD4 seeing some deployment on the Internet, this specification obsoletes [MD4] because MD4 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 MD4 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. MD4 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 MD4. Obviously, we have to thank all the cryptographers who produced the results we refer to in this document. We’d also like to thank Ran Atkinson, Sue Hares, Sam Hartman, Alfred Hoenes, John Linn, Catherine Meadows, Magnus Nystrom, and Martin Rex for their input.

9. Informative References

[denBORBOS1992]
B. den Boer and A. Bosselaers. An attack on the last two rounds of MD4. In Advances in Cryptology - Crypto ’91, pages 194-203, Springer-Verlag, 1992.

[DES-DIE] Astrand, L., "Deprecate DES support for Kerberos", Work in Progress, July 2010.

[DOBB1995] H. Dobbertin. Alf swindles Ann. CryptoBytes, 1(3): 5, 1995.

[DOBB1996] H. Dobbertin. Cryptanalysis of MD4. In Proceedings of the 3rd Workshop on Fast Software Encryption, Cambridge, U.K., pages 53-70, Lecture Notes in Computer Science 1039, Springer-Verlag, 1996.

[GLRW2010] Guo, J., Ling, S., Rechberger, C., and H. Wang, "Advanced Meet-in-the-Middle Preimage Attacks: First Results on Full Tiger, and Improved Results on MD4 and SHA-2", http://eprint.iacr.org/2010/016.pdf.

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

[LUER2008] G. Leurent. MD4 is Not One-Way. Fast Software Encryption 2008, Lausanne, Switzerland, February 10-13, 2008, LNCS 5086. Springer, 2008.

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

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

[MS-AdviceOnMD4] Howard, M., "Secure Habits: 8 Simple Rules For Developing More Secure Code", http://msdn.microsoft.com/en-us/magazine/cc163518.aspx#S6.

[RFC1629] Colella, R., Callon, R., Gardner, E., and Y. Rekhter, "Guidelines for OSI NSAP Allocation in the Internet", RFC 1629, May 1994.

[RFC1760] Haller, N., "The S/KEY One-Time Password System", RFC 1760, February 1995.

[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.

[RFC2289] Haller, N., Metz, C., Nesser, P., and M. Straw, "A One-Time Password System", STD 61, RFC 2289, February 1998.

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

[RFC2433] Zorn, G. and S. Cobb, "Microsoft PPP CHAP Extensions", RFC 2433, October 1998.

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

[RFC2548] Zorn, G., "Microsoft Vendor-specific RADIUS Attributes", RFC 2548, March 1999.

[RFC2759] Zorn, G., "Microsoft PPP CHAP Extensions, Version 2", RFC 2759, January 2000.

[RFC3174] Eastlake 3rd, D. and P. Jones, "US Secure Hash Algorithm 1 (SHA1)", RFC 3174, September 2001.

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

[RFC3961] Raeburn, K., "Encryption and Checksum Specifications for Kerberos 5", RFC 3961, February 2005.

[RFC3962] Raeburn, K., "Advanced Encryption Standard (AES) Encryption for Kerberos 5", RFC 3962, February 2005.

[RFC4086] Eastlake 3rd, D., Schiller, J., and S. Crocker, "Randomness Requirements for Security", BCP 106, RFC 4086, June 2005.

[RFC4226] M'Raihi, D., Bellare, M., Hoornaert, F., Naccache, D., and O. Ranen, "HOTP: An HMAC-Based One-Time Password Algorithm", RFC 4226, December 2005.

[RFC4271] Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, January 2006.

[RFC4757] Jaganathan, K., Zhu, L., and J. Brezak, "The RC4-HMAC Kerberos Encryption Types Used by Microsoft Windows", RFC 4757, December 2006.

[RFC4962] Housley, R. and B. Aboba, "Guidance for Authentication, Authorization, and Accounting (AAA) Key Management", BCP 132, RFC 4962, July 2007.

[RFC5126] Pinkas, D., Pope, N., and J. Ross, "CMS Advanced Electronic Signatures (CAdES)", RFC 5126, March 2008.

[RFC5281] Funk, P. and S. Blake-Wilson, "Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)", RFC 5281, August 2008.

[RFC6151] Turner, S. and L. Chen, "Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms", RFC 6151, March 2011.

[RSA-AdviceOnMD4] Robshaw, M.J.B., "On Recent Results for MD2, MD4 and MD5", November 1996, ftp://ftp.rsasecurity.com/pub/pdfs/bulletn4.pdf.

[RSYNC] rsync web pages, http://www.samba.org/rsync/.

[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.

[WLDCY2005] X. Wang, X. Lai, D. Feng, H. Chen, and X. Yu, Cryptanalysis of Hash Functions MD4 and RIPEMD, LNCS 3944, Advances in Cryptology - EUROCRYPT2005, Springer, 2005.

[WOK2008] L. Wang, K. Ohta, and N. Kunihiro, New Key-recovery Attacks on HMAC/NMAC-MD4 and NMAC-MD5, EUROCRYPT 2008, LNCS 4965, Springer, 2008.

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