Network Working Group
Internet-Draft
Intended Status: Informational
Expires: August 3, 2011

T. Polk
L. Chen
NIST
S. Turner
IECA
P. Hoffman
VPN Consortium

February 3, 2011

Security Considerations for the SHA-0 and SHA-1 Message-Digest Algorithms
draft-turner-sha0-sha1-seccon-05

Abstract

This document includes security considerations for the SHA-0 and SHA-1 message digest algorithm.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on August 3, 2011.

Copyright Notice

described in the Simplified BSD License.

1. Introduction

The Secure Hash Algorithms are specified in [SHS]. A previous version of [SHS] also specified SHA-0. SHA-0, first published in 1993, and SHA-1, first published in 1996, are message digest algorithms, sometimes referred to as hash functions or hash algorithms, that take as input a message of arbitrary length and produce as output a 160-bit "fingerprint" or "message digest" of the input. The published attacks against both algorithms show that it is not prudent to use either algorithm when collision resistance is required.

[HASH-Attack] summarizes the use of hashes in Internet 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.

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

2. SHA-0 Security Considerations

What follows are summaries of recent attacks against SHA-0's collision, pre-image, and second pre-image resistance. Additionally, attacks against SHA-0 when used as a keyed-hash (e.g., HMAC-SHA-0) are discussed.

The U.S. National Institute of Standards and Technology (NIST) withdrew SHA-0 in 1996. That is, NIST no longer considers it appropriate to use SHA-0 for any transactions associated with the use of cryptography by U.S. Federal government agencies for the protection of sensitive, but unclassified information. SHA-0 is discussed here only for the sake of completeness.

Any use of SHA-0 is strongly discouraged. Analysis of SHA-0 continues today because many see it as a weaker version of SHA-1.

2.1. Collision Resistance

The first attack on SHA-0 was published in 1998 [CHJO1998] and showed that collisions can be found in 2^61 operations. In 2006, [NSSYK2006] showed an improved attack that can find collisions in 2^36 operations.

In any case, the known research results indicate that SHA-0 is not as collision resistant as expected. The collision security strength is significantly less than an ideal hash function (i.e., 2^36 compared

to 2^80).

2.2. Pre-image and Second Pre-image Resistance

The pre-image and second pre-image attacks published on reduced versions of SHA-0 (i.e., less than 80 rounds) indicate that the security margin of SHA-0 is resistant to these attacks. [deCARE2008] showed a pre-image attack on 49 out of 80 rounds with complexity of 2^159 and [AOSA2009] showed a pre-image attack on 52 out of 80 rounds with a complexity of 2^156.

2.3. HMAC-SHA-0

The current attack vectors on HMAC can be classified as follows: distinguishing attacks, existential forgery attacks, and key recovery attacks. Key recovery attacks are by far the most severe.

Attacks on hash functions can be conducted entirely offline, since the attacker can generate unlimited plaintext-ciphertext pairs. Attacks on HMACs must be online because attackers need a large amount of HMAC values to deduce the key. The best results for a partial key recovery attack on HMAC-SHA0 were published at ASIACRYPT 2006 with 2^84 queries and 2^60 SHA-0 computations [COYI2006].

3. SHA-1 Security Considerations

What follows are recent attacks against SHA-1's collision, pre-image, and second pre-image resistance. Additionally, attacks against SHA-1 when used as a keyed-hash (i.e., HMAC-SHA-1) are discussed.

It must be noted that NIST has recommended that SHA-1 not be used for generating digital signatures after Dec 31st 2010 and has specified that it not be used for generating digital signatures by U.S. Federal government agencies "for the protection of sensitive, but unclassified information" after December 31st 2013 [SP800-131].

3.1. Collision Resistance

The first attack on SHA-1 was published in early 2005 [RIOS2005]. This attack described a theoretical attack on a version of SHA-1 reduced to 53 rounds. The very next month [WLY2005] showed collisions in the full 80 rounds in 2^69 operations. Since then, many new analysis methods have been developed to improve the attack presented in [WLY2005]. However, there are no published results that improve upon the results found in [WLY2005]. The IACR ePrint version [Man2008/469] of [Man2009] claimed that using the method presented in the paper, a collision of full SHA-1 can be found in 2^51 hash function calls. However, this claim is absent from the published

conference paper [Man2009].

In any case, the known research results indicate that SHA-1 is not as collision resistant as expected. The collision security strength is significantly less than an ideal hash function (i.e., 2^69 compared to 2^80).

3.2. Pre-image and Second Pre-image Resistance

There are no known pre-image or second pre-image attacks that are specific to the full round SHA-1 algorithm. [KeSch] discovered a general result for all narrow pipe Merkle-Damgaard hash functions (which includes SHA-1), finding a second pre-image takes less than 2^n computations. When n = 160 as is the case for SHA-1, it will take 2^106 computations to find a second pre-image in a 60-byte message.

In the absence of full round attacks, cryptographers consider reduced-round attacks for clues regarding an algorithm's strength. Reduced-round attacks, where the number of reduced rounds is not more than a few less than the full rounds, have not been shown to relate to full-round attacks. However, the best reduced round attack indicates a certain security margin. For example, if the best known attack is on 60 out of 80 rounds, then the algorithm has about 20 rounds to resist improved attacks. However, the relationship between the number of rounds an attack can reach and the number of rounds defined in the algorithm is not linear; it does not provide a mathematical proof. In other words, reduced round attacks indicate how strong the algorithm is with regard to a certain attack, not how close it is to being broken. Therefore, the following information about reduced-round attacks is included only for completeness.

The pre-image and second pre-image attacks published on reduced versions of SHA-1 (i.e., less than 80 rounds) indicate that SHA-1 retains a significant security margin against these attacks. [AOSA2009] showed a pre-image attack on 48 out of 80 rounds with complexity of 2^159.

3.3. HMAC-SHA-1

As of today, there is no indication that attacks on SHA-1 can be extended to HMAC-SHA-1.

4. Conclusions

SHA-1 provides less collision resistance than was originally expected, and collision resistance has been shown to affect some (but not all) applications that use digital signatures. Designers of IETF protocols that use digital signature algorithms should strongly

consider support for a hash algorithm with greater collision resistance than that provided by SHA-1. Of course, SHA-0 should continue to not be used in any IETF protocol.

[Note: Protocol designers should review the current state of the art to ensure that selected hash algorithms provide sufficient security. At the time of publication, SHA-256 [SHS] is the most commonly specified alternative. The known (reduced round) attacks on the collision resistance of SHA-256 indicate a significant security margin, and the longer message digest provides increased strength.]

Nearly all IETF protocols that use signatures assume existing public key infrastructures, and SHA-1 is still used in signatures nearly everywhere. Therefore, it is unwise to strictly prohibit the use of SHA-1 in signature algorithms. Protocols that permit the use of SHA-1 based digital signatures as an option should strongly consider referencing this document in the security considerations.

A protocol designer might want to consider the use of SHA-1 with randomized hashing such as is specified in [SP800-107]. Note that randomized hashing expands the size of signatures and requires protocols to carry material that is not needed today. HMAC-SHA-1 remains secure and is the preferred keyed-hash algorithm for IETF protocol design.

5. Security Considerations

This entire document is about security considerations.

6. IANA Considerations

None.

7. Acknowledgements

We'd like to thank Ran Atkinson and Sheila Frankel for their comments and suggestions.

8. Normative References

[AOSA2009] Aoki, K., and K. Saski, "Meet-in-the-Middle Preimage Attacks Against Reduced SHA-0 and SHA-1", Crypto 2009.

[deCARE2008] De Canniere, C. and C. Rechberger, "Preimages for Reduced SHA-0 and SHA-1", Crypto 2008.

[CHJO1998] Chaubad, F., and A. Joux, "Differential Collisions in SHA-0", Crypto 1998.

[COYI2006] Contini, S., and Y. Lin, "Forgery and Partial Key-Recovery Attacks on HMAC and NMAC Using Hash Collisions", Asiacrypt 2006.

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

[KeSch] Kelsey, J., and B. Schneier, "Second Preimages on n-Bit Hash Functions for Much Less than 2n Work", In Cramer, R., ed.: EUROCRYPT'05. Volume 3494 of Lecture Notes in Computer Science, Springer (2005) 474-490.

[Man2008/469] Manuell, S., "Classification and Generation of Disturbance Vectors for Collision Attacks against SHA-1", http://eprint.iacr.org/2008/469.pdf.

[Man2009] Manuell, S., "Classification and Generation of Disturbance Vectors for Collision Attacks against SHA-1", International Workshop on Coding and Cryptography, 2009, Norway.

[NSSYK2006] Naito, Y., Sasaki, Y., Shimoyama, T., Yajima, J., Kunihiro, N. and K. Ohta, "Improved Collision Search for SHA-0", ASIACRYPT 2006.

[RIOS2005] Rijmen, V., and E. Oswald, "Update on SHA-1", CT-RSA 2005, LNCS 3376, pp. 58-71.

[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.

[SP800-107] National Institute of Standards and Technology (NIST), Special Publication 800-107: Recommendation for Applications using Approved Hash Algorithms, February 2009.

[SP800-131] National Institute of Standards and Technology (NIST), Special Publication 800-131A: Recommendation for the Transitioning of Cryptographic Algorithms and Key Sizes, January 2011.

[WLY2005] Wang, X., Yin, Y. and H. Yu., "Finding Collisions in the

Full SHA-1", Crypto 2005.

Authors' Addresses

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

EMail: tim.polk@nist.gov

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

EMail: lily.chen@nist.gov

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

EMail: turners@ieca.com

Paul Hoffman
VPN Consortium

EMail: paul.hoffman@vpnc.org