Network Working Group P Metzger
Internet Draft W A Simpson
expires in six months April 1995

IP Authentication using Keyed MD5
draft-ietf-ipsec-ah-md5-03.txt

Status of this Memo

This document is a submission to the IP Security Working Group of the Internet Engineering Task Force (IETF). Comments should be submitted to the ipsec@ans.net mailing list.

Distribution of this memo is unlimited.

This document is an Internet-Draft. Internet Drafts are working documents of the Internet Engineering Task Force (IETF), its Areas, and its Working Groups. Note that other groups may also distribute working documents as Internet Drafts.

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 not appropriate to use Internet Drafts as reference material, or to cite them other than as a ``working draft'' or ``work in progress.''

To learn the current status of any Internet-Draft, please check the ``1id-abstracts.txt'' listing contained in the internet-drafts Shadow Directories on:

ftp.is.co.za (Africa)
nic.nordu.net (Europe)
ds.internic.net (US East Coast)
ftp.isi.edu (US West Coast)
munnari.oz.au (Pacific Rim)

Abstract

This document describes the use of keyed MD5 with the IP Authentication Header.

1. Introduction

The Authentication Header (AH) [A-AH] provides integrity and authentication for IP datagrams.

This specification describes the AH use of Message Digest 5 (MD5) [RFC-1321].

All implementations that claim conformance or compliance with the Authentication Header specification MUST implement this MD5 mechanism.

Implementors should consult the most recent version of the IAB Standards [RFC-1720] for further guidance on the status of this document.

This document assumes that the reader is familiar with the related document "Security Architecture for the Internet Protocol" [A-SA], which defines the overall security plan for IP, and provides important background for this specification.

1.1. Keys

The secret authentication key shared between the communicating parties SHOULD be a pseudo-random number, not a guessable string of any sort.

1.2. Data Size

MD5's 128-bit output is naturally 64-bit aligned. Typically, there is no further padding of the Authentication Data field.

1.3. Performance

MD5 reportedly has a throughput of about 60 Mbps on a fast 64-bit RISC processor with slightly tuned MD5 code [Touch94].

Nota Bene: This is possibly too slow. Suggestions are sought on alternative authentication algorithms that have significantly faster throughput, are not patent-encumbered, and still retain adequate cryptographic strength.

2. Calculation

The 128-bit digest is calculated as described in [RFC-1321]. The specification of MD5 includes a portable 'C' programming language description of the MD5 algorithm.

The variable length secret authentication key is zero-filled to the next 128-bit boundary, concatenated with (immediately followed by) the invariant fields of the entire IP datagram, concatenated with (immediately followed by) the variable length secret authentication key again (trailing padding is added by the MD5 algorithm). The resulting 128-bit digest is inserted into the Authentication Data field.

Care must be taken that the keys and padding are not sent over the link.

Security Considerations

Users need to understand that the quality of the security provided by this specification depends completely on the strength of the MD5 hash function, the correctness of that algorithm's implementation, the security of the key management mechanism and its implementation, the strength of the key [CN94], and upon the correctness of the implementations in all of the participating nodes.

Among other considerations, applications may wish to take care not to select weak keys, although the odds of picking one at random are low [Schneier94, p 233].

At the time of writing of this document, it is known to be possible to produce collisions in the compression function of MD5 [BB93]. There is not yet a known method to exploit these collisions to attack MD5 in practice, but this fact is disturbing to some authors

[Schneier94].

It has also recently been determined [OW94] that it is possible to build a machine for $10 Million that could find messages that hash to an arbitrary given MD5 hash. This attack requires approximately 24 days. Although this is not a substantial weakness for most IP security applications, it should be recognized that current technology is catching up to the 128-bit hash length used by MD5. Applications requiring extremely high levels of security may wish to move in the near future to algorithms with longer hash lengths.

Acknowledgements

Some of the text of this specification was derived from work by Randall Atkinson for the SIP, SIPP, and IPv6 Working Groups.

The basic concept and use of MD5 is derived in large part from the work done for SNMPv2 [RFC-1446].

Steve Bellovin, Steve Deering, Frank Kastenholz, Charles Lynn, and Dave Mihelcic provided useful critiques of earlier versions of this draft. *

References

[A-SA] Randall Atkinson, "Security Architecture for the Internet Protocol", work in progress.

[A-AH] Randall Atkinson, "IP Authentication Header", work in progress.

[BB93] B. den Boer and A. Bosselaers, "Collisions for the Compression function of MD5", Advances in Cryptology -- Eurocrypt '93 Proceedings, Berlin: Springer-Verlag 1994

[CN94] Carroll, J.M., and Nudiati, S., "On Weak Keys and Weak Data: Foiling the Two Nemeses", Cryptologia, Vol. 18 No. 23 pp. 253-280, July 1994.

[RFC-1321]
Ronald Rivest, "The MD5 Message-Digest Algorithm", RFC-1321, DDN Network Information Center, April 1992.

[RFC-1446]
Galvin, J., and McCloghrie, K., "Security Protocols for Version 2 of the Simple Network Management Protocol (SNMPv2)", RFC-1446, DDN Network Information Center, April 1993. *

[RFC-1700]
Reynolds, J., and Postel, J., "Assigned Numbers", STD 2, RFC 1700, USC/Information Sciences Institute, October 1994. |

[RFC-1720] |
Postel, J., "Internet Official Protocol Standards", STD 1, | RFC 1720, USC/Information Sciences Institute, November 1994.

[OW94] Paul C. van Oorschot & Michael J. Wiener, "Parallel Collision Search with Application to Hash Functions and Discrete Logarithms", Proceedings of the 2nd ACM Conf. Computer and Communications Security, Fairfax, VA, Nov 3-5 1994.

[Schneier94]
Schneier, B., "Applied Cryptography", John Wiley & Sons, New York, NY, 1994. ISBN 0-471-59756-2

[Touch94]
Touch, J., "Report on MD5 Performance", work in progress, December 1994.

Author's Address

Questions about this memo can also be directed to:

Perry Metzger
Piermont Information Systems Inc.

160 Cabrini Blvd., Suite #2
New York, NY 10033

perry@piermont.com

William Allen Simpson
Daydreamer
Computer Systems Consulting Services
1384 Fontaine
Madison Heights, Michigan 48071

Bill.Simpson@um.cc.umich.edu
bsimpson@MorningStar.com

Table of Contents