Network Working Group
Request for Comments: 1828
Category: Standards Track

P. Metzger
Piermont
W. Simpson
Daydreamer

August 1995

IP Authentication using Keyed MD5

Status of this Memo

Abstract

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

Table of Contents

1. Introduction

The Authentication Header (AH) [RFC-1826] provides integrity and authentication for IP datagrams. This specification describes the AH use of keys with Message Digest 5 (MD5) [RFC-1321].

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

This document assumes that the reader is familiar with the related document "Security Architecture for the Internet Protocol" [RFC-1825], 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 cryptographically strong random number, not a guessable string of any sort.

The shared key is not constrained by this transform to any particular size. Lengths of up to 128 bits MUST be supported by the implementation, although any particular key may be shorter. Longer keys are encouraged.

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 software speeds are adequate for commonly deployed LAN and WAN links, but reportedly are too slow for newer link technologies [RFC-1810].

Nota Bene:
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 form of the authenticated message is

key, keyfill, datagram, key, MD5fill

First, the variable length secret authentication key is filled to the next 512-bit boundary, using the same pad with length technique defined for MD5.

Then, the filled key is concatenated with (immediately followed by) the invariant fields of the entire IP datagram (variant fields are zeroed), concatenated with (immediately followed by) the original variable length key again.

A trailing pad with length to the next 512-bit boundary for the entire message is added by MD5 itself. The 128-bit MD5 digest is calculated, and the result is inserted into the Authentication Data field.

Discussion:
When the implementation adds the keys and padding in place before and after the IP datagram, care must be taken that the keys and/or padding are not sent over the link by the link driver.

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.

At the time of writing of this document, it is known to be possible to produce collisions in the compression function of MD5 [dBB93]. 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 [vOW94] that it is possible to build a machine for $10 Million that could find two chosen text

variants with a common MD5 hash value. However, it is unclear whether this attack is applicable to a keyed MD5 transform.

This attack requires approximately 24 days. The same form of attack is useful on any iterated n-bit hash function, and the time is entirely due to the 128-bit length of the MD5 hash.

Although there is no 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

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

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, Phil Karn, Charles Lynn, Dave Mihelcic, Hilarie Orman, Jeffrey Schiller, Joe Touch, and David Wagner provided useful critiques of earlier versions of this draft.

References

[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.

[dBB93] den Boer, B., and Bosselaers, A., "Collisions for the Compression function of MD5", Advances in Cryptology -- Eurocrypt ’93 Proceedings, Berlin: Springer-Verlag 1994

[KR95] Kaliski, B., and Robshaw, M., "Message authentication with MD5", CryptoBytes (RSA Labs Technical Newsletter), vol.1 no.1, Spring 1995.

[RFC-1321]
Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, MIT and RSA Data Security, Inc., April 1992.

[RFC-1446]
Galvin, J., and K. McCloghrie, "Security Protocols for Version 2 of the Simple Network Management Protocol (SNMPv2)", RFC 1446, TIS, Hughes LAN Systems, April 1993.

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

[RFC-1800]
Postel, J., "Internet Official Protocol Standards", STD 1, RFC 1800, USC/Information Sciences Institute, July 1995.

[RFC-1810]
Touch, J., "Report on MD5 Performance", RFC 1810, USC/Information Sciences Institute, June 1995.

[RFC-1825]
Atkinson, R., "Security Architecture for the Internet Protocol", RFC 1825, NRL, August 1995.

[RFC-1826]
Atkinson, R., "IP Authentication Header", RFC 1826, NRL August 1995.

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

[vOW94] van Oorschot, P. C., and Wiener, M. J., "Parallel Collision Search with Applications to Hash Functions and Discrete Logarithms", Proceedings of the 2nd ACM Conf. Computer and Communications Security, Fairfax, VA, November 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